ПО-16-1034
21.08.2020

ДОГОВОР

Днес,.........................2020 г., в гр. София, между:

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ" АД, ЕИК: 831641791, със седалище и адрес на управление: гр. София 1504, район „Оборище", ул. „Панайот Волов"№ 2, представлявано от Ивайло Филипов – изпълнителен директор на дружеството, в качеството му на системен интегратор по чл. 7с от Закона за електронното управление и публичен възложител на обществени поръчки по смисъла на § 45, ал. 1 от Преходните и заключителни разпоредби към Закона за изменение и допълнение на Закона за електронното управление, наричано по-долу за краткост **ВЪЗЛОЖИТЕЛ**, от една страна,

и

„А1 БЪЛГАРИЯ" ЕАД, със седалище и адрес на управление гр. София, п.к. 1309 район „Илинден", ул. „Кукуш" № 1, ЕИК/БУЛСТАТ: 131468980, представлявано заедно от Александър Димитров – главен изпълнителен директор и Младен Маркоски – изпълнителен директор чрез Лилия Христова и Иван Иванов – пълномощници, съгласно нотариално заверено пълномощно рег. № 4836/2020 на нотариус Валентина Механджийска в район СРС, рег. № 074 на Нотариалната камара, наричан по-натагък за краткост **„ИЗПЪЛНИТЕЛ"**

(**ВЪЗЛОЖИТЕЛЯТ** и **ИЗПЪЛНИТЕЛЯТ** наричани заедно „Страните", а всеки от тях поотделно „Страна")

на основание чл. 112 от Закона за обществените поръчки (ЗОП), във връзка с чл. 69 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП), след проведена „открита" процедура за възлагане на обществена поръчка с предмет **„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите"**
и въз основа на Решение № 51-00-30-19/31.07.2020 г. на изпълнителния директор на „Информационно обслужване" АД за определяне на изпълнител на обществена поръчка по обособена позиция № 2 с предмет: „Доставка на софтуерно дефинирана мрежа за пренос на данни" (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, се сключи този договор (**„Договора/Договорът"**) за възлагане на обществена поръчка.

Страните се споразумяха за следното:

Заличаванията на информация в документа са на основания чл. 4 от Общ регламент за защита на данните.

I. ПРЕДМЕТ НА ДОГОВОРА

Чл. 1. (1) **ВЪЗЛОЖИТЕЛЯТ** възлага, а **ИЗПЪЛНИТЕЛЯТ** приема срещу възнаграждение да осъществи следните дейности:

1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването" или „доставките"), подробно описано по вид, количество и технически характеристики в Техническата спецификация на **ВЪЗЛОЖИТЕЛЯ** с предмет: „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите" – Приложение № 1 (наричана по-нататък „Техническа спецификация"), Приложение към нея, относимо към обособена позиция № 2 с предмет „Доставка на софтуерно дефинирана мрежа за пренос на данни" - Приложение № 1.2 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* и Техническото предложение на **ИЗПЪЛНИТЕЛЯ** по обособена позиция № 2 – Приложение № 2.2 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, представляващи неразделна част от настоящия договор.

2. гаранционно обслужване на доставеното по т. 1 оборудване (наричано алтернативно „гаранция и поддръжка"), осигурено в рамките на срока на гаранционно обслужване по чл. 4, ал. 3 в съответствие с предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) Доставката на оборудването по ал. 1, т. 1 се извършва от **ИЗПЪЛНИТЕЛЯ** въз основа на писмена заявка до **ИЗПЪЛНИТЕЛЯ**, отправена чрез адреса за кореспонденция на хартиен носител, или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на **ВЪЗЛОЖИТЕЛЯ** или упълномощен негов представител, съгласно клаузите на този договор. В писмената заявка се посочват:

1. Вид и количество на оборудването, което следва да бъде доставено;
2. Място на доставка на оборудването;
3. Срок на доставка, съобразен със сроковете и условията на доставка по настоящия договор.
4. Друга информация по преценка на **ВЪЗЛОЖИТЕЛЯ**, относима към изпълнението на договора.

II. ЦЕНИ И НАЧИН НА ПЛАЩАНЕ

Чл. 2. (1) Общата цена по договора е в размер на 4 086 643.00 лева (четири милиона осемдесет и шест хиляди шестотин четиридесет и три лева и нула стотинки) без ДДС, съгласно Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.2 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, неразделна част от настоящия договор.

(2) **ВЪЗЛОЖИТЕЛЯТ** заплаща на **ИЗПЪЛНИТЕЛЯ** цената за изпълнената доставка съобразно цените на оборудването, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.2

към настоящия договор (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*, умножено по броя на съответното доставено и прието оборудване (хардуер и софтуер).

(3) В цените по ал. 2, съответно в общата цена по ал. 1, са включени всички разходи на **ИЗПЪЛНИТЕЛЯ** по изпълнението на договора, като **ВЪЗЛОЖИТЕЛЯТ** не дължи заплащането на каквито и да е други разноски по договора.

(4) Цените по ал. 2, съответно общата цена по ал. 1, посочени в Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.2 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* са крайни и не могат да бъдат променяни за срока на договора, освен в случаите, когато промяната е в полза на **ВЪЗЛОЖИТЕЛЯ,** както и при спазване на реда и условията на ЗОП.

Чл. 3. (1) Плащането се извършва в срок до 30 (тридесет) дни след представяне на следните документи:

1. Двустранно подписан приемо-предавателен протокол за извършена доставка по чл. 6, ал. 1; съответно чл. 6, ал. 3, когато е приложимо.

2. Оригинална фактура, предоставена от **ИЗПЪЛНИТЕЛЯ,** която съдържа подробна разбивка по единични цени, по услуги и видове за всеки един компонент, съдържащ се в доставеното оборудване.

(2) Плащането се спира, когато **ИЗПЪЛНИТЕЛЯТ** бъде уведомен, че фактурата му не може да бъде платена, тъй като сумата не е дължима поради липсващи и/или некоректни придружителни документи или наличие на доказателства, че разходът е неправомерен. В този случай, **ИЗПЪЛНИТЕЛЯТ** трябва да даде разяснения, да направи изменения или представи допълнителна информация в срок до 3 (три) работни дни, след като бъде уведомен за това. В този случай срокът за извършване на плащане към **ИЗПЪЛНИТЕЛЯ** започва да тече от датата на която **ВЪЗЛОЖИТЕЛЯТ** получи правилно оформена фактура и/или поисканите разяснения, корекции и/или допълнителна информация.

(3) Плащанията се извършват от **ВЪЗЛОЖИТЕЛЯ** в български левове, с платежно нареждане по банкова сметка, посочена от **ИЗПЪЛНИТЕЛЯ**, както следва:

Банка: Райфайзенбанк

IBAN: BG94RZBB91551060362319

BIC: RZBBBGSF

(4) **ИЗПЪЛНИТЕЛЯТ** е длъжен да уведомява писмено **ВЪЗЛОЖИТЕЛЯ** за всички последващи промени по ал. 3 в срок до 3 (три) дни, считано от момента на промяната. В случай че **ИЗПЪЛНИТЕЛЯТ** не уведоми **ВЪЗЛОЖИТЕЛЯ** в този срок, счита се, че плащанията са надлежно извършени.

(5) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, **ВЪЗЛОЖИТЕЛЯТ** извършва окончателно плащане към него, след като бъдат представени доказателства, че

ИЗПЪЛНИТЕЛЯТ е заплатил на подизпълнителя/подизпълнителите за изпълнените от тях работи, които са приети по реда на раздел IV и са спазени условията на раздел IXа от настоящия договор.

III. СРОК И МЯСТО ЗА ИЗПЪЛНЕНИЕ

Чл. 4. (1) Договорът влиза в сила от датата на подписването му от двете страни и действието му се прекратява с изтичането на гаранционното обслужване, посочено в ал. 3. Датата на подписване е датата, посочена в деловодния номер на **ВЪЗЛОЖИТЕЛЯ**, поставен на стр. 1 от настоящия договор.

(2) Срокът на извършване на доставката на оборудването е до 78 (седемдесет и осем) календарни дни *(до 80 календарни дни съгласно изискванията на документацията за обществената поръчка по съответната обособена позиция)* от получаване на писмената заявка по чл. 1, ал. 2 от **ВЪЗЛОЖИТЕЛЯ**.

(3) Срокът на гаранционно обслужване на доставеното оборудване е 5 години *(минимум 5 (пет) години съгласно изискванията на документацията за обществената поръчка)* и започва да тече от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.

Чл. 5. (1) Мястото на извършване на доставката е на територията на гр. София, като **ВЪЗЛОЖИТЕЛЯТ** ще посочи в писмената заявка по чл. 1, ал. 2 конкретния адрес на извършване на доставката.

(2) Гаранционното обслужване ще се извършва по местонахождението на доставеното и инсталирано оборудване.

IV. УСЛОВИЯ НА ДОСТАВКА. ПРЕДАВАНЕ И ПРИЕМАНЕ НА ИЗПЪЛНЕНИЕТО

Чл. 6. (1) Приемането на всяка конкретна доставка на оборудването се удостоверява с двустранен приемо-предавателен протокол, който се подписва от упълномощените представители на страните по договора. При извършване на доставка на софтуер, **ИЗПЪЛНИТЕЛЯТ** представя на **ВЪЗЛОЖИТЕЛЯ** необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера. („**Приемо-предавателен протокол за доставка на оборудването**").

(2) **ВЪЗЛОЖИТЕЛЯТ** е длъжен да прегледа доставеното оборудване в момента на доставката и незабавно да уведоми **ИЗПЪЛНИТЕЛЯ** за несъответствия по отношение на количеството и качеството на някое от доставеното оборудване, в противен случай се счита, че същите са предадени без недостатъци. Приемането на доставката на оборудването с приемо-предавателен протокол няма отношение към установените впоследствие в срока на гаранционно обслужване дефекти и/или несъответствия, които **ИЗПЪЛНИТЕЛЯТ** е длъжен да отстрани за своя сметка в съответствие с условията на настоящия договор.

(3) При констатиране на явни недостатъци, повреди, дефекти, липси, и/или несъответствия на оборудването с Техническата спецификация – Приложение № 1, Приложение № 1.2 към нея *(попълва се за съответната позиция, за която участникът е избран за изпълнител)* или Техническото

предложение – Приложение № 2.2 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)* при извършване на прегледа по ал. 2, **ВЪЗЛОЖИТЕЛЯТ** има право да откаже да подпише съответния приемо-предавателен протокол. В тези случаи страните подписват двустранен констативен протокол, в който се описват констатираните недостатъци, повреди, дефекти, липси и/или несъответствия и се посочва срокът, в който същите да бъдат отстранени (**„Констативен протокол за липса на съответствие“**). След отстраняването им страните подписват двустранен приемо-предавателен протокол по реда и условията на ал. 1 за приемане на доставката.

(4) Правилото по ал. 2 не се прилага за недостатъци, които не са могли да бъдат забелязани при обикновен преглед. В тези случаи правата на **ВЪЗЛОЖИТЕЛЯ** по ал. 3 се запазват, ако той незабавно уведоми **ИЗПЪЛНИТЕЛЯ** за открития недостатък.

(5) Собствеността на доставеното оборудване и всички рискове преминават върху **ВЪЗЛОЖИТЕЛЯ** от датата на подписване на двустранния приемо-предавателен протокол по ал. 1 за приемане на доставката, съответно от датата на подписване на приемо-предавателния протокол по ал. 3, когато е приложимо.

(6) Когато **ИЗПЪЛНИТЕЛЯТ** е сключил договор/договори за подизпълнение, работата на подизпълнителя/подизпълнителите се приема от **ВЪЗЛОЖИТЕЛЯ** в присъствието на **ИЗПЪЛНИТЕЛЯ** и подизпълнителя/подизпълнителите.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ ПО ДОГОВОРА

Чл. 7. Изброяването на конкретни права и задължения на страните в този раздел от договора е неизчерпателно и не засяга действието на други клаузи от договора или от приложимото право, предвиждащи права и/или задължения на която и да е от страните.

Чл. 8. **ВЪЗЛОЖИТЕЛЯТ** има право да:

1. изисква от **ИЗПЪЛНИТЕЛЯ** да получи оборудването съгласно условията на настоящия договор и приложенията към него;

2. извършва проверка във всеки момент от изпълнението на договора относно качество, количества, стадий на изпълнение, технически параметри без с това да пречи на оперативната дейност на **ИЗПЪЛНИТЕЛЯ**;

3. изисква от **ИЗПЪЛНИТЕЛЯ** да сключи и да му представи договори за подизпълнение с посочените в офертата му подизпълнители.

Чл. 9. **ВЪЗЛОЖИТЕЛЯТ** е длъжен да:

1. оказва необходимото съдействие на **ИЗПЪЛНИТЕЛЯ** за изпълнение на задълженията, произтичащи от договора;

2. приеме доставеното оборудване при качествено и точно изпълнение на задълженията от страна на **ИЗПЪЛНИТЕЛЯ**;

3. да използва оборудването съобразно предназначението му и предписанията на производителя;

4. да заплати цената при извършване на доставката при качествено и точно изпълнение на задълженията, съгласно клаузите на настоящия договор.

Чл. 10. ИЗПЪЛНИТЕЛЯТ има право:

1. при пълно, точно и навременно изпълнение на задълженията си да получи уговореното възнаграждение при условията и в сроковете, посочени в настоящия договор;

2. да иска от **ВЪЗЛОЖИТЕЛЯ** необходимото съдействие за осъществяване на задълженията си по договора;

3. да иска от **ВЪЗЛОЖИТЕЛЯ** приемане на доставката, когато тя отговаря на изискванията, посочени в настоящия договор и приложенията към него.

Чл. 11. ИЗПЪЛНИТЕЛЯТ е длъжен да:

1. изпълни поръчката, предмет на настоящия договор, в срок и качествено, в съответствие с изискванията на Техническата спецификация и Техническото предложение, които представляват неразделна част от настоящия договор;

2. информира текущо **ВЪЗЛОЖИТЕЛЯ** за хода на изпълнението на настоящия договор и да го уведомява за всяко възникнало събитие, което би довело до забава и/или неизпълнение на задължение по договора и да предложи мерки за неговото преодоляване;

3. да предаде оборудването на **ВЪЗЛОЖИТЕЛЯ** в състояние, отговарящо на следните изисквания:

3.1. да е ново и оригинално, опаковано в оригинална опаковка на производителя с ненарушена цялост и всички необходимо, придружено със съответната техническа документация на електронен носител;

3.2. да отговаря на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа;

4. да заменя доставеното оборудване при констатиране от **ВЪЗЛОЖИТЕЛЯ** на скрити недостатъци с ново оборудване, отговарящо на изискванията на **ВЪЗЛОЖИТЕЛЯ**, съгласно клаузите на настоящия договор. Всички разходи по замяната са за сметка на **ИЗПЪЛНИТЕЛЯ**;

5. да извършва гаранционно обслужване на оборудването съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него,

6. по отношение на доставения софтуер (когато е приложимо):

6.1. да предоставя всички нови версии на софтуерните продукти, с оказване на необходимото съдействие на **ВЪЗЛОЖИТЕЛЯ** за изтеглянето им и за работата с тях (когато е приложимо);

6.2. да предоставя информация по запитвания и заявки от страна на **ВЪЗЛОЖИТЕЛЯ** във връзка с ползването на продуктите (когато е приложимо);

6.3. да оказва висококвалифицирана специализирана помощ и съдействие за отстраняването на възникнали инциденти и проблеми (когато е приложимо);

6.4. да отстранява възникнали грешки в софтуера и своевременното да го обновява (когато е приложимо);

6.5. да осигури свободно и безпрепятствено ползване на продуктите за срока на действие на доставените за тях лицензи (когато е приложимо).

7. да уведоми незабавно **ВЪЗЛОЖИТЕЛЯ** при възникване на пречки от стопански, административен или друг характер, които могат да забавят или да направят невъзможно изпълнението на този договор, като може да поиска от **ВЪЗЛОЖИТЕЛЯ** указания и/или съдействие за отстраняването им.

VI. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ

Чл. 12. (1) При подписването на този договор, **ИЗПЪЛНИТЕЛЯТ** предоставя на **ВЪЗЛОЖИТЕЛЯ** гаранция за изпълнение в размер на 1% (едно на сто) от стойността по чл. 2, ал. 1. („**Гаранцията за изпълнение**") или **40 866,43 лв.** (четиридесет хиляди осемстотин шестдесет и шест лева и четиридесет и три стотинки).

(2) Гаранцията за изпълнение е предназначена за обезпечаване на задълженията на **ИЗПЪЛНИТЕЛЯ** по договора, както следва:

1. 50% от сумата по ал. 1 – за изпълнение на дейностите по доставка на оборудването;

2. 50 % от сумата по ал. 1 – за изпълнение на дейностите по гаранционно обслужване.

(3) **ИЗПЪЛНИТЕЛЯТ** избира формата на гаранцията в една от следните форми:

1. парична сума внесена по банковата сметка на Възложителя;

2. банкова гаранция; или

3. застраховка, която обезпечава изпълнението чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ.**

Чл. 13. (1) В случай на изменение на договора, извършено в съответствие с този договор и приложимото право, **ИЗПЪЛНИТЕЛЯТ** се задължава да предприеме необходимите действия за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора, в срок до 3 (три) работни дни от подписването на допълнително споразумение за изменението.

(2) Действията за привеждане на Гаранцията за изпълнение в съответствие с изменените условия на договора могат да включват, по избор на **ИЗПЪЛНИТЕЛЯ**:

1. внасяне на допълнителна парична сума по банковата сметка на **ВЪЗЛОЖИТЕЛЯ**, при спазване на чл. 14 от договора; и/или;

2. предоставяне на документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, при спазване на изискванията на чл. 15 от договора; и/или

3. предоставяне на документ за изменение на първоначалната застраховка или нова застраховка, при спазване на изискванията на чл. 16 от договора.

Чл. 14. (1) Когато гаранцията се предоставя във вид на парична сума, тя се внася по следната банкова сметка на **ВЪЗЛОЖИТЕЛЯ:**

IBAN: BG43CECB979010C7866100;

BIC: CECBBGSF

Банка: „Централна кооперативна банка" АД

(2) Всички банкови разходи, свързани с преводите на сумата са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 15. (1) Когато като гаранция за изпълнение се представя банкова гаранция, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на банкова гаранция, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, която трябва да отговаря на следните изисквания:

1. да бъде безусловна и неотменяема банкова гаранция във форма, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, и да съдържа задължение на банката-гарант да извърши плащане при първо писмено искане от **ВЪЗЛОЖИТЕЛЯ**, деклариращ, че е налице неизпълнение на задължение на **ИЗПЪЛНИТЕЛЯ** или друго основание за задържане на Гаранцията за изпълнение по този договор;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на банковата гаранция се удължава или се издава нова.

(2) Всички банкови разходи свързани с откриването и обслужването на банковата гаранция, по усвояването на средства от страна на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, както и при нейното връщане са за сметка на **ИЗПЪЛНИТЕЛЯ**.

Чл. 16. (1) Когато като Гаранция за изпълнение се представя застраховка, **ИЗПЪЛНИТЕЛЯТ** предава на **ВЪЗЛОЖИТЕЛЯ** оригинален екземпляр на застрахователна полица, предварително съгласувана с **ВЪЗЛОЖИТЕЛЯ**, издадена в полза на **ВЪЗЛОЖИТЕЛЯ**, в която **ВЪЗЛОЖИТЕЛЯТ** е посочен като трето ползващо се лице (бенефициер), която трябва да отговаря на следните изисквания:

1. да обезпечава изпълнението на този договор чрез покритие на отговорността на **ИЗПЪЛНИТЕЛЯ** в определения в чл. 12, ал. 1 размер;

2. да бъде със срок на валидност за целия срок на действие на договора, плюс 30 (тридесет) дни, като при необходимост срокът на валидност на гаранцията се удължава или се издава нова.

3. Застрахователната премията по застраховката следва да е платена на сто процента (не се допуска разсрочено заплащане на застрахователната премия) и не може да бъде използвана за обезпечение на отговорността на изпълнителя по друг договор.

(2) Разходите по сключването на застрахователния договор и поддържането на валидността на застраховката за изисквания срок, както и по всяко изплащане на застрахователно обезщетение в полза на **ВЪЗЛОЖИТЕЛЯ**, при наличието на основание за това, са за сметка на **ИЗПЪЛНИТЕЛЯ**

Чл. 17. (1) **ВЪЗЛОЖИТЕЛЯТ** освобождава гаранцията за изпълнение, както следва:

1. Сумата по чл. 12, ал. 2, т. 1 се освобождава в срок до 30 (тридесет) дни след окончателното приемане на доставката, ако липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

2. Сумата по чл. 12, ал. 2, т. 2 се освобождава в срок до 30 (тридесет) дни след изтичане на срока на гаранционното обслужване, посочен в чл. 4, ал. 3, в случай, че липсват основания за задържането от страна на **ВЪЗЛОЖИТЕЛЯ**, на каквато и да е сума по нея.

(2) Освобождаването на Гаранцията за изпълнение се извършва, както следва:

1. когато е във формата на парична сума – чрез превеждане на сумата по банковата сметка на **ИЗПЪЛНИТЕЛЯ**, посочена в чл. 12, ал. 1 от договора;

2. когато е във формата на банкова гаранция – чрез връщане на нейния оригинал на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице;

3. когато е във формата на застраховка – чрез връщане на оригинала на застрахователната полица/застрахователния сертификат на представител на **ИЗПЪЛНИТЕЛЯ** или упълномощено от него лице.

(3) Гаранцията или съответната част от нея не се освобождава от **ВЪЗЛОЖИТЕЛЯ**, ако в процеса на изпълнение на договора е възникнал спор между Страните относно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** и въпросът е отнесен за решаване пред съд. При решаване на спора в полза на **ВЪЗЛОЖИТЕЛЯ** той може да пристъпи към усвояване на гаранциите.

Чл. 18. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи съответна част и да се удовлетвори от Гаранцията за изпълнение, когато **ИЗПЪЛНИТЕЛЯТ** не изпълни някое от неговите задължения по договора, както и в случаите на лошо, частично и забавено изпълнение на което и да е задължение на **ИЗПЪЛНИТЕЛЯ**, като усвои такава част от Гаранцията за изпълнение, която съответства на уговорената в договора неустойка за съответния случай на неизпълнение.

Чл. 19. **ВЪЗЛОЖИТЕЛЯТ** има право да задържи Гаранцията за изпълнение в пълен размер, в следните случаи:

1. при пълно неизпълнение и разваляне на договора от страна на **ВЪЗЛОЖИТЕЛЯ** на това основание;

2. при прекратяване на дейността на **ИЗПЪЛНИТЕЛЯ** или при обявяването му в несъстоятелност.

Чл. 20. Във всеки случай на задържане на Гаранцията за изпълнение, **ВЪЗЛОЖИТЕЛЯТ** уведомява **ИЗПЪЛНИТЕЛЯ** за задържането и неговото основание. Задържането на Гаранцията за изпълнение изцяло или частично не изчерпва правата на **ВЪЗЛОЖИТЕЛЯ** да търси обезщетение в по-голям размер.

Чл. 21. Когато **ВЪЗЛОЖИТЕЛЯТ** се е удовлетворил от Гаранцията за изпълнение и договорът продължава да е в сила, **ИЗПЪЛНИТЕЛЯТ** се задължава в срок до 5 (пет) дни да допълни Гаранцията за изпълнение, като внесе усвоената от **ВЪЗЛОЖИТЕЛЯ** сума по сметката на **ВЪЗЛОЖИТЕЛЯ** или предостави документ за изменение на първоначалната банкова гаранция или нова банкова гаранция, съответно застраховка, така че във всеки момент от действието на договора размерът на Гаранцията за изпълнение да бъде в съответствие с чл. 12, ал. 1 от договора.

Чл. 22. **ВЪЗЛОЖИТЕЛЯТ** не дължи лихва за времето, през което средствата по Гаранцията за изпълнение са престояли при него законосъобразно.

VII. ГАРАНЦИОННО ОБСЛУЖВАНЕ

Чл. 23. (1) **ИЗПЪЛНИТЕЛЯТ** гарантира за срока, посочен в чл. 4, ал. 3, пълната функционална годност на доставеното оборудване съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(2) В рамките на срока по ал. 1 **ИЗПЪЛНИТЕЛЯТ** отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на настоящия договор и приложенията към него.

(3) В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

Чл. 24. (1) В случай на констатиран дефект и/или несъотвествие от страна на **ВЪЗЛОЖИТЕЛЯ**, последният се задължава своевременно да уведоми **ИЗПЪЛНИТЕЛЯ** за възникналия дефект и/или несъответствие по факс, електронна поща (e-mail) или чрез регистрация в електронната система на **ИЗПЪЛНИТЕЛЯ** (**„рекламационно съобщение“**).

(2) **ИЗПЪЛНИТЕЛЯТ** е длъжен да осигури преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч. след получаване на рекламационното съобщение на **ВЪЗЛОЖИТЕЛЯ** по ал. 1. След преглед на оборудването се съставя констативен протокол за вида на повредата и/или несъответствието, работите и срока, необходими за отстраняването (**„Констативен протокол за повредата“**). Констативният протокол за повредата се подписва от представители на страните по договора.

(3) **ИЗПЪЛНИТЕЛЯТ** се задължава да отстрани настъпилата повреда и/или несъотвествие и възстановяване на пълната работоспособност на оборудването. Остраняването на настъпила повреда и/или несъответствието се осъществява по местоположението на оборудването.

(4) При невъзможост за отстраняване на настъпила повреда и/или несъответствие в срок от следващите два работни дни, **ИЗПЪЛНИТЕЛЯТ** осигурява на **ВЪЗЛОЖИТЕЛЯ** оборотно оборудване, притежаващо характеристиките в Техническото предложение на **ИЗПЪЛНИТЕЛЯ**, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното остраняване на повреда или несъотвествие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата.

(5) В случай, че повредата и/или несъотвествието прави устройството негодно за използване по предназначението му, **ИЗПЪЛНИТЕЛЯТ** е длъжен да замени го замени с ново, с параметри гарантиращи същата или по-добра функционалност и производителност. Приемането на новото устройство е по реда на чл. 6, ал. 1 (съответно чл. 6, ал. 3, когато е приложимо). В този случай продължава да тече срока на гаранционно обслужване за съответното заменено устройство, част от оборудването, част от оборудването, считано от датата на приемането му с приемо-предавателен протокол по чл. 6, ал. 1, (съответно чл. 6, ал. 3, когато е приложимо). Всички разходи за замяната са за сметка на **ИЗПЪЛНИТЕЛЯ.**

(6) За всяка извършена дейност по гаранционно обслужване се съставя протокол, който съдържа описание на извършената дейност. Протоколът се подписва от представители на страните по договора.

Чл. 25. (1) **ИЗПЪЛНИТЕЛЯТ** се задължава да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от **ВЪЗЛОЖИТЕЛЯ**. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които **ИЗПЪЛНИТЕЛЯТ** е отстранил проблемите.

(2) В случай, че **ВЪЗЛОЖИТЕЛЯТ** има забележки по представения отчет по ал. 1, **ВЪЗЛОЖИТЕЛЯТ** може да откаже да го подпише. В този случай **ВЪЗЛОЖИТЕЛЯТ** уведомява писмено **ИЗПЪЛНИТЕЛЯ** и в срок до 10 (десет) работни дни от получаване на уведомлението, страните подписват констативен протокол, в който се отразяват направените забележки и се определя срок за тяхното отстраняване. В случай че **ИЗПЪЛНИТЕЛЯТ** откаже да подпише констативния протокол **ВЪЗЛОЖИТЕЛЯТ** има право сам да състави такъв протокол като съдържанието му е задължително за **ИЗПЪЛНИТЕЛЯ**. Приемането се извършва след отстраняване на забележките в установения срок с подписването на коригиран отчет.

(3) Ако забележките не бъдат отстранени в установения срок, **ВЪЗЛОЖИТЕЛЯТ** може да развали договора с едностранно уведомление, отправено до другата страна, без да дава допълнителен срок за изпълнение.

VIII. НЕУСТОЙКИ

Чл. 26. (1) При пълно неизпълнение на договора от страна на **ИЗПЪЛНИТЕЛЯ, ВЪЗЛОЖИТЕЛЯТ** усвоява предоставената гаранция за изпълнение.

(2) При забавено изпълнение на задължения по договора от страна на **ИЗПЪЛНИТЕЛЯ** в нарушение на уговорените в този договор срокове, същият заплаща на **ВЪЗЛОЖИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден.

(3) При забава на **ВЪЗЛОЖИТЕЛЯ** за изпълнение на задълженията му за плащане по договора, същият заплаща на **ИЗПЪЛНИТЕЛЯ** неустойка в размер на 0,1 % (нула цяло и една десета на сто) от сумата по чл. 2, ал. 1, за всеки просрочен ден, но не повече от 3 на сто (три на сто) от тази сума.

(4) При системно (три и повече пъти) неизпълнение на задълженията за сервизно обслужване в гаранционния срок, **ИЗПЪЛНИТЕЛЯТ** дължи на **ВЪЗЛОЖИТЕЛЯ**, неустойка в размер на 0.5 (нула цяло и пет десети на сто) на сто от сумата по чл. 2, ал. 1.

Чл. 27. ВЪЗЛОЖИТЕЛЯТ може да претендира обезщетение за нанесени вреди и пропуснати ползи по общия ред, независимо от начислените неустойки и независимо от усвояването на гаранцията за изпълнение.

IXа. ПОДИЗПЪЛНИТЕЛИ (когато е приложимо)[1]

Чл. 27а. (1) **ИЗПЪЛНИТЕЛЯТ** е длъжен в срок от три дни от сключването на договор за подизпълнение, както и на допълнително споразумение за замяна на посочен в офертата подизпълнител, да изпрати на **ВЪЗЛОЖИТЕЛЯ** копие на договора/допълнителното споразумение, заедно с доказателства, че са изпълнени условията на чл. 66, ал. 2 или ал. 14 от ЗОП.

(2) **ИЗПЪЛНИТЕЛЯТ** носи пълна отговорност за действията и/или бездействията на подизпълнителите си, като участието им при изпълнението на поръчката, не изменя или намалява задълженията на **ИЗПЪЛНИТЕЛЯ**, съгласно настоящия договор. Видът и делът на участието на подизпълнителя/те следва да бъдат същите, като посочените в офертата на **ИЗПЪЛНИТЕЛЯ.**

(3) При сключването на договор/и с подизпълнител/и, оферирани/и в офертата на **ИЗПЪЛНИТЕЛЯ,** последният е длъжен да създаде условия, че:

1. приложимите клаузи на договора са задължителни за изпълнение от подизпълнителя/ите;

2. действията на подизпълнителя/ите няма да доведат пряко или косвено до неизпълнение на договора, за което **ИЗПЪЛНИТЕЛЯТ** да иска освобождаването си от отговорност;

3. при осъществяване на правата си по настоящия договор, **ВЪЗЛОЖИТЕЛЯТ** ще може без ограничения да извършва проверка на дейността и документацията на подизпълнителя/ите;

[1] Изискванията и условията, предвидени в този раздел се прилагат в случаите, когато Изпълнителят е предвидил използването на подизпълнители

4. подизпълнителят няма право да превъзлага една или повече от дейностите, които са включени в предмета на договора за подизпълнение.

(4) **ИЗПЪЛНИТЕЛЯТ** може да извършва замяна на посочените подизпълнители за изпълнение на договора, както и да включва нови подизпълнители в предвидените в ЗОП случаи и при предвидените в ЗОП условия.

(5) Сключването на договор с подизпълнител, който не е обявен в офертата на **ИЗПЪЛНИТЕЛЯ** и не е включен по време на изпълнение на договора по предвидения в ЗОП ред или изпълнението на дейностите по договора от лице, което не е подизпълнител, обявено в офертата на **ИЗПЪЛНИТЕЛЯ**, се счита за неизпълнение на договора и е основание за едностранно прекратяване на договора от страна на Възложителя и за усвояване на пълния размер на гаранцията за изпълнение.

(6) Независимо от използването на подизпълнители, отговорността за изпълнение на настоящия договор е на **ИЗПЪЛНИТЕЛЯ.**

Чл. 27б. (1) Когато частта от поръчката, която се изпълнява от подизпълнител, може да бъде предадена като отделен обект на **ИЗПЪЛНИТЕЛЯ** или на **ВЪЗЛОЖИТЕЛЯ**, **ВЪЗЛОЖИТЕЛЯТ** заплаща възнаграждение за тази част директно на подизпълнителя.

(2) Разплащанията по ал. 1 се осъществяват въз основа на искане, отправено от подизпълнителя до **ВЪЗЛОЖИТЕЛЯ** чрез **ИЗПЪЛНИТЕЛЯ**, който е длъжен да го предостави на **ВЪЗЛОЖИТЕЛЯ** в 15-дневен срок от получаването му.

(3) Към искането по ал. 2 **ИЗПЪЛНИТЕЛЯТ** предоставя становище, от което да е видно дали оспорва плащанията или част от тях като недължими.

(4) **ВЪЗЛОЖИТЕЛЯТ** има право да откаже плащане по ал. 2, когато искането за плащане е оспорено, до момента на отстраняване на причината за отказа.

IX. ПРЕКРАТЯВАНЕ И РАЗВАЛЯНЕ НА ДОГОВОРА

Чл. 28. (1) Настоящият договор се прекратява:

1. с изпълнение на всички задължения на страните по договора;

2. при настъпване на обективна невъзможност за изпълнение на договора, включително отмяна на изключителните права за системния интегртор за изпълнение на съответните дейности, посредством промяна в нормативната уредба.

3. при настъпване на друга невиновна невъзможност за изпълнение, непредвидено или непредотвратимо събитие от извънреден характер, възникнало след сключването на договора („непреодолима сила“), продължила повече от 45 дни;

4. при прекратяване на юридическо лице – Страна по договора без правоприемство, по смисъла на законодателството на държавата, в която съответното лице е установено;

5. при условията по чл. 5, ал. 1, т. 3 от Закона за икономическите и финансовите отношения с дружествата, регистрирани в юрисдикции с преференциален данъчен режим, контролираните от тях лица и техните действителни собственици.

(2) Настоящият договор може да бъде прекратен:

1. по взаимно съгласие на Страните, изразено в писмена форма;

2. когато за **ИЗПЪЛНИТЕЛЯ** бъде открито производство по несъстоятелност или ликвидация – по искане на **ВЪЗЛОЖИТЕЛЯ;**

Чл. 29. **ВЪЗЛОЖИТЕЛЯТ** прекратява договора в случаите по чл. 118, ал. 1 от ЗОП, без да дължи обезщетение на **ИЗПЪЛНИТЕЛЯ** за претърпени от прекратяването на Договора вреди, освен ако прекратяването е на основание чл. 118, ал. 1, т. 1 от ЗОП. (В последния случай размерът на обезщетението се определя в протокол или споразумение, подписано от Страните, а при непостигане на съгласие – по реда на клаузата за разрешаване на спорове по този договор.)

Чл. 30. (1) Всяка от страните може да развали договора при виновно неизпълнение на съществено задължение на другата страна по договора, при условията и с последиците съгласно чл. 87 и сл. от Закона за задълженията и договорите, чрез отправяне на писмено предупреждение от изправната страна до неизправната и определяне на подходящ срок за изпълнение. Разваляне на договора не се допуска, когато неизпълнената част от задължението е незначителна с оглед на интереса на изправната страна.

(2) По смисъла на този договор „виновно неизпълнение на съществено задължение на **ИЗПЪЛНИТЕЛЯ**" е:

1. когато **ИЗПЪЛНИТЕЛЯТ** забави изпълнението на задължение по настоящия договор с повече от 30 (тридесет) календарни дни;

2. при системно (три или повече пъти) неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционно обслужване на оборудването и при пълно неизпълнение на задълженията на **ИЗПЪЛНИТЕЛЯ** за гаранционното оборудване;

3. когато **ИЗПЪЛНИТЕЛЯТ** използва подизпълнител, без да е декларирал това в офертата си.

Чл. 31. При предсрочно прекратяване на договора, **ВЪЗЛОЖИТЕЛЯТ** е длъжен да заплати на **ИЗПЪЛНИТЕЛЯ** реално изпълнените и приети по установения ред доставки/услуги.

X. НЕПРЕОДОЛИМА СИЛА

Чл. 32. (1) Страните се освобождават от отговорност за неизпълнение на задълженията си, когато невъзможността за изпълнение се дължи на непреодолима сила. Никоя от страните не може да се позовава на непреодолима сила, ако е била в забава и не е информирала другата страна за възникването на непреодолима сила.

(2) Страната, засегната от непреодолима сила, е длъжна да предприеме всички разумни усилия и мерки, за да намали до минимум понесените вреди и загуби, както и да уведоми писмено другата страна незабавно при настъпване на непреодолимата сила.

(3) Докато трае непреодолимата сила, изпълнението на задължението се спира.

(4) Не може да се позовава на непреодолима сила онази страна, чиято небрежност или умишлени действия или бездействия са довели до невъзможност за изпълнение на договора.

XI. КОНФИДЕНЦИАЛНОСТ

Чл. 33. (1) Всяка от страните по този договор се задължава да пази в поверителност и да не разкрива или разпространява информация за другата страна, станала известна при или по повод изпълнението на договора (**„Конфиденциална информация“**) включително и след прекратяването на същия, неограничено във времето. Конфиденциална информация включва, без да се ограничава до: всякаква финансова, търговска, техническа или друга информация, анализи, съставени материали, изследвания, документи или други материали, свързани с бизнеса, управлението или дейността на другата Страна, от каквото и да е естество, или в каквато и да е форма, включително финансови и оперативни резултати, пазари, настоящи или потенциални клиенти, собственост, методи на работа, персонал, договори, ангажименти, правни въпроси или стратегии, продукти, процеси, свързани с документация, чертежи, спецификации, диаграми, планове, уведомления, данни , образци, модели, мостри, софтуер, софтуерни приложения, компютърни устройства или други материали или записи или друга информация, независимо дали в писмен или устен вид, или съдържаща се на компютърен диск или друго устройство. Не се смята за конфиденциална информацията, касаеща наименованието на договора, стойността и предмета на този договор, с оглед бъдещо позоваване на придобит професионален опит от **ИЗПЪЛНИТЕЛЯ**.

(2) Конфиденциална информация за целите на настоящия договор включва и :

1. съдържанието на данъчна и осигурителна информация, лични данни или друга защитена от закон или по силата на договора информация, която е станала известна при изпълнението на този договор.

2. информация, която е станала известна при изпълнението на този договор относно вътрешни правила и процедури, структура, начин на функциониране на Националната агенция за приходите (НАП) и **ВЪЗЛОЖИТЕЛЯ**, комуникации, мрежи и информационни системи на НАП и на **ВЪЗЛОЖИТЕЛЯ**, изготвени в хода на изпълнението на документи и/или всякакви други резултати от изпълнението, разработена в полза на НАП или предоставена им документация или програмен код в явен и изпълним вид във връзка с изпълнението на настоящия договор.

(3) Лични данни се обработват от Страните единствено за целите на изпълнение на договора, при стриктно спазване на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април

2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свобдното движение на такива данни и действащата нормативна уредба.

(4) Не се счита за нарушение на задълженията за неразкриване на Конфиденциална информация, когато:

1. Информацията е станала или става публично достъпна, без нарушаване на този договор от която и да е от страните;

2. Информацията се изисква по силата на закон, приложим спрямо която и да е от страните; или

3. Предоставянето на информацията се изисква от регулаторен или друг компетентен орган и съответната страна е длъжна да изпълни такова изискване;

В случаите по точки 2 или 3 страната, която следва да предостави информацията, уведомява незабавно другата страна по договора.

(5) Задълженията на **ИЗПЪЛНИТЕЛЯ** във връзка с изискванията за конфиденциалност включват и:

1. задължение да спазва вътрешните правила за достъп и режим на работа до сградите на НАП и на **ВЪЗЛОЖИТЕЛЯ**, когато е приложимо;

2. да спазва всички процедури и изисквания на НАП за работа в информационната инфраструктура на НАП;

3. да пази в поверителност и да не разкрива или разпространява информация за другата Страна, станала му известна при или по повод изпълнението на дейностите, предмет на договора.

4. представляващите **ИЗПЪЛНИТЕЛЯ** и лицата, които имат достъп до системите на НАП е необходимо за предоставят подписани декларации за опазване на информацията по образец, утвърден от НАП при подписване на договора и при необходимост от предоставяне на достъп до системите на НАП.

(6) С изключение на случаите, посочени в ал. 4, конфиденциална информация може да бъде разкривана само след предварително писмено одобрение от другата страна, като това съгласие не може да бъде отказано безпричинно.

(7) Задълженията по опазване от нерегламентиран достъп до конфиденциална информация се отнасят до **ИЗПЪЛНИТЕЛЯ**, всички негови поделения, контролирани от него фирми и организации, всички негови служители и наети от него физически или юридически лица, в това число подизпълнители, като **ИЗПЪЛНИТЕЛЯТ** отговаря за изпълнението на тези задължения от страна на такива лица.

(8) Всяка от страните се задължава да информира другата при нарушаване на изискванията за опазване на поверителност на информацията по този договор.

(9) Задълженията, свързани с неразкриването на Конфиденциалната информация остават в сила и след прекратяване на договора, на каквото и да е основание.

XII. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Чл. 34. (1) Освен ако са дефинирани изрично по друг начин в този договор, използваните в него понятия имат значението, дадено им в ЗОП, съответно в легалните дефиниции в Допълнителните разпоредби на ЗОП или, ако няма такива за някои понятия – според значението, което им се придава в основните разпоредби на ЗОП.

(2) При противоречие между различни разпоредби или условия, съдържащи се в договора и Приложенията, се прилагат следните правила:

1. специалните разпоредби имат предимство пред общите разпоредби;
2. разпоредбите на Приложенията имат предимство пред разпоредбите на Договора.

(3) В случаите, когато **ИЗПЪЛНИТЕЛЯТ** е представил Общи условия в офертата си, при възникнало противоречие между тях и клаузите на настоящия договор, с приоритет се прилагат клаузите на договора.

Чл. 35. Настоящият договор може да бъде изменян или допълван от страните при условията на чл. 116 от ЗОП.

Чл. 36. (1) Всички уведомления между Страните във връзка с този Договор се извършват в писмена форма и могат да се предават лично или чрез препоръчано писмо, по куриер, по факс, електронна поща или по телефон, което се потвърждава писмено на следните адреси:

1. За **ВЪЗЛОЖИТЕЛЯ**:

Адрес за кореспонденция: гр. София 1504, ул. „Панайот Волов“ № 2

Факс: 02/ 943 66 07

e-mail: office@is-bg.net;

тел. 02/942 03 40

2. За **ИЗПЪЛНИТЕЛЯ**:

Адрес за кореспонденция: гр. София, Община „Илинден“, ж.к. „Захарна фабрика“, п.к.1309, ул. „Кукуш“ №1

Факс: 02 495 79 07

e-mail: martin.yordanov@a1.bg

тел. 0882204054

(2) Страните упълномощават следните представители, които да проследяват и приемат изпълнението на задълженията им по настоящия договор, да осъществяват контрол по цялостното изпълнение на Договора и да подписват предвидените в Договора документи (уведомления, протоколи и др.), както следва:

1. За **ВЪЗЛОЖИТЕЛЯ**:

[redacted] - Ръководител, информационни и комуникационни технологии, Отдел „Комуникации“, e-mail:[redacted], тел. [redacted]

2. За **ИЗПЪЛНИТЕЛЯ**

[redacted] Акаунт мениджър "Държавни структури" при А1 България ЕАД; e-mail: [redacted] тел.[redacted]

(3) За дата на получаване на уведомлението/заявката се счита:

1. датата на предаването – при лично предаване на уведомлението;

2. датата на пощенското клеймо на обратната разписка – при изпращане по пощата;

3. датата на доставка, отбелязана върху куриерската разписка – при изпращане по куриер;

4. датата, посочена в извлечението от факс устройството– при изпращане по факс;

5. датата на която уведомлението/заявката е постъпила в посочената от **ИЗПЪЛНИТЕЛЯ** информационна система (e-mail) – при изпращане по електронна поща.

(4) Всяка кореспонденция между Страните ще се счита за валидна, ако е изпратена на посочените по-горе адреси (в т.ч. електронни), чрез посочените по-горе средства за комуникация и на посочените лица по ал. 2. При промяна на посочените адреси, телефони и други данни за контакт, съответната Страна е длъжна да уведоми другата в писмен вид в срок до 3 (три) работни дни от настъпване на промяната. При неизпълнение на това задължение всяко уведомление ще се счита за валидно връчено, ако е изпратено на посочените по-горе адреси, чрез описаните средства за комуникация и на посочените лица за контакт.

(5) При преобразуване без прекратяване, промяна на наименованието, правноорганизационната форма, седалището, адреса на управление, предмета на дейност, срока на съществуване, органите на управление и представителство на **ИЗПЪЛНИТЕЛЯ**, същият се задължава да уведоми **ВЪЗЛОЖИТЕЛЯ** за промяната в срок до 3 (три) дни от вписването ѝ в съответния регистър.

Чл. 37. Всички спорове по този договор ще се уреждат чрез преговори между страните, а при непостигане на съгласие, ще се отнасят за решаване от компетентния съд в Република България.

Чл. 38. За всички неуредени в този договор въпроси се прилагат разпоредбите на действащото законодателство.

Неразделна част от настоящия договор са:

1. Техническа спецификация на **ВЪЗЛОЖИТЕЛЯ** – Приложение № 1;

1.1. Приложение № 1.2 – Техническа спецификация, относима към обособена позиция № 2 с предмет „Доставка на софтуерно дефинирана мрежа за пренос на данни“ - Приложение № 1.2 (*попълва се за съответната позиция, за която участникът е избран за изпълнител)*

2. Техническо предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 2.2;

3. Ценовото предложение на **ИЗПЪЛНИТЕЛЯ** – Приложение № 3.2.

При подписване на договора, се представиха следните документи:

1. Гаранция за изпълнение на договора;

2. Документи по чл. 112, ал. 1 от ЗОП.

Настоящият договор се състави в 2 (два) еднообразни оригинални екземпляра на български език – 1 (един) за **ВЪЗЛОЖИТЕЛЯ** и 1 (един) за **ИЗПЪЛНИТЕЛЯ**, и се подписа, както следва:

ЗА ВЪЗЛОЖИТЕЛЯ:	**ЗА ИЗПЪЛНИТЕЛЯ:**
[redacted]	[redacted]
....	....
Ивайло Филипов	(подпис и печат)
Изпълнителен директор	**Лилия Христова**
	Пълномощник
[redacted]	[redacted]
....	....
Камелия Софрониева	**Иван Иванов**
Главен счетоводител	*Пълномощник*

[redacted]

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ПО ОТКРИТА ПРОЦЕДУРА ЗА ВЪЗЛАГАНЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

„ДОСТАВКА НА КОМУНИКАЦИОННО ОБОРУДВАНЕ, ХАРДУЕР И СОФТУЕР, НЕОБХОДИМИ ЗА ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ“

I. ПРЕДМЕТ НА ОБЩЕСТВЕНАТА ПОРЪЧКА

1. В предмета на обществената поръчка по обособени позиции №1, № 2, № 3, № 4, № 5, № 6 и № 9 се включват следните дейности:

1.1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването“), подробно описани по вид, количество и технически характеристики в настоящата Техническата спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

1.2. гаранционно обслужване на доставеното по т. 1.1. оборудване, осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

2. В предмета на обществената поръчка по обособени позиции № 7 и № 8 се включват следните дейности:

2.1. доставка на софтуер, необходим за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „софтуер“ или „доставките“), подробно описан по вид, количество и технически характеристики в настоящата Техническа спецификация, Приложенията към нея и Техническото предложение на участника, избран за изпълнител по съответната обособена позиция.

2.2. гаранционно обслужване на доставения софтуер по т. 2.1 (наричано алтернативно „гаранция и поддръжка“), осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ПОРЪЧКАТА

1. Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ".

Важно! *Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

2. Оборудването, предмет на доставката, се състои от хардуер и софтуер, които трябва да съответстват или да надвишават в техническо отношение посочените минимални изисквания в настоящата Техническа спецификация и/или приложенията към нея. За целта участникът представя към Техническото си предложение по съответната обособена позиция подробно описание на предлаганото от него оборудване/предлагания софтуер.

3. Оборудването (хардуер и софтуер), предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя към датата на сключване на договора за възлагане на обществената поръчка и да не е спряно от производство.

4. Хардуерните компоненти на оборудването трябва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

5. Оборудването следва да бъде доставено в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, в случай, че са различни от стандартни IEC C14 - IEC C13 или IEC C20 - IEC C19. Необходимата техническа документация, като потребителски, инсталационни, конфигурационни и др. ръководства да се представят на електронен носител за всеки тип от предлаганите устройства.

6. При доставката на софтуер следва да бъдат предоставени необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера.

III. УСЛОВИЯ НА ДОСТАВКА

1. Доставката на оборудването (хардуер и софтуер) се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка. В писмената заявка се посочват:

1.1. Вид и количество на оборудването (хардуер и софтуер), което следва да бъде доставено;

1.2. Място на доставка на оборудването (хардуер и софтуер);

1.3. Срок на доставка, съобразен със сроковете и условията на доставка по договора за обществена поръчка.

1.4. Друга информация по преценка на възложителя, относима към изпълнението на договора за обществена поръчка.

2. Приемането и предаването на изпълнението се осъществява въз основа на изискванията на договора за обществена поръчка.

IV. ГАРАНЦИЯ И ПОДДРЪЖКА. УСЛОВИЯ НА ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. Участникът, избран за изпълнител, гарантира за срока, посочен в т. V.2., пълната функционална годност на доставеното оборудване/доставения софтуер съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него.

2. В рамките на срока по посочен в т. V.2. и в съответствие с режима на гаранционно обслужване участникът, избран за изпълнител, отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на договора за обществена поръчка по съответната обособена позиция и приложенията към него. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

3. Режимът на гаранционното обслужване на хардуера е 5 дни в седмицата (от понеделник до петък), 8 часа в рамките на работното време от 9.00 ч. до 17.30 ч.

4. Времето за реакция на избрания за изпълнител участник е до следващия работен ден от уведомяването му.

* *Време за реакция е времето от момента на уведомяване от страна на Възложителя за възникнал проблем до обратна реакция (обаждане или пристигане на място) от участника, избран за изпълнител.*

5. Избраният за изпълнител участник е длъжен да осигури преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.

6. Избраният за изпълнител участник се задължава да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местоположение на оборудването.

7. При невъзможност за отстраняване на настъпила повреда и/или несъответствие в срок от следващите два работни дни, следва да бъде осигурено оборотно оборудване, притежаващо

характеристиките в Техническото предложение на участника, избран за изпълнител, включително нови алтернативни решения при запазване на пълната изисквана функционалност, до пълното отстраняване на повреда или несъответствие, като срока на гаранционно обслужване на оборудването в процес на поправяне, се удължава със срока, през който е траело отстраняването на повредата.

8. В случай, че повредата и/или несъответствието прави устройството негодно за използване по предназначението му, избраният за изпълнител участник е длъжен да го замени с ново, с параметри гарантиращи същата или по-добра функционалност и производителност.

9. За всяка извършена дейност, избраният за изпълнител участник изготвя и предоставя протокол, който съдържа описание на извършеното. Протоколът се подписва от представители на двете страни.

10. Избраният за изпълнител участник следва да предоставя обобщен отчет за извършените дейности по гаранционно обслужване на всяко тримесечие, които се приемат от възложителя. В обобщените отчети се посочва най-малко следната информация: период на покритие на отчета и списък с възникналите проблеми и параметрите, при които избраният за изпълнител участник е отстранил проблемите.

11. Всички разходи по време на гаранционното обслужване да са за сметка на избрания за изпълнител участник.

V. СРОК НА ИЗПЪЛНЕНИЕ

1. Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по т. III.1.

2. Срокът на гаранционно обслужване е минимум 5 (пет) години, считано от датата на приемо-предавателния протокол за доставка на оборудването (хардуер и софтуер). Участникът следва да посочи в офертата си срок на гаранционно обслужване, който да отговаря на съответните изисквания.

VI. МЯСТО НА ИЗПЪЛНЕНИЕ

1. Мястото на извършване на доставката е на територията на гр. София, като конкретния адрес на извършване на доставката ще бъде посочен в писмената заявка по т. III.1. .

2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталирано оборудване.

VII. ДРУГИ ИЗИСКВАНИЯ. ДОКУМЕНТИ КЪМ ОФЕРТАТА НА УЧАСТНИКА

1. В случай, че не е производител участникът следва да е упълномощен от производителя или от официален представител на производителя за доставка и гаранционно обслужване на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на територията на Република България.

За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлаганото оборудване. Горепосоченият документ се представя в техническото предложение на участника.

Забележка: *В случаите на представяне от участника на оторизационно писмо от официален представител на производителя, в офертата се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлаганото оборудване.*

2. Участникът следва да представи Общи условия или други приложими условия за гаранционно обслужване от производителя на продуктите, предмет на обществената поръчка, като ги приложи към техническото си предложение по съответната обособена позиция, в случай, че е приложимо.

VIII. ПРИЛОЖЕНИЯ:

1. Техническа спецификация по обособена позиция № 1 с предмет: **„Доставка на централен процесорен блок за обработка на информация, софтуерни пакети и операционни системи за виртуализация и сървъри за точно време "** – Приложение № 1.1.;
2. Техническа спецификация по обособена позиция № 2 с предмет: **„Доставка на софтуерно дефинирана мрежа за пренос на данни"** – Приложение № 1.2.;
3. Техническа спецификация по обособена позиция № 3 с предмет: **„Доставка на система за филтриране, проследяване и блокиране на Интернет трафик, система за управление на технически уязвимости и защитни стени за граничен слой"** – Приложение № 1.3.;
4. Техническа спецификация по обособена позиция № 4 с предмет: **„Доставка на дискови масиви за данни и хардуерни устройства и софтуерни пакети за създаване на резервни копия и възстановяване на данни"** – Приложение № 1.4.;
5. Техническа спецификация по обособена позиция № 5 с предмет: **„Доставка на софтуерни пакети и хардуерни устройства за дефиниране на опорна мрежа, мрежово оборудване за достъп до масивите за данни, защитни стени за интернет трафик и електронна поща и за локална мрежа"** – Приложение № 1.5.";

6. Техническа спецификация по обособена позиция № 6 с предмет **„Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“** – Приложение № 1.6.

7. Техническа спецификация по обособена позиция № 7 с предмет: **„Доставка на система за защита от изтичане/загуба на данни от крайните точки и от мрежата“** – Приложение № 1.7.;

8. Техническа спецификация по обособена позиция № 8 с предмет: **„Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“** – Приложение № 1.8.;

9. Техническа спецификация по обособена позиция № 9 с предмет: **„Доставка на хардуерни устройства и софтуерни пакети за платформа за управление на събития и сигурността на информацията“** – Приложение № 1.9.

Приложение № 1.2.

Техническа спецификация по обособена позиция № 2 с предмет: „Доставка на софтуерно дефинирана мрежа за пренос на данни“

1. **Софтуерно дефиниран маршрутизатор тип 1 – 36 броя.**

	Обща информация
REQ.1.	Захранване –в диапазона от минимум 100 до 240 VAC
REQ.2.	Работен температурен диапазон от 0° до +40 °C
REQ.3.	Безшумна работа – без вентилатори
REQ.4.	Минимум четири интерфейса 100/1000BASE-T
REQ.5.	Брой USB портове - минимум един, версия 3.0 или по-висока
REQ.6.	Сериен конзолен порт - минимум един
REQ.7.	Минимум 4GB DRAM
REQ.8.	Минимум 4 GB Flash
REQ.9.	Производителност от минимум 500Mbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.10.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.11.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.12.	Да поддържа изграждането на SDWAN overlay с използването на IPSec върху различни WAN мрежи – Internet и MPLS
REQ.13.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика
REQ.14.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.15.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.16.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.17.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SDWAN контролерите
REQ.18.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.19.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.20.	Да поддържа използване на сертификати от CA на възложителя
REQ.21.	Да поддържа минимум AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.22.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.
REQ.23.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.24.	Да поддържа автоматично маршутизиране на ниво приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay
REQ.25.	Да има вграден zone firewall
REQ.26.	Да има application firewall с вградено разпознаване на приложенията
REQ.27.	Да поддържа филтриране на трафика чрез ACL
REQ.28.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите.

REQ.29.	Да поддържа управляеми SDWAN IPSec топологии – hub-and-spoke, full mesh и комбинации между двете.
REQ.30.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.31.	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP
REQ.32.	Да поддържа PIM
REQ.33.	Да поддържа следните видове NAT услуги • статичен NAT • симетричен NAT • NAT64 • NAT pools • PAT
REQ.34.	Да поддържа изграждане на SD-WAN IPSec през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.35.	Да поддържа QoS: • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управление на задрсътванията с RED и WRED алгоритми • Traffic policing • Traffic shaping
REQ.36.	Да поддържа packet duplication – изпращане на един пакет по два или повече отделни SDWAN IPSec тунела до приемащия SD-WAN маршрутизатор
REQ.37.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.38.	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика

	• Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управелние на достъпа чрез RADIUS и TACACS+ системи.
REQ.39.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.40.	Устройството да е окомплектовано с SDWAN лицензи за минимум 100Mbps WAN трафик.
Гаранция и поддръжка:	
REQ.41.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.42.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.43.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.44.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

2. **Софтуерно дефиниран маршрутизатор тип 2 – 42 броя.**

Обща информация	
REQ.45.	Захранване –в диапазона от минимум 100 до 240 VAC
REQ.46.	Работен температурен диапазон от 0º до +40 ºC
REQ.47.	Безшумна работа – без вентилатори
REQ.48.	Минимум четири интерфейса 100/1000BASE-T и два интерфейса SFP
REQ.49.	Брой USB портове - минимум един, версия 3.0 или по-висока
REQ.50.	Сериен конзолен порт - минимум един
REQ.51.	Минимум 4GB DRAM
REQ.52.	Минимум 4 GB Flash
REQ.53.	Производителност от минимум 1Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.54.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.55.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.56.	Да поддържа изграждането на SDWAN overlay с използването на IPSec
REQ.57.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика
REQ.58.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.59.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.60.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.61.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите
REQ.62.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.63.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.64.	Да поддържа използване на сертификати от CA на възложителя
REQ.65.	Да поддържа минимум AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.66.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.

REQ.67.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.68.	Да поддържа автоматично маршутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay.
REQ.69.	Да има вграден zone firewall
REQ.70.	Да има application firewall с вградено разпознаване на приложенията
REQ.71.	Да поддържа филтриране на трафика чрез ACL
REQ.72.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите
REQ.73.	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете
REQ.74.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.75.	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP • VRRP
REQ.76.	Да поддържа 802.1Q
REQ.77.	Да поддържа обединяване на интерфейси в bridge групи
REQ.78.	Да поддържа IGMP v1 и v2
REQ.79.	Да поддържа PIM
REQ.80.	Да поддържа следните видове NAT услуги • статичен NAT • динамичен NAT • NAT64 • NAT pools • PAT
REQ.81.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.82.	Да поддържа QoS: • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управелние на задрсътванията с RED и WRED алгоритми • Traffic policing • Traffic shaping
REQ.83.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор
REQ.84.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.85.	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание

	• DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.86.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.87.	Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик.
Гаранция и поддръжка:	
REQ.88.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.89.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.90.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.91.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

3. **Софтуерно дефиниран маршрутизатор тип 3 – 36 броя.**

Обща информация	
REQ.92.	Захранване –в диапазона от минимум 100 до 240 VAC
REQ.93.	Работен температурен диапазон от 0° до +40 °C
REQ.94.	Шаси за монтаж в 19“ шкаф
REQ.95.	Два токозахранващи модула
REQ.96.	Минимум четири интерфейса, които поддържат 100/1000BASE-T и SFP
REQ.97.	Брой USB портове - минимум 1
REQ.98.	Конзолен порт - 1
REQ.99.	Минимум 8GB DRAM
REQ.100.	Възможност за добавяне на модул с LTE cat. 6 модем
REQ.101.	Възможност за добавяне на минимум осем 1000Base-T порта
REQ.102.	Производителност от минимум 3Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.103.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.104.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.105.	Да поддържа изграждането на SDWAN overlay с използването на IPSec
REQ.106.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика

REQ.107.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.108.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.109.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.110.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите
REQ.111.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.112.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.113.	Да поддържа използване на сертификати от CA на възложителя
REQ.114.	Да поддържа минимум AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.115.	Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация
REQ.116.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.
REQ.117.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.118.	Да поддържа автоматично маршутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay
REQ.119.	Да има вграден zone firewall
REQ.120.	Да има application firewall с вградено разпознаване на приложенията
REQ.121.	Да поддържа филтриране на трафика чрез ACL
REQ.122.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите
REQ.123.	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете
REQ.124.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.125.	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP • VRRP
REQ.126.	Да поддържа 802.1Q
REQ.127.	Да поддържа IGMP v2 и v3
REQ.128.	Да поддържа минимум PIM SSM
REQ.129.	Да поддържа PIM rendezvous point
REQ.130.	Да поддържа статичен и динамичен NAT и NAT pool
REQ.131.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.132.	Да поддържа QoS: • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм

	• Управелние на задрсътванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропусквателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики
REQ.133.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор
REQ.134.	Да има вграден IPS
REQ.135.	Да има вградена Anti Malware защита
REQ.136.	Да има URL филтриране по категории
REQ.137.	Да осигурява декриптиране на SSL и TLS за инспектиране на криптиран трафик
REQ.138.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.139.	Да поддържа висока надеждност чрез съвместна работа с второ устройство от същия тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели
REQ.140.	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управелние на достъпа чрез RADIUS и TACACS+ системи.
REQ.141.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.142.	Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик
Гаранция и поддръжка:	
REQ.143.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.144.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.145.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.146.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

4. **Софтуерно дефиниран маршрутизатор тип 4 – 2 броя.**

Обща информация	
REQ.147.	Захранване –в диапазона от минимум 100 до 240 VAC
REQ.148.	Работен температурен диапазон от 0° до +40 °C
REQ.149.	Шаси за монтаж в 19" шкаф
REQ.150.	Два токозахранващи модула
REQ.151.	Минимум шест 1000BaseT и два SFP+ порта.
REQ.152.	Устройството да бъде доставено с четири 10GBASE-SR SFP+ модула
REQ.153.	Брой USB портове - минимум 1,
REQ.154.	Сериен конзолен порт - минимум 1
REQ.155.	Минимум 8GB DRAM
REQ.156.	Производителност от минимум 6Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя
REQ.157.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание
REQ.158.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи
REQ.159.	Да поддържа изграждането на SDWAN overlay с използването на IPSec
REQ.160.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика
REQ.161.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм
REQ.162.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.163.	Да поддържа изграждане на GRE тунели до външни системи за сигурност
REQ.164.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите
REQ.165.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати
REQ.166.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност
REQ.167.	Да поддържа използване на сертификати от CA на възложителя
REQ.168.	Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.169.	Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация
REQ.170.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.
REQ.171.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.172.	Да поддържа автоматично маршутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay
REQ.173.	Да има вграден zone firewall
REQ.174.	Да има application firewall с вградено разпознаване на приложенията
REQ.175.	Да поддържа филтриране на трафика чрез ACL
REQ.176.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите
REQ.177.	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете

REQ.178.	Да поддържа отделна, виртуална, топология за всеки сегмент
REQ.179.	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP • VRRP
REQ.180.	Да поддържа 802.1Q
REQ.181.	Да поддържа IGMP v2 и v3
REQ.182.	Да поддържа минимум PIM SSM
REQ.183.	Да поддържа PIM rendezvous point
REQ.184.	Да поддържа статичен и динамичен NAT и NAT pool
REQ.185.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay
REQ.186.	Да поддържа QoS: • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управление на задрсътванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропускателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики
REQ.187.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор
REQ.188.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS
REQ.189.	Да поддържа висока надеждност чрез съвместна работа с второ устройство от същия тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели
REQ.190.	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP

	• SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управелние на достъпа чрез RADIUS и TACACS+ системи.
REQ.191.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;
REQ.192.	Устройството да е окомплектовано с SDWAN лицензи за минимум 5Gbps WAN трафик
Гаранция и поддръжка:	
REQ.193.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.194.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.195.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.196.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

5. **Софтуер за управление на софтуерно дефинирана мрежа**

Обща информация	
REQ.197.	Софтуерни контролери за изграждане и управление на SDWAN мрежа с SDWAN маршрутизаторите в това задание
REQ.198.	Инсталация – върху VMWare ESXi на възложителя
REQ.199.	Количество – съгласно изискванията на производителя за постигане на висока надеждност и резервиране на SDWAN контролната система
REQ.200.	Автоматично присъединяване и провизиране на маршрутизаторите в SDWAN средата чрез използване на компонент за оркестриране, който осигурява plug-and-play, zero touch plug&play и подобни решения за автоматизация.
REQ.201.	Управление на маршрутизаторите и техните функции в SDWAN мрежата чрез темплейти
REQ.202.	Управление на услугите и виртуалните топологии в SDWAN мрежата чрез политики
REQ.203.	Управление на транспортната IPSec топология чрез политики
REQ.204.	Динамично управление на различни трафични класове през IPSec транспортната инфраструктура на база параметрите на тунелите – jitter, latency, загуба на пакети
REQ.205.	Управление на IPS, application Firewall, URL Filter и Malware защитата в SDWAN машршрутизаторите с такива функции.
REQ.206.	Наблюдение на SDWAN маршрутизаторите
REQ.207.	Наблюдение на SDWAN IPSec транспортните тунели и техните параметри – минимум up/down, packet loss, jitter и delay
REQ.208.	Наблюдение на трафичните параметри от различни класове приложения, които използват SD-WAN мрежата
REQ.209.	Визуализация на маршрутите за различните класове трафик през SDWAN мрежата
REQ.210.	Изграждане на карта с топологията на SD-WAN мрежата с овърлей върху географска карта на страната.
REQ.211.	Визуализация на пътя на трафичните потоци, на ниво приложения, върху транспортните тунели.
REQ.212.	Преодставяне на информация за QoS на трафичните потоци от приложенията

REQ.213.	Исторически справки за трафичните потоци през SDWAN мрежата
REQ.214.	Web GUI интерфейс
REQ.215.	Role based access controll
REQ.216.	Да поддържа SSO съвместимо с Microsoft ADFS
REQ.217.	Да има REST API за интеграция с външни софтуерни системи
Гаранция и поддръжка:	
REQ.218.	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.219.	Срок на техническа поддръжка – минимум 5 (пет) години.
REQ.220.	Получаване на нови версии на софтуера - минимум 5 (пет) години.
REQ.221.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години

6. **Съвместимост на компоненти**

Обща информация	
REQ.222.	За постигането на пълна съвместимост и улеснена експлоатация на SDWAN мрежата, предлаганите SDWAN рутери, SFP+ модули и софтуерни компоненти за сигурност трябва да са от един производител.

П Ъ Л Н О М О Щ Н О

Долуподписаната,

СТАНИСЛАВА ДИМИТРОВА ШИЯКОВА,
ЕГН: [redacted], л. к. № [redacted] издадена на [redacted], на длъжност Старши Продуктов Мениджър „Ценообразуване“, отдел „Държавни структури“, Направление „Корпоративни продажби” при „А1 България” ЕАД,

в качеството си на пълномощник на Изпълнителните директори на **„А1 България” ЕАД**, със седалище и адрес на управление: гр. София 1309, Столична община, район „Илинден”, ул. “Кукуш” № 1, регистрирано в Търговски регистър – Агенция по вписванията с ЕИК: 131468980, ИН по ЗДДС: BG131468980, с пълномощно рег. № 1287/ 2020 г., нотариално заверено от нотариус Мира Глосова, с район на действие СРС с рег. № 074 на Нотариалната камара,

П Р Е У П Ъ Л Н О М О Щ А В А М:

МАРТИН ДИМИТРОВ ЙОРДАНОВ,
ЕГН[redacted], на длъжност Акаунт Мениджър "Държавни структури", отдел "Държавни структури", направление „Корпоративни продажби” при „А1 БЪЛГАРИЯ” ЕАД,

СТАНИСЛАВ АНГЕЛОВ АНГЕЛОВ,
ЕГН:[redacted], на длъжност Акаунт Мениджър “Държавни структури”, отдел "Държавни структури", направление „Корпоративни продажби” при „А1 БЪЛГАРИЯ” ЕАД;

заедно и поотделно да представляват “А1 БЪЛГАРИЯ” ЕАД пред **„Информационно обслужване" АД**, като извършват всички необходими правни и фактически действия, свързани с участие в обществена поръчка със следния предмет:

„ДОСТАВКА НА КОМУНИКАЦИОННО ОБОРУДВАНЕ, ХАРДУЕР И СОФТУЕР, НЕОБХОДИМИ ЗА ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ“ Обособена позиция № 1 с предмет: „Доставка на централен процесорен блок за обработка на информация, софтуерни пакети и операционни системи за виртуализация и сървъри за точно време, Обособена позиция № 2 с предмет: „Доставка на софтуерно дефинирана мрежа за пренос на данни, Обособена позиция № 3 с предмет: „Доставка на система за филтриране, проследяване и блокиране на Интернет трафик, система за управление на технически уязвимости и защитни стени за граничен слой, Обособена позиция № 4 с предмет: „Доставка на дискови масиви за данни и хардуерни устройства и софтуерни пакети за създаване на резервни копия и възстановяване на данни“, Обособена позиция № 5 с предмет: „Доставка на софтуерни пакети и хардуерни устройства за дефиниране на опорна мрежа, мрежово оборудване за достъп до масивите за данни, защитни стени за интернет трафик и електронна поща и за локална мрежа“, Обособена позиция № 6 с предмет „Доставка на хардуерни устройства и софтуерни пакети за платформа за защита от съществуващи и новооткрити кибер заплахи“, , Обособена позиция № 7 с предмет: „Доставка на система за защита от изтичане/загуба

[redacted]

[redacted]

[redacted]

КП2

на данни от крайните точки и от мрежата“, Обособена позиция № 8 с предмет: „Доставка на система за управление и контрол на електронната идентичност и достъпа до информацията“, Обособена позиция № 9 с предмет: „Доставка на хардуерни устройства и софтуерни пакети за платформа за управление на събития и сигурността на информацията“

Упълномощените лица имат право включително и без ограничение, да подават и получават документи по процедурата, да заверяват за вярност с оригинала и да подписват офертата, включително ценовата оферта и всички представени документи, да участват при отваряне и разглеждане на предложенията, да участват в преговори и др.

ПРЕУПЪЛНОМОЩИТЕЛ:

..............[redacted]..

СТАНИСЛАВА ДИМИТРОВА ШИЯКОВА

На **2.7.2020 г.**, **Мира Глосова** - помощник-нотариус по заместване при **Валентина Механджийска**, нотариус в район **СРС**, рег. № **074** на Нотариалната камара, удостоверявам подписите върху този документ, положени от:
СТАНИСЛАВА ДИМИТРОВА ШИЯКОВА, ЕГН [redacted] като пълномощник на А1 БЪЛГАРИЯ ЕАД, БУЛСТАТ/ЕИК 131468980, ф.д. 67/2005, ОС СОФИЯ ГРАД
Рег. № **4142/2020**, Събрана такса: 12.00 лв.

Помощник-нотариус по заместване: [redacted]

НОТАРИУС № 074 * Валентина МЕХАНДЖИЙСКА Район на действие р.с. СОФИЯ * РЕПУБЛИКА БЪЛГАРИЯ

[redacted]

ПЪЛНОМОЩНО

Долуподписаните **АЛЕКСАНДЪР ВАСИЛЕВ ДИМИТРОВ**, [redacted]

МЛАДЕН МАРКОСКИ, македонски гражданин, [redacted] Македония, притежател на паспорт [redacted] издаден на [redacted]. от властите на Македония,

в качеството си съответно на Главен изпълнителен директор и на Изпълнителен директор на "А1 България" ЕАД, със седалище и адрес на управление: гр. София, ул. "Кукуш" №1, ЕИК 131468980, ДДС № BG 131468980 („Дружеството"),

УПЪЛНОМОЩАВАМЕ:

СТАНИСЛАВА ДИМИТРОВА ШИЯКОВА, ЕГН: [redacted], издадена на [redacted], на длъжност Старши Продуктов Мениджър „Ценообразуване", отдел „Държавни структури", Направление „Корпоративни продажби" при „А1 България" ЕАД

със следните права:

1. Да представлява "А1 България" ЕАД при участия на дружеството в Процедури за възлагане на обществени поръчки, провеждани по реда на действащото законодателство, включително, но не само на: Закона за обществените поръчки (ЗОП), както и по реда на други действащи нормативни актове (в това число и подзаконови актове), като извършва всички необходими правни и фактически действия, включително, но без ограничение, да подава и получава документи по процедурите, да представя предложения (оферти), да заверява за вярност с оригинала, да подписва оферти, включително ценови оферти, и всякакви представяни във връзка с процедурите документи, да участва при отваряне и разглеждане на предложенията, да участва в преговори и др.

2. Упълномощеното лице има право да преупълномощава заедно или поотделно, трети лица - служители на „А1 България" ЕАД, с всички или с част от правата по настоящото пълномощно. Настоящото пълномощно се прекратява с оттеглянето му или при прекратяване на трудовия договор на упълномощения, което от двете събития настъпи по-рано.
Това пълномощно е изготвено на български и

POWER OF ATTORNEY

[redacted]

WE HEREBY EMPOWER:

[redacted]

with the following rights:

1. To represent A1 Bulgaria EAD in public procurement procedures carried out according to the operative legislation, including but not limited to the Public Procurement Law (PPL), as well as according to the active legislation (including secondary legislation), as to perform all necessary legal and factual activities related thereto, including but not limited to submitting and receiving of documents related to the procedures, to file proposals, certifying for authenticity the copies and signing offers, including price offers, and any other submitted documents related to the procedures, participating upon opening and supervising offers, participating in negotiations etc.

2. The authorised person shall be entitled to re-authorise jointly or separately third parties-employees of A1 Bulgaria EAD, with all or part of the rights granted herein.
The present power of attorney shall be terminated on case of the withdrawal there of or termination of the employment contract of the authorized, which event shall occur earlier.
This power [redacted]

ВЯРНО С ОРИГИНАЛА

[redacted]

Днес на ...17.02.........2020г., подписаната Мира Гасабова – пом.-нотариус по заместване при... - Нотариус с район на действие-района на Софийски районен съд, вписана в регистъра на нотариалната камара под № ....074............, на основание чл.582 от ГПК назначих за преводач лицето [redacted] с ЕГН [redacted], притежаваща л. к. № [redacted] София, и след като се уверих в липсата на пречки по чл. 584 от ГПК, го предупредих за отговорността по чл. 290 ал.2 от НК за неверен превод. Преводачът даде обещание да направи верен превод и за истинността за това, което потвърждава пред мен – нотариуса, съгласно чл. 585 ал.1 от ГПК във връзка с чл.170 от ГПК, след което текстът на документа се прочете на английски език от преводача [redacted] на **Младен Маркоски**, македонски гражданин [redacted] от властите на Македония, и след одобрението им се подписа от **Младен Маркоски**, и от преводача.

On this .... day of ....2020, I, the undersigned .... [redacted]

[redacted]

МЛАДЕН МАРКОСКИ / MLADEN MARKOSKI

[redacted]

ПРЕВОДАЧ / TRANSLATOR

[redacted]

ВЯРНО С ОРИГИНАЛА

A1 ЕАД

[redacted]

ПРИЛОЖЕНИЕ № 2.2

ДО
„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД
ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите"***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 2: „Доставка на софтуерно дефинирана мрежа за пренос на данни "***
Наименование на участника:	*А1 БЪЛГАРИЯ ЕАД*
Правно-организационна форма на участника:	*Еднолично Акционерно дружество* *(физическо или юридическо лице, обединение или друго образувание, което има право да изпълнява доставки съгласно законодателството на държавата, в която е установено)*
Седалище по регистрация и адрес на управление:	гр. София, Община „Илинден“, ж.к. „Захарна фабрика“, п.к.1309, ул. „Кукуш“ №1
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	ЕИК 131468980
Представляващ	МАРТИН ДИМИТРОВ ЙОРДАНОВ- Акаунт Мениджър “Държавни структури”- упълномощено лице *(законен представител или лице, специално упълномощено за участие в процедурата[1]*

[redacted]ъгласно чл. 41, ал. 5 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) когато документи, [redacted]рзани с участие в обществени поръчки се подават от лице, което представя участника по пълномощие, в Единния [redacted]опейски документ за обществени поръчки (ЕЕДОП) се посочва информация относно обхвата на [redacted]ата [redacted]власт.

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След запознаване с документацията за участие в обществената поръчка с горепосочения предмет, ние предоставяме следното техническо предложение по горецитираната обособена позиция, съдържащо:

I.ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛЕНИЕ НА ПОРЪЧКАТА

В качеството си на представляващ участника, декларирам, че сме запознати с условията на поръчката и с подаването на настоящото предложение удостоверявам следното:

1. Предмет на обществената поръчка:

1.1. Декларирам, че представляваният от мен участник ще изпълни поръчката, съобразявайки се с условията по изпълнение, посочени от възложителя в документацията за обществената поръчка.

1.2. Запознати сме, че съгласно чл. 39, ал. 1 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) с подаването на офертата по настоящата обществена поръчка се счита, че се съгласяваме с всички условия на възложителя, в т.ч. с определения срок за валидност на офертата и с проекта на договор, неразделна част от документацията за обществената поръчка.

1.3. Задължаваме се да извършим следните дейности:

1.3.1. доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция по приходите (наричано по-нататък за краткост „оборудването"), подробно описано по вид, количество и технически характеристики в Техническата спецификация, Приложение 1.2. към нея, относимо към настоящата обособена позиция, за която подаваме оферта и настоящето Техническо предложение.

1.3.2. гаранционно обслужване на доставеното по т. 1.3.1. оборудване (наричано по-нататък алтернативно „гаранция и поддръжка"), осигурено в рамките на срока по т. 5.2. в съответствие с предписанията на производителя, изискванията на договора за обществена поръчка и приложенията към него.

1.4. Подробно описание на вида, количеството и техническите характеристики на доставеното от нас оборудване, хардуер и софтуер, е описано, както следва:

1.4.1. Софтуерно дефиниран маршрутизатор тип 1 – 36 броя.

Изискано от Възложителя	Предложено от участника
А.	Б.
Обща информация	

REQ.1.	Захранване –в диапазона от минимум 100 до 240 VAC.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 притежава захранване в диапазона 100 до 240 VAC
REQ.2.	Работен температурен диапазон от 0° до +40 °С.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 има работен темп. диапазон от 0 до 40°С
REQ.3.	Безшумна работа – без вентилатори.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа безшумна работа без вентилатори.
REQ.4.	Минимум четири интерфейса 100/1000BASE-T.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 притежава 4 интерфейса 100/1000BASE-T
REQ.5.	Брой USB портове - минимум един, версия 3.0 или по-висока.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 притежава един USB порт версия 3.0
REQ.6.	Сериен конзолен порт - минимум един.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 притежава един RJ45 конзолен порт
REQ.7.	Минимум 4GB DRAM.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 притежава 4GB DRAM
REQ.8.	Минимум 4 GB Flash.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 притежава 8 GB Flash.
REQ.9.	Производителност от минимум 500Mbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 притежава производителност от 730Mbps throughput за IPSec SDWAN трафик с 1400 байта. Производителността на предлаганото устройство от А1 България ЕАД се удостоверява с декларация от производителя
REQ.10.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 участва в

		SDWAN мрежата под управление на SDWAN контролерите.
REQ.11.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа IPv4 и IPv6 WAN транспортни мрежи.
REQ.12.	Да поддържа изграждането на SDWAN overlay с използването на IPSec върху различни WAN мрежи – Internet и MPLS.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа изграждането на SDWAN overlay с използването на IPSec върху всякакви WAN мрежи, включително Internet и MPLS
REQ.13.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа AES-256 GCM алгоритъм за криптиране на трафика.
REQ.14.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа IPsec AH с използване на HMAC-SHA1 алгоритъм
REQ.15.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.16.	Да поддържа изграждане на GRE тунели до външни системи за сигурност.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа изграждане на GRE тунели до външни системи за сигурност.
REQ.17.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SDWAN контролерите.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа TLS и DTLS протоколи за изграждане на контролните връзки до SDWAN контролерите.

[redacted]

А1 България ЕАД [redacted]

REQ.18.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа 2048 bit RSA Authentification (удостоверяване на идентичността) между маршрутизаторите и контролерите с използване на цифрови сертификати.
REQ.19.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 има Trusted board iD чип (хардуерно решение за защита на сертификатите и ключовете с подобна функционалност), в който се съхранявва цифровият сертификат на маршрутизатора. Този сертификат включва публичния и частният ключове, както и серийният номер на сертификате.
REQ.20.	Да поддържа използване на сертификати от CA на възложителя.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа използването на сертификати, подписани от CA на възложителя.
REQ.21.	Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните
REQ.22.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS протокол за сегментация.
REQ.23.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа автоматично измерване на packet loss,

		jitter и delay за всеки SDWAN IPSec тунел.
REQ.24.	Да поддържа автоматично маршутизиране на ниво приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа автоматично маршрутизиране на ниво приложение през различни типове WAN връзки на база динамичните параметри на IPSec WAN тунелите packet loss, jitter и delay.
REQ.25.	Да има вграден zone firewall.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 има вграден zone firewall.
REQ.26.	Да има application firewall с вградено разпознаване на приложенията.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 има Application Firewall с вградена система, която разпознава над 1400 приложения на Layer7.
REQ.27.	Да поддържа филтриране на трафика чрез ACL.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа филтриране на трафика чрез ACL.
REQ.28.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play за автоматично откриване и свързване към SD-WAN контролерите.
REQ.29.	Да поддържа управляеми SDWAN IPSec топологии – hub-and-spoke, full mesh и комбинации между двете.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа работа в различни SDWAN IPSec топологии, като hub-and-spoke, full mesh и комбинация между двете.
REQ.30.	Да поддържа отделна, виртуална, топология за всеки сегмент.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа

		отделна, виртуална, логическа топология за всеки VPN (VRF) сегмент.
REQ.31.	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа следните протоколи за интеграция с външни мрежи: Static route, OSPF и BGP
REQ.32.	Да поддържа PIM.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа PIM.
REQ.33.	Да поддържа следните видове NAT услуги • статичен NAT • симетричен NAT • NAT64 • NAT pools • PAT	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа NAT услуги, вкл. Статичен NAT, симетричен NAT, NAT64, NAT pools, PAT
REQ.34.	Да поддържа изграждане на SD-WAN IPSec през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа изграждане на SDWAN IPSec през различни видове NAT на външно устройство (CPE, Internet Gateway и подобни), както и NAT Overlay- NAT на клиентският трафик преди вкарването му в SDWAN тунела.
REQ.35.	Да поддържа QoS: • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управление на задръстванията с RED и WRED алгоритми • Traffic policing • Traffic shaping	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа QoS: • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP алгоритъм • Управление на задръстванията с RED и WRED алгоритми • Traffic policing • Traffic shaping

REQ.36.	Да поддържа packet duplication – изпращане на един пакет по два или повече отделни SDWAN IPSec тунела до приемащия SD-WAN маршрутизатор.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа packet duplication – изпращане на един пакет по два или повече отделни SDWAN IPSec тунела до приемащия SD-WAN маршрутизатор.
REQ.37.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа автоматичен избор на най-добър маршрут през директна Internet връзка и през Internet връзката на централна локация до SaaS приложения, Microsoft Office 365 и AWS на база закъснение и загуба на пакети.
REQ.38.	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управелние на достъпа чрез RADIUS и TACACS+ системи.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 поддържа методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управелние на достъпа чрез RADIUS и TACACS+ системи.

REQ.39.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 е окомплектован с всички необходими лицензи и права за използване, съгласно изискванията на производителя Cisco Systems.
REQ.40.	Устройството да е окомплектовано с SDWAN лицензи за минимум 100Mbps WAN трафик.	Предложеното от А1 България ЕАД Cisco ISR1100-4GPM20 е предложен с SDWAN лицензен абонамент за 100Mbps WAN трафик, за срок от 5 години. Продуктов номер **E2N-SDWAN-C-T1-G-A** (Enterprise WAN Tier 1 Cloud (100M) DNA EA Advantage)
	Гаранция и поддръжка:	
REQ.41.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Cisco ISR1100-4GPM20 е предложен със сервизен пакет **CON-SNT-ISR1104G** (SNTC-8X5XNBD ISR1100 Series Router, 4 Eth LAN/WAN Por), който осигурява хардуерна гаранция за 5 години с предарителна подмяна по схема 8x5xNBD Ship.
REQ.42.	Срок на техническа поддръжка – минимум 5 (пет) години.	Cisco ISR1100-4GPM20 е предложен със сервизен пакет **CON-SNT-ISR1104G** (SNTC-8X5XNBD ISR1100 Series Router, 4 Eth LAN/WAN Por), който осигурява достъп до центъра за техническа поддръжка (Technical Assistance Center-TAC) на Cisco Systems за срок от 5 години.
[redacted]EQ.43.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Cisco ISR1100-4GPM20 е предложен със сервизен пакет **CON-SNT-ISR1104G** (SNTC-8X5XNBD ISR1100 Series Router, 4 Eth LAN/WAN Por), който осигурява

		достъп до всички софтуерни ъпдейти и ъпгрейди за продукта през Web сайта на производителя за срок от 5 години.
REQ.44.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години	Cisco ISR1100-4GPM20 е предложен с абонаментен лиценз **E2N-SDWAN-C-T1-G-A**, който дава право на възложителя да използва всички софтуерни функции на продукта, описани в техническите изисквания за него, за срок от 5 години.

1.4.2. Софтуерно дефиниран маршрутизатор тип 2 – 42 броя.

Изискано от Възложителя		Предложено от участника
А.		Б.
Обща информация		
REQ.45.	Захранване –в диапазона от минимум 100 до 240 VAC.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 притежава захранване работещо в диапазона 100 до 240 VAC
REQ.46.	Работен температурен диапазон от 0° до +40 °С	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 има работен темп. диапазон от 0 до 40°С
REQ.47.	Безшумна работа – без вентилатори.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа безшумна работа, без вентилатори.
REQ.48.	Минимум четири интерфейса 100/1000BASE-T и два интерфейса SFP.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 притежава 4 интерфейса 100/1000BASE-T и 2 интерфейса SFP
REQ.49.	Брой USB портове - минимум един, версия 3.0 или по-висока.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 притежава един USB порт версия 3.0

REQ.50.	Сериен конзолен порт - минимум един.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 притежава един RJ45 конзолен порт
REQ.51.	Минимум 4GB DRAM.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 притежава 4GB DRAM.
REQ.52.	Минимум 4 GB Flash.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 притежава 8 GB Flash.
REQ.53.	Производителност от минимум 1Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 притежава производителност от 1,8Gbps throughput за IPSec SDWAN трафик с 1400 байта. Производителността на предлаганото от А1 България ЕАД устройство се удостоверява с декларация от производителя.
REQ.54.	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 участва в SDWAN мрежата под управление на SDWAN контролерите.
REQ.55.	Да поддържа IPv4 и IPv6 WAN транспортни мрежи.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа IPv4 и IPv6 WAN транспортни мрежи.
REQ.56.	Да поддържа изграждането на SDWAN overlay с използването на IPSec.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа изграждането на SDWAN overlay с използването на IPSec.
REQ.57.	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа AES-256 GCM алгоритъм за криптиране на трафика.
REQ.58.	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа IPsec

		АН с използване на минимум HMAC-SHA1 алгоритъм .
REQ.59.	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.60.	Да поддържа изграждане на GRE тунели до външни системи за сигурност.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа GRE тунели до външни системи за сигурност.
REQ.61.	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа TLS и DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите.
REQ.62.	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа 2048 bit RSA Authentication (удостоверяване на идентичността) на Control Plane между маршрутизаторите и контролерите с използване на цифрови сертификати.
REQ.63.	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 има Trusted Board ID чип (хардуерно решение за защита на сертификатите и ключовете с подобна функционалност), в който е инсталиран цифровия сертификат на маршрутизатора. Този сертификат включва публичния и частният ключове, както и серийният номер на сертификата.
REQ.64.	Да поддържа използване на сертификати от СА на възложителя.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа използването на сертификат, подписан от СА на възложителя.

REQ.65.	Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.66.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS протокол за сегментация.
REQ.67.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.68.	Да поддържа автоматично маршутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа автоматично маршрутизиране на ниво приложение и групи от приложения през различни типове WAN връзки на база динамичните параметрите на IPSec WAN тунелите - packet loss, jitter и delay.
REQ.69.	Да има вграден zone firewall.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 има вграден zone firewall.
REQ.70.	Да има application firewall с вградено разпознаване на приложенията.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 има Application Firewall с вградена система, която разпознаван над 1400 приложения на Layer 7.
[redacted]EQ.71.	Да поддържа филтриране на трафика чрез ACL.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа филтриране на трафика чрез ACL.

[redacted]

REQ.72.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play за автоматично откриване и свързване към SD-WAN контролерите.
REQ.73.	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа работа в различни SDWAN IPSec топологии, като hub-and-spoke, full mesh и комбинация между двете.
REQ.74.	Да поддържа отделна, виртуална, топология за всеки сегмент	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа отделна, виртуална, логическа топология за всеки VPN (VRF) сегмент.
REQ.75.	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP • VRRP	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа следните протоколи за интеграция с външни мрежи: Static route, OSPF, BGP и VRRP.
REQ.76.	Да поддържа 802.1Q	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа 802.1Q
REQ.77.	Да поддържа обединяване на интерфейси в bridge групи	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа обединяване на интерфейси в bridge групи.
REQ.78.	Да поддържа IGMP v1 и v2	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа IGMP v1 и v2.
REQ.79.	Да поддържа PIM	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа PIM

София
КП2

REQ.80.	Да поддържа следните видове NAT услуги • статичен NAT • динамичен NAT • NAT64 • NAT pools • PAT	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа NAT услуги, вкл. Статичен NAT, динамичен NAT, NAT64, NAT pools, PAT.
REQ.81.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа изгражане на SD-WAN IPSec през различни видове NAT на външно устройство (CPE, Internet Gateway и подобни), както и NAT Overlay – NAT на клиентския трафик преди вкарването му в SDWAN тунела.
REQ.82.	Да поддържа QoS: • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управелние на задрсътванията с RED и WRED алгоритми • Traffic policing • Traffic shaping	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа QoS: • CoS маркиране • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP алгоритъм • Управелние на задрсътванията с RED и WRED алгоритми • Traffic policing • Traffic shaping
REQ.83.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор.
REQ.84.	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа автоматичен избор на най-добър маршрут през директна Internet връзка и през Internet връзката на централна

	през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS	локация до SaaS приложения, включително Microsoft Office 365 и AWS на база закъснение и загуба на пакети.
REQ.85.	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 поддържа методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • Split DNS • DDOS защита • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.86.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;	Предложеният от А1 България ЕАД Cisco ISR1100-6GPM20 е окомплектован с всички необходими лицензи и права за използване, съгласно изискванията на производителя Cisco Systems
REQ.87.	Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик.	Cisco ISR1100-6GPM20 е предложен с SDWAN лицензен абонамент за 1Gbps WAN трафик, за срок от 5 години. Продуктов номер **E2N-SDWAN-C-T2-G-A** (Enterprise WAN Tier 2 Cloud (1G) DNA EA Advantage).

[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

	Гаранция и поддръжка:	
REQ.88.	Срок на хардуерната гаранция - минимум 5 (пет) години.	Cisco ISR1100-6GPM20 е предложен със сервизен пакет **CON-SNT-GSR11060** (SNTC-8X5XNBD ISR1100 Router, 4 GE LAN/WAN Ports and 2), който осигурява хардуерна гаранция за 5 години с предарителна подмяна по схема 8x5xNBD Ship.
REQ.89.	Срок на техническа поддръжка – минимум 5 (пет) години.	Cisco ISR1100-6GPM20 е предложен със сервизен пакет **CON-SNT-GSR11060** (SNTC-8X5XNBD ISR1100 Router, 4 GE LAN/WAN Ports and 2), който осигурява достъп до центъра за техническа поддръжка (Technical Assistance Center-TAC) на Cisco Systems за срок от 5 години.
REQ.90.	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Cisco ISR1100-6GPM20 е предложен със сервизен пакет **CON-SNT-GSR11060** (SNTC-8X5XNBD ISR1100 Router, 4 GE LAN/WAN Ports and 2), който осигурява достъп до всички софтуерни ъпдейти и ъпгрейди за продукта през Web сайта на производителя за срок от 5 години.
REQ.91.	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години.	Cisco ISR1100-6GPM20 е предложен с абонаментен лиценз **E2N-SDWAN-C-T2-G-A** , който дава право на възложителя да използва всички софтуерни функции на продукта, описани в техническите изисквания за него, за срок от 5 години.

1.4.3.Софтуерно дефиниран маршрутизатор тип 3 – 36 броя.

Изискано от Възложителя	Предложено от участника
А.	**Б.**
Обща информация	

REQ.92.	Захранване –в диапазона от минимум 100 до 240 VAC.	Предложеният от А1 България ЕАД Cisco ISR 4451 притежава захранване в диапазона 100 до 240 VAC
REQ.93.	Работен температурен диапазон от 0º до +40 ºC	Предложеният от А1 България ЕАД Cisco ISR 4451 има работен темп. диапазон от 0 до 40°C
REQ.94.	Шаси за монтаж в 19" шкаф	Предложеният от А1 България ЕАД Cisco ISR 4451 е изпълнен от производителя в шаси за монтаж в 19" шкаф.
REQ.95.	Два токозахранващи модула	Предложеният от А1 България ЕАД Cisco ISR 4451 има два токозахранващи модула.
REQ.96.	Минимум четири интерфейса, които поддържат 100/1000BASE-T и SFP	Предложеният от А1 България ЕАД Cisco ISR 4451 има четири интефейса, поддържащи 100/1000BASE-T и SFP. Като има възможност за добавяне на допълнителна карта с портове.
REQ.97.	Брой USB портове - минимум 1,	Предложеният от А1 България ЕАД Cisco ISR 4451 притежава USB порт версия 3.0
REQ.98.	Конзолен порт - 1	Предложеният от А1 България ЕАД Cisco ISR 4451 притежава RJ45 конзолен порт
REQ.99.	Минимум 8GB DRAM	Предложеният от А1 България ЕАД Cisco ISR 4451 притежава 8GB DRAM
REQ.100.	Възможност за добавяне на модул с LTE cat. 6 модем	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа LTE cat. 6 модем.
REQ.101.	Възможност за добавяне на минимум осем 1000Base-T порта	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа възможност за добавяне на допълнителни осем порта 1000Base-T.

[redacted] [redacted] [redacted] [redacted] [redacted]

REQ.102	Производителност от минимум 3Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя	Предложеният от А1 България ЕАД Cisco ISR 4451притежава производителност от 3,6Gbps throughput за IPSec SDWAN за 1400 байтови пакети. Производителността на предлаганото устройство от А1 България ЕАД се удостоверява с декларация от производителя.
REQ.103	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание	Предложеният от А1 България ЕАД Cisco ISR 4451 участва в SDWAN мрежата под управление на SDWAN контролерите.
REQ.104	Да поддържа IPv4 и IPv6 WAN транспортни мрежи	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа IPv4 и IPv6 WAN транспортни мрежи.
REQ.105	Да поддържа изграждането на SDWAN overlay с използването на IPSec	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа изграждането на SDWAN overlay с използването на IPSec върху всякакви WAN мрежи
REQ.106	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа AES-256 GCM алгоритъм за криптиране на трафика.
REQ.107	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа IPsec AH с използване на HMAC-SHA1 алгоритъм.
REQ.108	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys	Предложеният от А1 България ЕАД Cisco ISR 4451 използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.109	Да поддържа изграждане на GRE тунели до външни системи за сигурност	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа изграждане на GRE тунели до външни системи за сигурност.

REQ.110	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите.
REQ.111	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа 2048 bit RSA Authentication (удостоверяване на идентичността) на Control Plane между маршрутизаторите и контролерите с използване на цифрови сертификати.
REQ.112	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност	Предложеният от А1 България ЕАД Cisco ISR 4451 има Trusted Board ID чип (хардуерно решение за защита на сертификатите и ключовете), в който е инсталиран цифровия сертификат на машрутизатора. Този сертификат включва публичния и частния ключове, както и серийния номер на сертификата.
REQ.113	Да поддържа използване на сертификати от СА на възложителя	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа използването на сертификат, подписан от СА на възложителя.
REQ.114	Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.115	Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS протокол за сегментация

REQ.116.	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа сегментриране на трафика при SDWAN преноса чрез VRF, MPLS протокол за сегментация.
REQ.117.	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.118.	Да поддържа автоматично маршутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа автоматично маршрутизиране на ниво приложения и групи от приложения през различни типове WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay.
REQ.119.	Да има вграден zone firewall	Предложеният от А1 България ЕАД Cisco ISR 4451 има вграден zone firewall.
REQ.120.	Да има application firewall с вградено разпознаване на приложенията	Предложеният от А1 България ЕАД Cisco ISR 4451 има Application Firewall с вградена система, която разпознаван над 1400 приложения на Layer 7
REQ.121.	Да поддържа филтриране на трафика чрез ACL	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа филтриране на трафика чрез ACL.
REQ.122.	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play за автоматично откриване и свързване към SD-WAN контролерите .
REQ.123.	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа работа в различни SDWAN IPSec топологии, като

		hub-and-spoke, full mesh и комбинация между двете.
REQ.124.	Да поддържа отделна, виртуална, топология за всеки сегмент	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа отделна, виртуална, логическа топология за всеки VPN (VRF) сегмент.
REQ.125.	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP • VRRP	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа следните протоколи за интеграция с външни мрежи: Static route, OSPF, BGP и VRRP
REQ.126.	Да поддържа 802.1Q	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа 802.1Q
REQ.127.	Да поддържа IGMP v2 и v3	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа IGMP v2 и v3
REQ.128.	Да поддържа минимум PIM SSM	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа PIM SSM
REQ.129.	Да поддържа PIM rendezvous point	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа PIM rendezvous point (RP)
REQ.130.	Да поддържа статичен и динамичен NAT и NAT pool	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа статичен NAT, вкл. динамичен NAT и NAT pool
REQ.131.	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа изгражане на SD-WAN през различни видове NAT на външно устройство (CPE, Internet Gateway и подобни), както и NAT Overlay – NAT на клиентския трафик преди вкарването му в SDWAN тунела.
REQ.132.	Да поддържа QoS: • Минимум 8 пакетни опашки на интерфейс	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа QoS:

	• LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управелние на задрсъванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропусквателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики	• Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP • Управелние на задрсъванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропусквателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики
REQ.133.	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор , с технологията Packet Duplication for Noisy Channels.
REQ.134.	Да има вграден IPS	Предложеният от А1 България ЕАД Cisco ISR 4451 има вграден IPS
REQ.135.	Да има вградена Anti Malware защита	Предложеният от А1 България ЕАД Cisco ISR 4451 има вградена Anti Malware защита
REQ.136.	Да има URL филтриране по категории	Предложеният от А1 България ЕАД Cisco ISR 4451 има URL филтриране по категории

A1
КП2

REQ.137	Да осигурява декриптиране на SSL и TLS за инспектиране на криптиран трафик	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа декриптиране на SSL и TLS за инспектиране на криптиран трафика
REQ.138	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа автоматичен избор на най-добър маршрут през директна Internet връзка и през Internet връзката на централна локация до SaaS приложения, включително Microsoft Office 365 и AWS на база закъснение и загуба на пакети.
REQ.139	Да поддържа висока надеждност чрез съвместна работа с второ устройство от същия тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа висока надеждност чрез работа с второ устройство от същият тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели.
REQ.140	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора	Предложеният от А1 България ЕАД Cisco ISR 4451 поддържа методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора

ЕАД

	• Автоматично откриване на MTU, на WAN транспортните мрежи • Управелние на достъпа чрез RADIUS и TACACS+ системи.	• Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи.
REQ.141	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;	Cisco ISR 4451 е окомплектован с всички необходими лицензи и права за използване, съгласно изискванията на производителя Cisco Systems
REQ.142	Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик	Cisco ISR 4451 е предложен с SDWAN лицензен абонамент за 1Gbps WAN трафик, за срок от 5 години. Продуктов номер **E2N-SDWAN-C-T2-G-A** (Enterprise WAN Tier 2 Cloud (1G) DNA EA Advantage).
	Гаранция и поддръжка:	
REQ.143	Срок на хардуерната гаранция - минимум 5 (пет) години.	Cisco ISR 4451 е предложен със сервизен пакет **CON-SNT-ISR445D1** (SNTC-8X5XNBD Cisco ISR 4451 (4 GE, 3 NIM, 2 SM) with), който осигурява хардуерна гаранция за 5г с предарителна подмяна по схема 8x5xNBD Ship.
REQ.144	Срок на техническа поддръжка – минимум 5 (пет) години.	Cisco ISR 4451 е предложен със сервизен пакет **CON-SNT-ISR445D1** (SNTC-8X5XNBD Cisco ISR 4451 (4 GE, 3 NIM, 2 SM) with), който осигурява достъп до центъра за техническа поддръжка (Technical Assistance Center- TAC) на Cisco Systems за срок от 5 години.
REQ.145	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Cisco ISR 4451 е предложен със сервизен пакет **CON-SNT-ISR445D1** (SNTC-8X5XNBD Cisco ISR 4451 (4 GE, 3 NIM, 2 SM) with), който осигурява достъп до всички софтуерни ъпдейти и ъпгрейди

		за продукта през Web сайта на производителя за срок от 5 години.
REQ.146	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години	Cisco ISR 4451 е предложен с абонаментен лиценз **E2N-SDWAN-C-T2-G-A**, който дава право на възложителя да използва всички софтуерни функции на продукта, описани в техническите изисквания за него, за срок от 5 години.

1.4.4.Софтуерно дефиниран маршрутизатор тип 4 – 2 броя.

Изискано от Възложителя		Предложено от участника
А.		Б.
Обща информация		
REQ.147	Захранване –в диапазона от минимум 100 до 240 VAC	Предложеният от А1 България ЕАД Cisco ASR 1001-X притежава захранване в диапазона 100 до 240 VAC
REQ.148	Работен температурен диапазон от 0° до +40 °C	Предложеният от А1 България ЕАД Cisco ASR 1001-X работен темп. диапазон от 0 до 40°C
REQ.149	Шаси за монтаж в 19“ шкаф	Предложеният от А1 България ЕАД Cisco ASR 1001-X е изпълнен от производителя в шаси за монтаж в 19“ шкаф.
REQ.150	Два токозахранващи модула	Предложеният от А1 България ЕАД Cisco ASR 1001-X има два токозахранващи модула.
REQ.151	Минимум шест 1000BaseT и два SFP+ порта.	Предложеният от А1 България ЕАД Cisco ASR 1001-X притежава шест интефейса 100/1000BASE-T и два SFP+ порта.
REQ.152	Устройството да бъде доставено с четири 10GBASE-SR SFP+ модула	Предложеният от А1 България ЕАД Cisco ASR 1001-X ще бъде доставено с четири 10GBASE-SR SFP+ модула.

ЕАД

REQ.153	Брой USB портове - минимум 1,	Предложеният от А1 България ЕАД Cisco ASR 1001-X притежава USB порт версия 3.0
REQ.154	Сериен конзолен порт - минимум 1	Предложеният от А1 България ЕАД Cisco ASR 1001-X притежава RJ45 конзолен порт.
REQ.155	Минимум 8GB DRAM	Предложеният от А1 България ЕАД Cisco ASR 1001-X притежава 8GB DRAM.
REQ.156	Производителност от минимум 6Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройство трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя	Предложеният от А1 България ЕАД Cisco ASR 1001-X притежава производителност от 7,8Gbps throughput за IPSec SDWAN трафик с 1400 байтови пакети. Производителността на предлаганото устройство от А1 България ЕАД се удостоверява с декларация от производителя.
REQ.157	Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание	Предложеният от А1 България ЕАД Cisco ASR 1001-X участва в SDWAN мрежата под управление на SDWAN контролерите.
REQ.158	Да поддържа IPv4 и IPv6 WAN транспортни мрежи	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа IPv4 и IPv6 WAN транспортни мрежи.
REQ.159	Да поддържа изграждането на SDWAN overlay с използването на IPSec	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа изграждането на SDWAN overlay с използването на IPSec върху всякакви WAN мрежи
REQ.160	Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа AES-256 GCM алгоритъм за криптиране на трафика.

REQ.161	Да поддържа IPsec AH с използване на минимум HMAC-SHA1 алгоритъм	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа IPsec AH с използване на HMAC-SHA1 алгоритъм.
REQ.162	Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys	Предложеният от А1 България ЕАД Cisco ASR 1001-X използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys
REQ.163	Да поддържа изграждане на GRE тунели до външни системи за сигурност	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа изграждане на GRE тунели до външни системи за сигурност.
REQ.164	Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите.
REQ.165	Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа 2048 bit RSA Authentication (удостоверяване на идентичността) на Conrol Plane между маршрутизаторите и контролерите с използване на цифрови сертификати.
REQ.166	Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност	Предложеният от А1 България ЕАД Cisco ASR 1001-X има Trusted Board ID чип(хардуерно решение за защита на сертификатите и ключовете), в който е инсталиран цифровия сертификат на машрутизатора. Този сертификат включва публичния и частния ключове, както и серийния номер на сертификата.
REQ.167	Да поддържа използване на сертификати от СА на възложителя	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа използването на сертификат, подписан от СА на възложителя.

REQ.168	Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа AES-256 GCM алгоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните.
REQ.169	Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS протокол за сегментация
REQ.170	Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация.	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа сегментриране на трафика при SDWAN преноса чрез VRF, MPLS протокол за сегментация.
REQ.171	Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел.
REQ.172	Да поддържа автоматично маршутизиране на приложения и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа автоматично маршрутизиране на ниво приложение и групи от приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay
REQ.173	Да има вграден zone firewall	Предложеният от А1 България ЕАД Cisco ASR 1001-X има вграден zone firewall.
REQ.174	Да има application firewall с вградено разпознаване на приложенията	Предложеният от А1 България ЕАД Cisco ASR 1001-X Application Firewall с вградена система, която разпознаван над 1400 приложения на Layer 7

REQ.175	Да поддържа филтриране на трафика чрез ACL	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа филтриране на трафика чрез ACL.
REQ.176	Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play за автоматично откриване и свързване към SD-WAN контролерите .
REQ.177	Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа работа в в различни SDWAN IPSec топологии, като hub-and-spoke, full mesh и комбинация между двете.
REQ.178	Да поддържа отделна, виртуална, топология за всеки сегмент	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа отделна, виртуална, логическа топология за всеки VPN (VRF) сегмент.
REQ.179	Да поддържа следните протоколи за интеграция с външни мрежи: • Static route • OSPF • BGP • VRRP	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа следните протоколи за интеграция с външни мрежи: Static route, OSPF, BGP и VRRP
REQ.180	Да поддържа 802.1Q	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа 802.1Q
REQ.181	Да поддържа IGMP v2 и v3	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа IGMP v2 и v3
REQ.182	Да поддържа минимум PIM SSM	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа PIM SSM
REQ.183	Да поддържа PIM rendezvous point	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа PIM rendezvous point (RP)

REQ.184	Да поддържа статичен и динамичен NAT и NAT pool	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа статичен NAT, вкл. динамичен NAT и NAT pool
REQ.185	Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа изграждане на SDWAN през различни видове NAT на външно устройство (CPE, Internet Gateway и подобни), както и NAT Overlay – NAT на клиентския трафик преди вкарването му в SDWAN тунела.
REQ.186	Да поддържа QoS: • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP или подобен алгоритъм • Управление на задрсътванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропускателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа QoS: • Минимум 8 пакетни опашки на интерфейс • LLQ опашка • Управление на пакетните опашки с WRP алгоритъм • Управление на задръстванията с RED и WRED алгоритми • Traffic policing • Traffic shaping • Автоматичен traffic shaping за всеки VPN тунел съобразно пропускателната способност на WAN връзката, на отдалечения SD-WAN рутер • QoS върху VLAN интерфейси • Премаркиране на DCSP полето на база политики
REQ.187	Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа packet duplication – изпращане на един пакет по

		два отделни маршрута до приемащия SD-WAN маршрутизатор, с технологията Packet Duplication for Noisy Channels.
REQ.188	Да поддържа автоматичен избор на най-добрия маршрут до SaaS приложения чрез измерване на закъснението и загубата на пакети до SaaS приложенията през директна Internet връзка и през Internet връзката на централна локация. Да поддържа минимум Microsoft Office 365 и AWS	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа автоматичен избор на най-добър маршрут през директна Internet връзка и през Internet връзката на централна локация до SaaS приложения, включително Microsoft Office 365 и AWS на база закъснение и загуба на пакети
REQ.189	Да поддържа висока надеждност чрез съвместна работа с второ устройство от същия тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа висока надеждност чрез работа с второ устройство от същият тип и използване на неговите WAN транспортни интерфейси за изграждане на IPSec SDWAN транспортни тунели.
REQ.190	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow или подобен протокол към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора • Автоматично откриване на MTU, на WAN транспортните мрежи • Управелние на достъпа чрез RADIUS и TACACS+ системи.	Предложеният от А1 България ЕАД Cisco ASR 1001-X поддържа методи за управление и наблюдение: • Управление чрез SD-WAN контролерите в това задание • DHCP клиент • DHCP сървър • DHCP Relay • DNS • NTP • SNMP • SSH • Експортиране на трафична информация чрез IPFIX, JFlow, NetFlow към външна система за анализ на трафика • Traffic policing за контролиране на трафика до контролната система на маршрутизатора

А1 България ЕАД

		• Автоматично откриване на MTU, на WAN транспортните мрежи • Управление на достъпа чрез RADIUS и TACACS+ системи
REQ.191	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя;	Cisco ASR 1001-X е окомплектован с всички необходими лицензи и права за използване, съгласно изискванията на производителя Cisco Systems
REQ.192	Устройството да е окомплектовано с SDWAN лицензи за минимум 5Gbps WAN трафик	Cisco ASR 1001-X е предложен с SDWAN лицензен абонамент за 5Gbps WAN трафик, за срок от 5 години. Продуктов номер **E2N-SDWAN-C-T3-G-A** (Enterprise WAN Tier 3 Cloud (10G) DNA EA Advantage).
Гаранция и поддръжка:		
REQ.193	Срок на хардуерната гаранция - минимум 5 (пет) години.	Cisco ASR 1001-X е предложен със сервизен пакет **CON-SNT-ASR1001A** (SNTC-8X5XNBD Cisco ASR 1001-X Crypto,6GE, Dual-PS wit) и **CON-SNT-FLSABGEX** (SNTC-8X5XNBD ASR1001-X Built-In 10GE 1-port License), който осигурява хардуерна гаранция за 5г с предарителна подмяна по схема 8x5xNBD Ship.
REQ.194	Срок на техническа поддръжка – минимум 5 (пет) години.	Cisco ASR 1001-X Cisco ASR 1001-X е предложен със сервизен пакет **CON-SNT-ASR1001A** (SNTC-8X5XNBD Cisco ASR 1001-X Crypto,6GE, Dual-PS wit) и **CON-SNT-FLSABGEX** (SNTC-8X5XNBD ASR1001-X Built-In 10GE 1-port License), който осигурява достъп до центъра за техническа поддръжка (Technical Assistance Center- TAC) на Cisco Systems за срок от 5 години.

REQ.195	Получаване на нови версии на софтуера - минимум 5 (пет) години.	Cisco ASR 1001-X е предложен със сервизен пакет **CON-SNT-ASR1001A** (SNTC-8X5XNBD Cisco ASR 1001-X Crypto,6GE, Dual-PS wit) и **CON-SNT-FLSABGEX** (SNTC-8X5XNBD ASR1001-X Built-In 10GE 1-port License), който осигурява достъп до всички софтуерни ъпдейти и ъпгрейди за продукта през Web сайта на производителя за срок от 5 години.
REQ.196	Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години.	Cisco ASR 1001-X е предложен с абонаментен лицензен **E2N-SDWAN-C-T3-G-A**, който дава право на възложителя да използва всички софтуерни функции на продукта, описани в техническите изисквания за него, за срок от 5 години.

1.4.5.Софтуер за управление на софтуерно дефинирана мрежа

Изискано от Възложителя		Предложено от участника
А.		Б.
Обща информация		
REQ.197	Софтуерни контролери за изграждане и управление на SDWAN мрежа с SDWAN маршрутизаторите в това задание.	Предложените от А1 България ЕАД Cisco vSmart софтуерни контролери за изграждане и vManage за управление на SDWAN мрежа с SDWAN маршрутизаторите в това задание.
REQ.198	Инсталация – върху VMWare ESXi на възложителя	Предложените от А1 България ЕАД Cisco софтуерни контролери са за инсталация върху VMWare ESXi на възложителя.
REQ.199	Количество – съгласно изискванията на производителя за постигане на висока	Предложените от А1 България ЕАД Cisco vSmart софтуерни контролери 2 броя, софтуерен мениджмънт vManage 1

	надеждност и резервиране на SDWAN контролната система	брой, софтуерен оркестратор vBond 1 брой, за постигане на висока надеждност и резервиране на SDWAN контролната система
REQ.200.	Автоматично присъединяване и провизиране на маршрутизаторите в SDWAN средата чрез използване на компонент за оркестриране, който осигурява plug-and-play, zero touch plug&play и подобни решения за автоматизация.	Предложените от А1 България ЕАД Cisco маршрутизатори поддържат автоматично присъединяване и провизиране в SDWAN средата чрез използването на компомент за оркестриране, vBond който осигурява plug-and-play, zero touch plug&play решения за автоматизация.
REQ.201.	Управление на маршрутизаторите и техните функции в SDWAN мрежата чрез темплейти	Управлението на маршрутизаторите предложени от А1 България ЕАД и техните функции в SDWAN мрежата се управляват чрез темплейти, което се извършва в Cisco vManage.
REQ.202.	Управление на услугите и виртуалните топологии в SDWAN мрежата чрез политики	Предложеното от А1 България ЕАД Cisco SDWAN решение управлява услугите и виртуалните топологии в SDWAN мрежата чрез политики в Cisco vManage
REQ.203.	Управление на транспортната IPSec топология чрез политики	Предложеното от А1 България ЕАД Cisco SDWAN решение управлява транспортната IPSec топология чрез политики в Cisco vManage.
REQ.204.	Динамично управление на различни трафични класове през IPSec транспортната инфраструктура на база параметрите на тунелите – jitter, latency, загуба на пакети	Предложеното от А1 България ЕАД Cisco SDWAN решение поддържа динамично управление на различни трафични класове през IPSec транспортната инфраструктура на база параметрите на тунелите – jitter, latency, загуба на пакети

[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

REQ.205	Управление на IPS, application Firewall, URL Filter и Malware защитата в SDWAN машршрутизаторите с такива функции.	Предложеното от А1 България ЕАД Cisco SDWAN решение поддържа управление на IPS, application Firewall, URL Filter и Malware защитата в SDWAN машрушрутизаторите с такива функции чрез предложеният от А1 България ЕАД Cisco софтуерен контролер vManage.
REQ.206	Наблюдение на SDWAN маршрутизаторите	Предложеното от А1 България ЕАД решение има наблюдение на SDWAN маршрутизаторите чрез Cisco vManage
REQ.207	Наблюдение на SDWAN IPSec транспортните тунели и техните параметри – минимум up/down, packet loss, jitter и delay	Предложеното от А1 България ЕАД LiveAction LiveNX решение има наблюдение на SDWAN IPSec транспортните тунели и техните параметри – минимум up/down, packet loss, jitter и delay
REQ.208	Наблюдение на трафичните параметри от различни класове приложения, които използват SD-WAN мрежата	Предложеното от А1 България ЕАД LiveAction LiveNX предлага наблюдение на трафичните параметри от различни класове приложения, които използват SD-WAN мрежата.
REQ.209	Визуализация на маршрутите за различните класове трафик през SDWAN мрежата	Предложеното от А1 България ЕАД LiveAction LiveNX предлага визуализация на маршрутите на различните класове трафик през SDWAN мрежата.
REQ.210	Изграждане на карта с топологията на SD-WAN мрежата с овърлей върху географска карта на страната.	Предложеното от А1 България ЕАД LiveAction LiveNX предлага изграждане на карта с топологията на SDWAN мрежата с овърлей върху географска карта на страната.
REQ.211	Визуализация на пътя на трафичните потоци, на ниво приложения, върху транспортните тунели.	Предложеното от А1 България ЕАД LiveAction LiveNX предлага визуализация на пътя на трафичните потоци, на ниво

		приложения, върху транспортните тунели.
REQ.212	Преодставяне на информация за QoS на трафичните потоци от приложенията	Предложеното от А1 България ЕАД LiveAction LiveNX предлага предоставяне на информация за QoS на трафичните потоци от приложенията
REQ.213	Исторически справки за трафичните потоци през SDWAN мрежата	Предложеното от А1 България ЕАД LiveAction LiveNX предлага исторически справки за трафичните потоци през SDWAN мрежата.
REQ.214	Web GUI интерфейс	Предложеното от А1 България ЕАД Cisco SDWAN софтуерен контролер има Web GUI интерфейс.
REQ.215	Role based access controll	Предложеното от А1 България ЕАД Cisco SDWAN софтуерен контролер има Role based access controll
REQ.216	Да поддържа SSO съвместимо с Microsoft ADFS	Предложеното от А1 България ЕАД Cisco SDWAN софтуерен контролер поддържа SSO съвместимо с Microsoft ADFS.
REQ.217	Да има REST API за интеграция с външни софтуерни системи	Предложеното от А1 България ЕАД Cisco SDWAN софтуерен контролер има REST API за интеграция с външни софтуерни системи.
	Гаранция и поддръжка:	
REQ.218	Срок на хардуерната гаранция - минимум 5 (пет) години.	Предложението от А1 България ЕАД включва следните софтуерни решения: vManage, vBond, vSmart, които са включените в лицензите на предложените Cisco маршрутизатори ISR1104, ISR1106, ISR4451, ASR1001-x за 5 години и не изискват допълнителен сервизен пакет. А1 България ЕАД предлага софтуерна и хардуерна

ЕАД

		гаранция за срок от 5 години. След получаването на гореспоменатите лицензи за маршрутизатори, изброените софтуерни решения са свободни за сваляне и инсталиране върху VMware среда на ВЪЗЛОЖИТЕЛЯ. Предложеният от А1 България ЕАД софтуер за визуализация на трафичните потоци LiveNX е със сервизен пакет за 125 устройства за 5 години- 5 броя M-SP-LA-E-25-K9 LiveNX Ent Annual Maint., 25 devices, unlimited history) и 10 броя M-SP-LA-E-50-K9 (LiveNX Ent Annual Maint., 50 devices, unlimited history)
REQ.219	Срок на техническа поддръжка – минимум 5 (пет) години.	Предложението от А1 България ЕАД включва 5 години техническа поддръжка
REQ.220	Получаване на нови версии на софтуера – минимум 5 (пет) години.	Предложението от А1 България ЕАД включва предоставянето на нови версии на софтуера за 5 (пет) години.
REQ.221	Срок . на абонаментите за използване на софтуерни функции - минимум 5 (пет) години.	Предложението от А1 България ЕАД е включен 5 годишен абонаментите за използване на софтуерни функции.

1.4.6.Съвместимост на компоненти

Изискано от Възложителя		Предложено от участника
А.		Б.
Обща информация		
REQ.222	За постигането на пълна съвместимост и улеснена експлоатация на SDWAN мрежата, предлаганите SDWAN рутери, SFP+ модули и софтуерни компоненти за сигурност трябва да са от един производител.	За постигането на пълна съвместимост и улеснена експлоатация на SDWAN мрежата, предоставените от А1 България ЕАД SDWAN рутери, SFP+ модули и софтуерни компоненти за сигурност са от един производител Cisco Systems.

Забележка: а) *Навсякъде в техническата спецификация, където се съдържа посочване на конкретен модел, източник, процес, търговска марка, патент, тип, произход, стандарт или производство да се чете и разбира „или ЕКВИВАЛЕНТ". Участникът следва да докаже, че предлаганите решения удовлетворяват по еквивалентен начин изискванията, определени от техническата спецификация.*

б) *Оборудването, предмет на доставката, се състои от хардуер и софтуер, които трябва да съответстват или да надвишават в техническо отношение посочените минимални изисквания в Техническата спецификация и приложението към нея, относимо към настоящата обособена позиция.*

2. Изисквания към изпълнението на поръчката:

2.1. Декларираме, че оборудването, предмет на доставката, ще бъде фабрично нов, неупотребяван, включен е в актуалните продуктови листи на производителя, ще продължава да бъде включен към датата на сключване на договора за възлагане на обществената поръчка и не е спрян от производство.

2.2. Хардуерните компоненти на оборудването ще отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.

2.3. Оборудването ще бъде доставено в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, в случай, че са различни от стандартни IEC C14 - IEC C13 или IEC C20 - IEC C19. Необходимата техническа документация, като потребителски, инсталационни, конфигурационни и др. ръководства ще се представят на електронен носител за всеки тип от предлаганите устройства.

2.4. При доставката на софтуер ще бъдат предоставени необходимите сертификати или други документи, удостоверяващи предоставеното право на ползване на софтуера.

3. Условия на доставка

3.1. Запознати сме, че доставката на оборудването (хардуер и софтуер) ще се извършва въз основа на писмена заявка, отправена чрез адреса за кореспонденция на хартиен носител или по електронна поща, подписана с електронен подпис, създаден с квалифицирано удостоверение за електронен подпис на възложителя или упълномощен негов представител, съгласно клаузите на договора за обществена поръчка.

3.2. Приемането и предаването на изпълнението ще се осъществява въз основа на изискванията на договора за обществена поръчка.

4. Условия на гаранционно обслужване

4.1. Гарантираме за срока, посочен в т. 5.2., пълната функционална годност на доставеното оборудване съгласно предписанията на производителя, изискванията на договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение и приложенията към него.

4.2. В рамките на срока по посочен в т. 5.2. се задължаваме да отстраняваме за наша сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя, изискванията на договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение и приложенията към него. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.

4.3. Редът за отстраняване на констатиран дефект и/или несъответствие в срока на гаранционно обслужване е описан в договора за обществена поръчка по обособената позиция, за която предоставяме настоящето Техническо предложение.

5. Срок на изпълнение

5.1. Задължаваме се да извършим доставка на оборудването в срок до 78 календарни дни, считано от датата на получаване на писмена заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.

Забележка: *Участникът следва да предложи в офертата си срок за извършване на доставката, който не може да бъде по-дълъг от 80 календарни дни, считано от получаване на писмената заявка по чл. 1, ал. 2 от проекта на договор за обществена поръчка.*

5.2. Срокът на гаранционно обслужване е 5 години, считано от датата на приемо-предавателния протокол за доставка на оборудването.

Забележка: *Участникът следва да предложи в офертата си срок за гаранционно обслужване, който следва да бъде минимум 5 (пет) години, считано от датата на подписване на двустранен приемо-предавателен протокол за приемане на доставката.*

6. Място на изпълнение

6.1. Потвърждаваме, че мястото на извършване на доставката е на територията на гр. София,

А1 България ЕАД

като сме запознати, че ще бъде посочено в писмената заявка конкретния адрес на извършване на доставката.

6.2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталирано оборудване.

7. Други изисквания

7.1. Декларираме, че сме производител на оборудването/сме надлежно упълномощени да извършваме доставка и гаранционно обслужване на предлаганото от нас комуникационно оборудване, хардуер и софтуер, на територията на Република България.

За удостоверяване на горното представяме Оторизационно писмо от производителя

(моля, посочете описание на документа)

Забележка:

За удостоверяване на горното участникът следва да представи Официално оторизационно писмо (или еквивалентен документ) с актуална дата от производителя или от официален представител на производителя на предлаганото оборудване. Горепосоченият документ се представя в техническото предложение на участника.

В случаите на представяне от участника на оторизационно писмо (или еквивалентен документ) от официален представител на производителя, в офертата се прилага и оторизационно писмо, издадено от производителя (или еквивалентен документ), с което се упълномощава официалния представител на производителя за доставка и гаранционно обслужване на предлаганото оборудване.

7.2. Прилагаме общи условия или други приложими условия за гаранционно обслужване от производителя на продуктите, предмет на обществената поръчка (в случай, че е приложимо).

Дата на подписване:	**13/ 07/ 2020 г.**
Подпис и печат:	[redacted]........................
Име и фамилия	[redacted]**тин Йорданов**
Длъжност	**Акаунт Мениджър "Държавни структури"**
Наименование на участника	**А1 БЪЛГАРИЯ ЕАД**

[redacted]

CISCO

Превод от английски език

ОТОРИЗАЦИОННО ПИСМО

Дата: **9 юли 2020 г.**

До: **Информационни услуги**

Относно: „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“

Cisco International Limited, регистрирана в Англия и Уелс (фирмен номер 06640658), със седалище в 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, Обединено кралство(“**Cisco**”), който е доставчик на мрежови продукти и услуги, с настоящото потвърждава, че към датата на настоящото писмо А1 България ЕАД, (“**Дилър** ”) желае да участва в търг или проект, посочени по-горе, и е сключила [партньорско споразумение за индиректен канал] [споразумение за технологичен интегратор на решения], което дава право на Дилъра да извършва следното:

(1) да препродава и/или да разпространява продукти и/или услуги на Cisco в БЪЛГАРИЯ към крайните потребители на тази територия;

(2) да наддава, да договаря и да сключи договор с вас за горепосочените продукти/услуги, произведени или предоставени от Cisco. Дилърът е независим изпълнител и няма право да ангажира и/или да обвързва по някакъв начин Cisco или свързаните с него лица.

В рамките на своите споразумения с разрешените канали Cisco ще предоставя поддръжка и гаранционни услуги за продукти на Cisco, придобити чрез неговите разрешени канали. Като такъв, Cisco препоръчва да получите потвърждение от посоченото по-долу лице за контакт на Cisco, че продуктите и/или услугите на Cisco се доставят чрез упълномощен източник на Cisco.

[redacted]

По подобен начин Cisco препоръчва да потвърдите серийните номера на продуктите на Cisco чрез инструмента за правилна покупка, намиращ се на адрес https://www.cisco.com/c/m/en_emear/brand-protection/index.html.

[redacted]

Допълнителна информация относно значението на закупуването чрез разрешени канали на Cisco може да бъде разгледана на линка, предоставен по-горе, а списъкът на упълномощените партньори на Cisco може да се види на: https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.do.

Потвърждението, предоставено съгласно настоящия Формуляр за разрешение, ще бъде достоверно към датата, посочена в горната част на това писмо и в продължение на 6 (шест) седмици от тази дата.

Ако имате нужда от допълнителна информация, моля да се свържете с Пламен Жечев на тел. +359 899 908 715. За повече информация относно партньорската програма на Cisco за канали, моля, посетете следния URL адрес: http://www.cisco.com/web/partners/index.html.

Надлежно упълномощен да подпише този Формуляр за упълномощаване от името на:
Cisco International Limited

Подпис- не се чете
Джеймс Гленистър
ДИРЕКТОР УПРАВЛЕНИЕ - ФИНАНСИ

Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
Обединено кралство

Подписаният Владимир Петков Найденов удостоверявам верността на извършения от мен превод от английски на български език на приложения документ "Оторизационно писмо". Преводът се състои от 2 (две) страници.

Преводач: [redacted]

Владимир Петков Найденов, 4308222229

MANUFACTURER'S AUTHORIZATION FORM

Date: **9 July 2020**

To: **Information Services**

Subject: **SUPPLY OF COMMUNICATION EQUIPMENT, HARDWARE AND SOFTWARE NECESSARY FOR UPDATING OF INFORMATION AND COMMUNICATION SYSTEMS OF THE NATIONAL REVENUE AGENCY .**

Cisco International Limited, registered in England and Wales (Company Number 06640658), having a principal place of business at 9-11 New Square Park, Bedfont Lakes, Feltham, England TW14 8HA, United Kingdom ("**Cisco**"), who is a provider of networking products and services, hereby confirms that, as of the date of this letter, A1 Bulgaria EAD ("**Reseller**") wishes to participate in the Bid or Project stated above and has entered into [an Indirect Channel Partner Agreement][a Solutions Technology Integrator Agreement] which entitles Reseller to do the following:

(1) resell and/or distribute Cisco products and/or services in BULGARIA to end users within that territory;

(2) bid, negotiate and conclude a contract with you for the above products/services manufactured or supplied by Cisco. The Reseller is an independent contractor and has no authority to commit and/or bind Cisco or its affiliates in any way.

Cisco will, within the scope of its agreements with the authorized channels, provide support and product warranty services for Cisco products acquired through its authorized channels. As such, Cisco recommends that you obtain confirmation, from the Cisco contact person listed below, that the Cisco products and/or services are being procured through a Cisco authorized source.

Similarly, Cisco recommends that you validate the serial numbers of the Cisco products through the Buy Right tool located at https://www.cisco.com/c/m/en_emear/brand-protection/index.html.

Additional information regarding the importance of purchasing through Cisco authorized channels can be reviewed at the link provided above and the list of Cisco authorized channel partners can be viewed at: https://locatr.cloudapps.cisco.com/WWChannels/LOCATR/openBasicSearch.do.

The confirmation provided under this Authorization form shall be accurate as of the date appearing at the top of this letter and for six (6) weeks from such date.

If you need any additional information, please do not hesitate to contact Plamen Zhechev at +359 899 908 715. For more information about Cisco's channel partner program, please visit the following URL: http://www.cisco.com/web/partners/index.html.

Duly authorized to sign this authorization form for and on behalf of: **Cisco International Limited**

[redacted]

James Glenister
DIRECTOR.MGMT-FINANCE

CISCO
Cisco International Limited
9-11 New Square Park
Bedfont Lakes, Feltham
Middlesex, TW14 8HA
United Kingdom

[redacted]

ВЯРНО С ОРИГИНАЛА

A1

[redacted]

[redacted]

[redacted]

[redacted]

ДО А1 БЪЛГАРИЯ ЕАД

ОТ СИСКО СИСТЕМС БЪЛГАРИЯ

УВЕДОМИТЕЛНО ПИСМО

Във връзка с Ваше участие в тръжна процедура с предмет: „Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите", декларираме, че изброените модели маршутизатори притежават SDWAN IPSec производителност, както следва:

- **ISR1100-4G – SDWAN IPSec производителност от 730Mbps за 1400 байтови пакети.**
- **ISR1100-6G – SDWAN IPSec производителност от 1.8Gbps за 1400 байтови пакети.**
- **ISR4451 – SDWAN IPSec производителност от 3.6Gbps за 1400 байтови пакети.**
- **ASR1001-X – SDWAN IPSec производителност от 7.8Gbps за 1400 байтови пакети.**

09.07.2020
София

СИСКО СИСТЕМС БЪЛГАРИЯ

С уважение: [redacted]

Сиско Системс България

[redacted]

[redacted]

[redacted]

[redacted]

ВЯРНО С ОРИГИНАЛА

[redacted]

[redacted]

ДЕКЛАРАЦИЯ

че при изготвяне на офертата са спазени задълженията, свързани с данъци и осигуровки, опазване на околната среда, закрила на заетостта и условията на труд

Долуподписаният **МАРТИН ДИМИТРОВ ЙОРДАНОВ**, л.к. [redacted], издадена на [redacted], на длъжност Акаунт Мениджър "Държавни структури", отдел "Държавни структури", направление „Корпоративни продажби" при „А1 БЪЛГАРИЯ" ЕАД

в качеството си на упълномощено лице на „А1 България" ЕАД, регистрирано в Агенцията по вписванията, с ЕИК: 131468980, ИН по ЗДДС: BG131468980, със седалище и адрес на управление: гр.София, ул. "Кукуш" №1,

участник в обществена поръчка с предмет:

„ДОСТАВКА НА КОМУНИКАЦИОННО ОБОРУДВАНЕ, ХАРДУЕР И СОФТУЕР, НЕОБХОДИМИ ЗА ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ"

За участие по Обособена позиция № 2 с предмет: „Доставка на софтуерно дефинирана мрежа за пренос на данни

Д Е К Л А Р И Р А М, че:

при изготвяне на офертата са спазени задълженията, свързани с данъци и осигуровки, опазване на околната среда, закрила на заетостта и условията на труд.

Дата: 13.07.2020 год. **Подпис:**..[redacted]........

Мартин Йорданов-
Акаунт Мениджър "Държавни структури"

Приложения към техническо предложение: брошури;

[redacted]

А1 България ЕАД

[redacted]

[redacted]

[redacted]

[redacted]

Агенция за преводи

ISO 9001:2000
Lloyd's Register Quality Assurance

Превод от английски език

ИНТЕРКОНСУЛТ ООД
ФИДЕС

CISCO

Информационен лист

Серия рутери за интегрирани услуги Cisco 4000

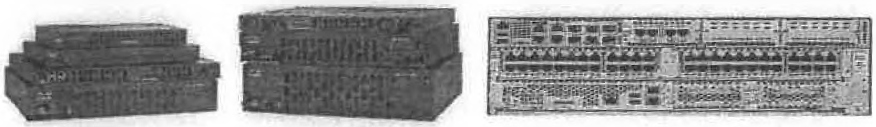
С[redacted]ия 1504, ул. "Св. Климент Охридски" №4
[redacted]: 02/ 946 13 92; тел./факс: 02/ 943 86 65
e-mail: office@fides.bg
www.fides.bg

Съдържание

Серията рутери за интегрирани услуги Cisco® 4000 (ISRs) формират софтуерно дефинирана WAN платформа, която осигурява производителност, сигурност и възможности за конвергенция, от които се нуждаят съвременните браншови офиси.

Преглед на продукта

Серията рутери за интегрирани услуги Cisco 4000 (ISR) революционизира WAN комуникациите в браншовете на предприятието. С новите нива на вградени интелигентни мрежови възможности и конвергенция, те са конкретно насочени към нарастващата нужда от свързаност на мрежата с приложенията, разпределени в различните обекти на предприятието. Тези обекти обикновено имат ограничени ИТ ресурси. Но често имат и нарастваща нужда от директна комуникация, както с центрове за лични данни, така и с публични облаци през различни връзки, включително Мултипротокол за превключване на етикети (MPLS) VPN и Интернет.
Серията Cisco 4000 съдържа следните платформи: 4461, 4451, 4431, 4351, 4331, 4321 и 4221 ISRs.



Фигура 1. Серия рутери за интегирани услуги Cisco 4000

Характеристики и предимства

Серията ISR на Cisco 4000 ви предоставят софтуерните функции на Cisco® Софтурно дефинирана WAN (SDWAN) и конвергирана инфраструктура на бранша. Заедно с превъзходната производителност, тези възможности формират градивните елементи на следващото поколение WAN решения за браншовия офис.

Софтурно дефинирана WAN на Cisco

Cisco SDWAN е набор от интелигентни софтуерни услуги, които ви позволяват надеждно и сигурно да свързвате потребители, устройства и локации на браншовете с един разнообразен комплект от транспортни връзки на WAN. Поддържани от SDWAN маршрутизатори като ISR 4000 динамично маршрутизират трафика през „най-добрата" връзка, базирана на актуално приложение и мрежови условия за пълноценно използване на приложението. Получавате строг контрол върху работата на приложението, използването на честотна лента, поверителността на данните и наличието на вашите WAN връзки - контрол, от който се нуждаете, тъй като вашите браншове извършват голям обем от критично важни за бизнеса дейности.

Cisco Конвертирана браншова инфраструктура

ISRs от серията Cisco 4000 консолидират много задължителни ИТ функции, включително мрежови, изчислителни и съхранителни ресурси. Високопроизводителните интегрирани маршрутизатори изпълняват множество едновременни услуги, включително криптиране, управление на трафика и оптимизация на WAN, без да забавят преминаването на вашите данни. Освен това вие можете да активирате нови услуги при поискване чрез обикновена промяна на лиценза.

„ФИДЕС ИНТЕРКОНСУЛТ" ООД • СОФИЯ •

[redacted]

[redacted]

A1 България ЕАД

Интернет-базирана мрежа на Cisco и Цифрова мрежова архитектура (Cisco DNA)

През последните няколко години се наблюдава бърза трансформация и приемане на цифровите технологии. Това оказва натиск върху мрежовите екипи, които поддържат тази променяща се инфраструктура - особено при осигуряването, управлението, мониторинга и отстраняването на неизправности при тези разнообразни устройства. Освен това иновации като софтуерно дефинирана WAN (SDWAN), виртуализация на мрежовите функции (NFV), отворени API и Облачно управление са многообещаващи за трансформирането на ИТ мрежите на организациите. Тази трансформация поставя допълнителни въпроси и предизвикателства пред ИТ екипите.

Цифровата мрежова архитектура на Cisco (Cisco DNA) е отворена, разширяема, софтуерно ориентирана архитектура, която осигурява по-бързи иновации, помага за генериране на по-дълбоки познания и предоставя изключителен опит в много различни приложения. Cisco DNA разчита на базирани на намерения мрежи, революционен подход в мрежите, който помага на организациите да автоматизират, опростят и защитят мрежата.

Базираната на намерения мрежа Cisco DNA е:

- Информирана от контекста: Интерпретира всеки байт данни, които преминават през нея, което води до по-добра сигурност, по-персонализирано използване и по-бързи операции.
- Задвижвана от намерението: Транслира вашето намерение в правилната мрежова конфигурация, като прави възможно управлението и предоставянето на множество устройства и неща за минути.
- Водена от интуицията: Непрекъснато се учи от огромните количества данни, преминаващи през нея, и превръща тези данни в действени изводи. Помага ви да решавате въпроси, преди те да са станали проблеми и да се поучите от всеки инцидент.

Центърът на Cisco DNA осигурява централизирано табло за управление в цялата ви мрежа - бранша, кампуса, центъра за данни и облака. Вместо да разчитате на управление на отделните елементи, можете да проектирате, осигурите и зададете политика от край до край от единствения интерфейс на Центърът на Cisco DNA. Това ви позволява да отговорите по-бързо на организационните нужди и да опростите ежедневните операции. Cisco DNA Анализ и Осигуряване и Мрежова платформа за данни на Cisco (NDP) ви помагат да извлечете максимума от вашата мрежа, като непрекъснато събирате и реализирате вашите интуитивни оценки. Cisco DNA е отворена, разширяема и програмируема на всяко ниво. Тя интегрира технологии на Cisco и на трети страни, отворени API и платформа на разработчика, за да поддържа богата екосистема от мрежови приложения.

Таблица 1 показва много от функциите и предимствата на Серията Cisco 4000, които създават софтуерно дефинирана WAN (SDWAN) и конвертирана браншова инфраструктура.

Таблица 1. Основни функции на серията ISRCisco 4000

Бизнес изискване(я)	Функция/Решение
Действие • Пропускателна способност • Надеждност на услугата	• Едновременни софтуерни услуги със скорост до 2 Gbps. Архитектурата на свързващата платка поддържа комуникация между модулите с висока честотна лента със скорост до 10 Gbps. • Разпределена многоядрена архитектура с първия за индустрията панел за вътрешни услуги. • Дистанционно инсталиране на свързани с приложенията услуги, които работят идентично със съответните елементи в определените уреди.
По-ниски разходи за WAN	• Вградено SDWAN решение за създаване на бизнес клас интернет връзки.
Заплащане с растежа на бизнеса • Модел за надграждане на производителността • Защита на инвестициите • Управление на бюджета за капиталови разходи	• Капацитетът на рутера може да бъде увеличен с отдалечено надграждане на лиценза за изпълнение по заявка (без надстройка на хардуера) за високи спестявания.
Превъзходно и сигурно използване на потребителските приложения	• Софтуерен пакет ISR-AX „Опит в приложението“ с разширени услуги за маршрутизиране и мониторинг на мрежата. • Динамичен мултиточков VPN (DMVPN), зоново-базирани защитни стени, предотвратяване на проникване (Snort & Umbrella Branch) и управление на съдържанието чрез изолиране на Cisco Cloud Web Security и OpenDNS защита на данните.

А1 България ЕАД

Бизнес изискване(я)	Функция/Решение
	предоставяне на идентификационни данни и предавания, които не се обработват обратно през центъра за данни. • Функцията за сигурно зареждане извършва хардуерно удостоверяване на софтуера за зареждане, за да предотврати зареждането на злонамерен или непредвиден софтуер в системата. • Влизането с код проверява цифровите сигнатури на изпълнимите файлове преди преди тяхното зареждане, за да се предотврати изпълнението на променен или повреден код. • Хардуерното удостоверяване предпазва от хардуерно фалшифициране чрез използване на силикон, предпазващ от фалшификации на платките, включително и за полевите заменяеми модули. Ако удостоверяването е не успешно, модулът не може да се стартира.
ИТ консолидация, спестяване на пространство и подобрени Общи разходи за собственост (TCO)	• Единичната конвергирана браншова платформа интегрира маршрутизация, комутация, виртуален сървър, съхранение, сигурност, унифицирани комуникации, WAN оптимизация и инструменти за управление на производителността.
Непрекъснатост на бизнеса и повишена гъвкавост	• Моделите от серията ISR 4400 (4461, 4451 и 4431 ISR) поддържат двойни интегрирани източници на енергия за архивиране. Цялата серия ISR 4000 поддържа опционално допълнително захранване, което може да достави допълнителна PoE мощност до крайните точки. • Модулни мрежови интерфейси с разнообразни възможности за свързване за балансиране на натоварването и устойчивост на мрежата. • Модулни интерфейси с онлайн премахване и поставяне (OIR) за надстройки на модули без прекъсване на мрежата. • Cisco Унифицирана телефония за оцеляване на отдалечени обекти (SRST), която служи за допълнителна гъвкавост на хостваното от Cisco решение за сътрудничество (HCS), Cisco облачно-базирана UC услуга. • Поддръжка на много и разнообразни връзки за достъп: T1/E1, T3/E3, Serial, xDSL, Gigabit и Ten-Gigabit Ethernet.
По-ниски разходи за телефония с VoIP и богат медиен опит	• Високопроизводителен аналогов/ цифров шлюз, позволяващ VoIP през по-евтини стволове на Session Initiation Protocol (SIP). • Интегриран IP PBX (Cisco Unified Communications Express) и сесиен граничен контролер (Cisco Unified Border Element или CUBE).
Easier manageability and support	• Единично, универсално софтуерно изображение за всички функции и гъвкавост на лицензирането по заявка. • Не са необходими допълнителни услуги и поддръжка за компютърна обработка и съхранение. • Поддържа се от инструменти за управление на Cisco и трети страни, с програмируемост и автоматизация.

Архитектура на платформата

Таблица 2 изброява основните хардуерни архитектурни характеристики и предимства на серията Cisco 4000. Рутерите работят с модулен софтуер Cisco IOS XE, широко използван в най-взискателните мрежи по света. Цялостното портфолио от услуги на софтуера обхваща множество технологични области, включително сигурност, оптимизация на WAN, качество на услугите за приложения и мрежи (QoS) и вградено управление.

Таблица 2. Важни архитектурни елементи

Архитектурни характеристики	Ползи/ Описание
Многоядрени процесори	• Високопроизводителните многоядрени процесори поддържат високоскоростни WAN връзки. Равнината на данните използва емулиран процесор на потока (FP), който осигурява ефективност подобна на специфична за приложението интегрална схема (ASIC), която не се влошава при добавяне на нови услуги.
Вградено хардуерно ускорение на VPN IP Security (IPsec)	• Увеличава мащабируемостта. В комбинация с опционален лиценз за софтуерна сигурност на Cisco IOS XE, дава възможност за сигурност на WAN връзка и VPN услуги.

A1 България ЕАД

Архитектурни характеристики	Ползи/ Описание
Интегрирани Gigabit Ethernet портове	• Серията Cisco 4000 осигурява до четири вградени 10/100/1000 Ethernet порта за WAN или LAN. • В зависимост от платформата, някои от портовете 10/100/1000 Ethernet могат да поддържат включваема свързаност с малък форм-фактор (SFP) в допълнение към RJ-45 връзки, което позволява свързване на медни или оптични проводници. • Опционално, в зависимост от платформата, до 30W PoE+ могат да бъдат активирани на два от вградените интерфейси Gigabit Ethernet на предния панел, за да осигурят захранване на външни устройства, като LTE рутери от четвърто поколение (4G). • За управление на устройството е осигурен допълнителен специален Gigabit Ethernet порт[1]
Достъп до USB-базирана конзола	• Един мини портал[1] тип B USB конзола поддържа свързаност за управлението, когато традиционните серийни портове не са налични. • Предлагат се и традиционните конзолни и спомагателни портове[2].
Опционално интегрирано захранване за разпределение на PoE	• Една опционална надстройка на вътрешното захранване осигурява линейно захранване (802.3af - съвместимо с PoE, или 802.3at - съвместимо с PoE +) към опционални интегрирани комутационни модули. • Резервните модули за преобразуване на PoE осигуряват допълнително ниво на толеранс.
Опционално интегрирано резервно захранване (RPS)	• За серията ISR 4400 се предлага резервирана мощност чрез инсталиране на опционален интегриран RPS за намаляване на прекъсване на мрежата и защита на мрежата от прекъсване на захранването. • Опционалният PoE усилващ режим увеличава общия PoE капацитет до 1000W.
Модул за подобрени услуги на Cisco (SM-X)	• Всеки слот за сервизен модул предлага висока способност за пропускане на данни до 10 Gbps към системата и до 1 Gbps към други слотове за модули. • Поддръжката както на единични, така и на двойно широки сервизни модули осигурява гъвкавост при опциите за внедряване. • Един слот SM-X може да бъде преобразуван в слот за мрежов интерфейсен модул (NIM), като се използва допълнителна носеща карта. • Сервизните модули поддържат онлайн добавяне и премахване (OIR), като се избягва прекъсване на мрежата при инсталиране на нови или заместващи модули[1].
Мрежови интерфейсни модули на Cisco (NIM)[3]	• До три интегрирани NIM слота при серията Cisco 4000 позволяват гъвкави конфигурации. • Всеки NIM слот предлага опции за до две 2Gbps връзки. Един към процесора на рутера и един за директна комуникация между модулите. ISR 4221 има само една връзка от 1Gbps към процесора на рутера. • NIM поддържат OIR. • Специалните NIM добавят поддръжка на дискове на твърди схеми (SSD) и твърди дискове (HDD)[1].
Вграден Слот за Cisco Карта за интегрирани услуги (ISC)	• Картата за интегрирани услуги поддържа пшо принцип новите модули за цифрови сигнални процесори с висока плътност на Cisco (PVDM4s), осигуряващи гласова връзка с по-голяма плътност на за много медии. • Всеки слот за карта за интегрирани услуги се свързва към системната архитектура чрез връзка до 2 Gbps. • Допълнителни модули могат да бъдат хоствани в слота за карта за интегрирани услуги, подобрявайки системните функции.
Поддръжка на флаш памет	• На разположение е един слот за флаш памет за поддържане на високоскоростни плътности на съхранение, които могат да се разширят до 32 GB. ISR4221 се доставя с фиксирана 8GB флаш памет. • Два USB порта тип A 2.0 предоставят възможности за удобно съхранение[1].

[1] Не се поддържа на ISR4221

[2] ISR4221 поддържа споделени конзолни и спомагателни портове

[3] Унифицирани комуникации (UC) и UC-базирани NIM не се поддържат

[redacted]

[redacted]

Архитектурни характеристики	Ползи/ Описание
DRAM (Динамична памет с произволен достъп)	• За серията ISR 4400 паметта на контролната равнина по подразбиране е 4 GB, надграждаща се до 16 GB, за да се осигури допълнителна мащабируемост на функциите на контролната равнина. Паметта на равнината на данни по подразбиране е 2 GB. • За серията ISR 4300 паметта по подразбиране е 4 GB, надграждаща се до 16 GB (само 8 GB за 4321), за да осигури допълнителна мащабируемост. • Серията ISR 4200 се предлага с 4GB фиксирана DRAM

Управление на вашите ISR от серията Cisco ISR 4000

Приложенията за управление на мрежата на Cisco, изброени в горната част на таблица 3, са самостоятелни продукти, които могат да бъдат закупени или изтеглени за управление на вашите Cisco мрежови устройства. Приложенията са изградени специално за различните работни фази; изберете тези, които най-добре отговарят на вашите нужди. Възможностите за управление, изброени под заглавието „Cisco IOS Софтуер XE за вградено управление" са директно интегрирани в софтуерната операционна система на рутерите.

Таблица 3. Cisco DNA Център

Работни фази	Приложение	Описание
Инсталиране и конфигуриране на устройството	WebUI (мрежов потребителски интерфейс)	• Инструмент за управление на устройства, базиран на GUI, за софтуерно базирани рутери за достъп на Cisco IOS и Cisco IOS XE. Този инструмент опростява маршрутизирането, защитната стена, VPN, унифицираните комуникации и WAN и LAN конфигурацията чрез лесни за използване спомагателни функции.
Инсталиране, конфигуриране, наблюдение и отстраняване на проблеми в цялата мрежа	Инфраструктура на Cisco Prime ™	• Предлага цялостно управление на жизнения цикъл на кабелен и безжичен достъп, мрежи на централен офис и на браншове, висока видимост в свързаността на крайния потребител и осигуряване на ефективността на приложението. • Осигурява жични функции на жизнения цикъл като управление на инвентара, конфигурация и управление на изображенията; автоматизирано внедряване; докладване за съответствие; интегрирани най-добри практики; и изготвяне на отчети.
Инсталиране, внедряване и промени в конфигурацията и файловете за изображения	Cisco програма за конфигуриране	• Защитен продукт за управление на мрежата, който осигурява автоматично разпределение на изображенията и конфигурацията чрез централизирано управление, основано на шаблони.
Конфигурация на сигурността и мониторинг в зависимост от контекста	Cisco Основен мениджър по сигурността	• Инструмент за управление за конфигуриране и управление на сигурността в зависимост от контекста. Приложението поддържа форм-фактори за управление както на отделни, така и на много устройства. . • Предоставя възможност за писане и прилагане на подробни политики за сигурност, съобразени с контекста.
Управление на Cisco услугата за приложения в широкообхватна мрежова среда (WAAS)	Cisco WAAS Централен мениджър	• Инструментът за управление на интегрираната услуга WAAS[1,4], (оптимизация на WAN и ускоряване на приложението). Осигурява централизиран механизъм за конфигуриране на WAAS функции, отчитане и наблюдение.

Възможности за управление на вградения софтуер на Cisco IOS XE	
Характеристика	Описание
Вграден мениджър на събития на Cisco IOS (EEM)	• Разпределен и персонализиран подход за откриване и възстановяване на събития. • Предлага възможност за наблюдение на събития и предприемане на информационни, коригиращи или желани EEM действия, когато наблюдаваните събития се появят или когато се достигне определен праг.
Споразумения за ниво на обслужване на Cisco IOS XE IP (IP SLAs)	• Помага да се осигури ефективността на нови критични за бизнеса IP приложения, както и на IP услуги, които използват данни и глас в IP мрежа.
SNMP Дистанционно наблюдение (RMON), системна регистрация ,NetFlow Експорт на информация за IP потока (IPFix)	• Мрежови инструменти за мониторинг и отчитане.

[redacted] я ЕАД

Спецификация на продукта

Таблица 4 изброява общите спецификации на продукта за рутерите от серията Cisco 4000.

Таблица 4. Спецификация на серията рутери за интегрирани услуги Cisco 4000

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Сумарна пропускателна способност (по подразбиране)	1.5Gbps	1 Gbps	500 Mbps	200 Mbps	100 Mbps	50 Mbps	35Mbps
Сумарна пропускателна способност (Лиценз за изпълнение)	3Gbps	2 Gbps	1 Gbps	400 Mbps	300 Mbps	100 Mbps	75 Mbps
Сумарно само за CEF[5] пропускателна способност (Лиценз за увеличаване)	Над 7Gbps	Над 4Gbps	Над 4Gbps	Над 2Gbps	Над 2Gbps	1.5Gbps	1.2Gbps
Всичко вградени WAN или LAN 10/100/1000 портове	4	4	4	3	3	2	2
Всичко вградени WAN или LAN 10Gbps портове	2	-	-	-	-	-	-
RJ-45-базирани портове	4	4	4	3	2	2	2
SFP-базирани портове	4	4	4	3	2	1	1

[5] Използване на Gigabit Ethernet интерфейси, вградени в дънната платка

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Разширени слотове за сервизни модули	3	2	0	2	1	0	0
Слотове за сервизни модули с двойна ширина	2	1 (предполага, че не са инсталирани SM-X модули с единична ширина)	0	1 (предполага, че не са инсталирани SM-X модули с единична ширина)	0	0	0
NIM слотове	3	3	3	3	2	2	2
OIR (всички Вх./Изх. модули)	Да	Да	Да	Да	Да	Да	Не
ISC слот на дънната платка	1	1	1	1	1	1	Не
По подразбиране памет с двойна скорост за данни 3 (DDR3) за код за корекция на грешки (ECC) DRAM (Комбинирани равнини на контрол/ услуги)	Няма	Няма	Няма	4 GB	4 GB	4 GB	4GB
Максимална памет DDR3 ECC DRAM (Комбинирани равнини на контрол/ услуги)	Няма	Няма	Няма	16 GB	16 GB	8 GB	4GB
Памет по подразбиране DDR3 ECC DRAM (равнина на данните)	4 GB	2 GB	2 GB	Няма	Няма	Няма	Няма
Максимална памет DDR3 ECC DRAM (равнина на данните)	4 GB	2 GB	2 GB	Няма	Няма	Няма	Няма
Памет по подразбиране DDR3 ECC DRAM (равнини на контрол/ услуги)	8 GB	4 GB	4 GB	Няма	Няма	Няма	Няма

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Максимална памет DDR3 ECC DRAM (равнини на контрол/ услуги)	32 GB	16 GB	16 GB	Няма	Няма	Няма	Няма
Флаш памет по подразбиране	8 GB	8 GB	8 GB	4 GB	4 GB	4 GB	8GB
Максимална флаш памет по подразбиране	32 GB	32 GB	32 GB	16 GB	16 GB	8 GB	8GB
Външни USB 2.0 слотове (тип А)	2	2	2	2	1	1	1
USB конзолен порт - тип В мини (до 115,2 kbps)	1	1	1	1	1	1	0
Сериен конзолен порт - RJ45 (до 115,2 Gbps	1	1	1	1	1	1	1 (комбиниран CON/AUX порт)
Сериен спомагателен порт - RJ45 (до 115,2 kbps)	1	1	1	1	1	1	1 (комбиниран CON/AUX порт)
Опции за ел. захранване	Вътрешни: AC, DC и PoE	Вътрешни: AC, DC и PoE	Вътрешни: AC, DC и PoE	Вътрешни: AC, DC и PoE	Вътрешни: AC,DC и PoE	Външни : AC и PoE	Само външно AC
Резервно ел. захранване	Вътрешни: AC, DC и PoE	Вътрешни: AC, DC и PoE	Вътрешни: AC, DC и PoE	Няма	Няма	Няма	Няма
Спецификации на ел. захранването							
Входно напрежение AC	100 до 240 VAC автоматично	100 до 240 VAC автоматично	100 до 240 VAC автоматично	100 до 240 VAC автоматично	100 до 240 VAC автоматично	100 до 240 VAC автоматично	100 до 240 VAC автоматично
Входно напрежение DC							
Входно напрежение	48 – 60V	48 – 60V	48 – 60V	Няма	24 – 60V	Няма	Няма
Входен ток	12A Макс.	12A Макс.	12A Макс.	Няма	14 - 5A	Няма	Няма
Входна честота AC	47 до 63 Hz	47 до 63 Hz	47 до 63 Hz	47 до 63 Hz	47 до 63 Hz	47 до 63 Hz	47 до 63 Hz
Диапазон на входния AC ток, AC ел. захранване (максимум)	7.1 до 3.0A	7.1 до 3.0A	3 до 1.3A	7.1 до 3.0A	3 до 1.3A	1.5 до 0.6A	1.5 до 0.6A
AC входен свръхток	60 A пиков ток и под 5 Arms за половин цикъл	<50 A	60 A пиков ток и под 5 Arms за половин цикъл	60 A пиков ток и под 12 Arms за половин цикъл	60 A пиков ток и под 5 Arms за половин цикъл	90 A пиков ток и под 3 Arms за половин цикъл	90 A пиков ток и под 3 Arms за половин цикъл
Стандартна мощност		158	65	48	42	36	24

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
(без модули) (ватове)							
Максимална мощност с AC ел. захранване (ватове)	1000W (без PoE)	450 (без PoE)	250 (без PoE)	430	250	125	90
Максимална мощност с DC ел. захранване (ватове)	437 (без PoE)	437 (без PoE)	437 (без PoE)	437 (без PoE)	250 (без PoE)		
Максимална мощност с PoE ел. захранване (само за платформата) (ватове)	1000 с резервирано PoE 1450 с PoE усилване без резервираност	1000 с резервирано PoE 1450 с PoE усилване без резервираност	500 с резервирано PoE 1000 с PoE усилване без резервираност	990	530	260	Няма (без PoE поддръжка)
Максимално крайно PoE захранване, налично от PoE ел. захранване (ватове)	500 W опционална резервираност	500 W опционална резервираност	250 W опционална резервираност	500	250	120	Няма (без PoE Поддръжка)
Максимален капацитет на крайно PoE захранване с PoE усилване (ватове)	950 W без резервираност	950 W без резервираност	500 W без резервираност	Няма	Няма	Няма	Няма (без PoE Поддръжка)
Размери и тегло							
Размери (В x Ш x Д)	3,5 x 17,25 x 18,5 инча 88,9 x 438,15 x 469,9 mm)	3,5 x 17,25 x 18,5 инча (88,9 x 438,15 x 469,9 x mm)	1,73 x 17,25 x 19,97 инча (43,9 x 438,15 x x 507,2 mm)	3,5 x 17,25 x 18.5 инча (88,9 x 438,15 x 469,9 mm)	1,75 x 17,25 x 17,25 инча (44,45 x 438,15 x x 438,15 mm)	1,75 x 14,55 x 11.60 инча (44.55 x 369,57 x x 294,64 mm)	1,72 x 12,7 x 10" (43,7 x 322,6 x 254 mm)

[redacted]

[redacted]

[redacted]

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Размери на външното на ел. захранване (В x Ш x Д)	Няма	Няма	Няма	Няма	Няма	2,95 x 1,18 x 6,10 инча (75 x 30 x 155 mm)	37 x 73 x 152 mm (Phihong mfg PN: AA90U-120A- R) 36,5 x 67 x 155 mm (Delta mfg PN: ADP90GR BA)
Размери на опаковъчната кутия (В x Ш x Д)	9,75 x 22,25 x 26 инча (24,76 x 56,51 x x 66,04 mm)	9,75 x 22,25 x 26 инча (24,76 x 56,51 x x 66,04 mm)	7,88 x 22,25 x 28,75 инча (200,2 x 565,1 x 730,25 mm)	9,75 x 22,25 x 26 инча (24,76 x 56,51 x 66,04 mm)	7,125 x 22,75 x 22,5 инча (180,98 x 577,85 x x 571,5 mm)	7,0 x 21,5 x 16,125 инча (177,8 x 546,1 x 409,6 mm)	4,13 x 18,25 x 12,94" (104,9 x 463,6 x 328,7 mm)
Височина на рака	3 Рак единици (3RU)	2 Рак единици (2RU)	1 Рак единица (1RU)	2 Рак единици (2RU)	1 Рак единица (1RU)	1 Рак единица (1RU)	1 Рак единица (1RU)
Монтируем в рак 19 инча (48.3 cm) EIA	Включено	Включено	Включено	Включено	Включено	Включено	Опция
Монтируем в рак 23 инча (58.4 cm) EIA	Опция	Опция	Опция	Опция	Опция	Няма	Няма
Стенен монтаж	Не	Не	Да	Не	Да	Монтажни отвори под шасито	Да
Тегло с 1, 450-WAC ел. захранване (без модули)		28.8 lb (13.1 kg)	Няма	28,8 lb (1,2 kg)	Няма	Няма	Няма
Тегло с 1 1000-WAC ел. захранване+ 1 PoE захр. модул (без други модули)		30,6 lb (13,9 kg)	Няма	29,0 lb (13,2 kg)	Няма	Няма	Няма
Тегло с AC E3 (без модули)		Няма	16,5 lb (8,4 kg)	Няма	13,5 lb (6,2 kg)	7,7 lb (3,5 kg) + 1,2 lb (0,66 kg) външно E3	7,1 lb (3,22kg)
Тегло с DC E3 (без модули)		28,8lb (1,2 kg)	28,8lb (1,2 kg)	28,8lb (1,2 kg)	13,5 lb (6,2 kg)		
Тегло с AC E3 с POE (без модули)		Няма	18,6 lb (8,4 kg)	Няма	14,1 lb (6,4 kg)	Няма	Няма
Стандартно тегло (напълно зареден с модули)		42,7 lb (19,4 kg)	22,4 lb (10,2 kg)	37,7 lb (17,1 kg)	16,1 lb (7,3 kg)	9,14 lb (4,2 kg) + 1,2 lb (+ 0,66 kg) външно E3	8,11 lb (3,68kg)
Пакетиране		6,4 lb (2,9 kg)	5,9 lb (2,7 kg)	6,4 lb (2,9 kg)	4,6 lb (2,1 kg)	2,2 lb (1 kg)	1,28 lb (0,58kg)

[redacted]

A1 България ЕАД [redacted]

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Тегло							
Въздушен поток	Вх./Изх. страна към рамката	Вх./Изх. страна към рамката	Вх./Изх. страна към рамката	Вх./Изх. страна към рамката	Вх./Изх. страна към рамката	Дясна Вх./Изх. страна към лява Вх./Изх. страна	Вх./Изх. страна към рамката
Средното време между отказите MTBF (часове)	480770	480770	512970	566310	587250	593270	593270
Екологични спецификации							
Работни условия							
Температура	32 до 104°F (0 до 40°C)	32 до 104°F (0 до 40°C)	32 до 104°F (0 до 40°C)	32 до 104°F (0 до 40°C)	32 до 104°F (0 до 40°C)	32 до 104°F (0 до 40°C)	32 до 104°F (0 до 40°C)
Надморска височина (Китай)	0 – 6560 фута (0 – 2 000 m)	0 – 6560 фута (0 – 2 000 m)	0 – 6560 фута (0 – 2 000 m)	0 – 6560 фута (0 – 2 000 m)	0 – 6560 фута (0 – 2 000 m)	0 – 6560 фута (0 – 2 000 m)	0 – 6560 фута (0 – 2 000 m)
Надморска височина (За останалия свят)	0 – 10000 фута (0 – 3 050 m)	0 – 10000 фута (0 – 3 050 m)	0 – 10000 фута (0 – 3 050 m)	0 – 10000 фута (0 – 3 050 m)	0 – 10000 фута (0 – 3 050 m)	0 – 10000 фута (0 – 3 050 m)	0 – 10000 фута (0 – 3 050 m)
Краткотрайна температура до 6560 фута за NEBS GR-63-CORE	Няма	Няма	Няма	Няма	32° до 131° (0° до 55° C) (за ISR4331-DC версия)	Няма	Няма
Относителна влажност	5% до 85%	5% до 85%	5% до 85%	5% до 85%	5% до 85%	5% до 85%	5% до 85%
Краткосрочна влажност	5% до 90% да не се надхвърля 0,024 kg вода/kg сух въздух	5% до 90% да не се надхвърля 0,024 kg вода/kg сух въздух	5% до 90%, да не надхвърля 0,024 kg вода/kg сух въздух	5% до 90%, да не надхвърля 0,024 kg вода/kg сух въздух	5% до 90%, да не надхвърля 0,024 kg вода/kg сух въздух	5% до 90%, да не надхвърля 0,024 kg вода/kg сух въздух	5% до 90%, да не надхвърля 0,024 kg вода/kg сух въздух
Акустика: Звуковото налягане (Стандартно/ максимално)	50,6/73,1 dBA	50,6/73,1 dBA	54,3/79,1 dBA	50,6/73,1 dBA	52,8/74,8 dBA	24,2/51,9 dBA	28,5/53 dBA

[redacted]

[redacted]

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Акустика: Звукова мощност (Стандартна/ максимална)	58,2/78,8 dBA	58,2/78,8 dBA	57,2/80,8 dBA	58,2/78,8 dBA	61,2/81,6 dBA	31,9/59,9 dBA	41/68 dBA
Неработни условия							
Температура	-40 до 158°F (-40 до 70°C)	-40 до 158°F (-40 до 70°C)	-40 до 158°F (-40 до 70°C)	-40 до 158°F (-40 до 70°C)	-40 до 158°F (-40 до 70°C)	-40 до 158°F (-40 до 70°C)	-40 до 158°F (-40 до 70°C)
Относителна влажност	5% до 95%	5% до 95%	5% до 95%	5% до 95%	5% до 95%	5% до 95%	5% до 95%
Надморска височина	15 584 фута (4750m)	15 584 фута (4750m)	15 584 фута (4750m)	15 584 фута (4750m)	15 584 фута (4750m)	15 584 фута (4750m)	15 584 фута (4750m)
Регулация и съответствие							
Безопасност	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Част 15 ICES-003 Клас A EN55032 Клас A CISPR32 Клас A AS/NZS CISPR 32 Клас A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (устойчивост) EN 55024, CISPR 24 KN22, KN24	47 CFR, Част 15 ICES-003 Клас A EN55032 Клас A CISPR32 Клас A AS/NZS CISPR 32Клас A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (устойчивост) EN 55024, CISPR 24 KN22, KN24	47 CFR, Част 15 ICES-003 Клас A EN55032 Клас A CISPR32 Клас A AS/NZS CISPR 32Клас A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (устойчивост) EN 55024, CISPR 24 KN22, KN24	47 CFR, Част 15 ICES-003 Клас A EN55032 Клас A CISPR32 Клас A AS/NZS CISPR 32Клас A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (устойчивост) EN 55024, CISPR 24 KN22, KN24	47 CFR, Част 15 ICES-003 Клас A EN55032 Клас A CISPR32 Клас A AS/NZS CISPR 32Клас A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (устойчивост) EN 55024, CISPR 24 KN22, KN24 EN 50121-1 EN61000-6-4 EN 50121-4	ICES-003 Клас A EN55032 Клас A CISPR32 Клас A AS/NZS CISPR 32Клас A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (устойчивост) EN 55024, CISPR 24 KN22, KN24	ICES-003 Клас A EN55032 Клас A CISPR32 Клас A AS/NZS CISPR 32Клас A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (устойчивост) EN 55024, CISPR 24 KN22, KN24
Телекомуникация	T1 IC CS- 03:2004	T1 IC CS-03:2004 TIA-968-	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101

“СИДЕС ИНЖЕНЕРИНГ КОНСУЛТ” ООД

КП2

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
	TIA-968-B:2009 НКТА 2028:2010 НКТА 2017:2010 НКТА 2015: 2006 G.703:2001 ID0002:2007 IS6100:2004 DSPR Сива книга:2000 DSPR Технически условия: 2004 E1 AS/ACIF S016: 2001 AS/ACIF S038: 2001 G.703:2001 TBR 4:1995 TBR 12:1993 TBR 13:1996 RRA 2009-38 (RRL 2005-96) IDA TS DLCN:2011 IDA TS ISDN PRA:2005 IS6100: 2004 PTC 220:2008 Ethernet IEEE 802.3 ANSA X3.263	B:2009 НКТА 2028:2010 НКТА 2017:2010 НКТА 2015: 2006 G.703:2001 ID0002:2007 IS6100:2004 DSPR Сива книга:2000 DSPR Технически условия: 2004 E1 AS/ACIF S016: 2001 AS/ACIF S038: 2001 G.703:2001 TBR 4:1995 TBR 12:1993 TBR 13:1996 RRA 2009-38 (RRL 2005-96) IDA TS DLCN:2011 IDA TS ISDN PRA:2005 IS6100: 2004 PTC 220:2008 Ethernet IEEE 802.3 ANSA X3.263	ITU-T G.823, G.824 IEEE 802.3 RTTE Директива Изискванията за хомологация варират в зависимост от държавата и типа интерфейс. За информация за конкретна държава вижте онлайн базата данни за одобрения на: https://www.ciscofax.com/	ITU-T G.823, G.824 IEEE 802.3 RTTE Директива Изискванията за хомологация варират в зависимост от държавата и типа интерфейс. За информация за конкретна държава вижте онлайн базата данни за одобрения на: https://www.ciscofax.com/	ITU-T G.823, G.824 IEEE 802.3 RTTE Директива Изискванията за хомологация варират в зависимост от държавата и типа интерфейс. За информация за конкретна държава вижте онлайн базата данни за одобрения на: https://www.ciscofax.com/	ITU-T G.823, G.824 IEEE 802.3 RTTE Директива Изискванията за хомологация варират в зависимост от държавата и типа интерфейс. За информация за конкретна държава вижте онлайн базата данни за одобрения на: https://www.ciscofax.com/	ITU-T G.823, G.824 IEEE 802.3 RTTE Директива Изискванията за хомологация варират в зависимост от държавата и типа интерфейс. За информация за конкретна държава вижте онлайн базата данни за одобрения на: https://www.ciscofax.com/

Cisco IOS XE Софтуер

Протоколи	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to- Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent

[redacted]

Технически спецификации	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
	Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), RSVP, CDP, ERSPAN, IPSLA, Call Home, EEM, IKE, ACL, EVC, DHCP, FR, DNS, LISP, OTV[6], HSRP, RADIUS, AAA, AVC, Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IP sec, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE802.1ag, and IEEE802.3ah						
Капсулиране	Генерично рутинг капсулиране (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 и FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), и PPP over Ethernet (PPPoE)						
Управление на трафика	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing, and NBAR.						
Криптографски алгоритми	Шифриране: DES, 3DES, AES-128 или AES-256 (в CBC и GCM режими); Удостоверяване: RSA (748/1024/2048 bit), ECDSA (256/384 bit); Интегритет: MD5, SHA, SHA-256, SHA-384, SHA-512						

Равнина на услугите: Активиране на Branch-in-a-Box

Всички маршрутизатори Cisco ISR 4000 съдържат като стандарт вградени процесорни ядра, за да позволяват пълнофункционални услуги да се изпълняват от платката. Това включва пълнофункционален Cisco WAAS, който осигурява ускорение на приложението и висока отзивчивост на виртуалния работния плот. Технологията е известна като Cisco Service Containers и използва стандартен хипервизор, за да позволи стартиране на приложения, базирани на x64.

Рутерите от серия 4000 могат да бъдат оборудвани с дискове на твърди схеми (SSD) и сървърни карти за локално съхранение и компютърни възможности. Сървърните карти Cisco UCS-E се предлагат с 8-ядрени процесори Intel Xeon с до 48 GB високоскоростна DDR3 памет и три вградени диска, предлагащи RAID 0,1 и 5. Това огромно количество изчислителна мощност може да премахне нуждата от всякакви специализирани сървъри в браншовите обекти. UCS-E картите могат да бъдат конфигурирани и управлявани с помощта на VMware vCenter и обединени с компютърните ресурси на Центъра за данни.

[6] Поддържа се само на 4451 за честотна лента <100Mbps

Абонамент за софтуер чрез Cisco DNA лицензиране

Серията ISR4000 поддържа софтуерно базиран абонамент, използвайки лицензиране на базата на Cisco DNA. За портфолиото на WAN са достъпни три базирани на Cisco DNA лиценза: Cisco DNA Essentials, Cisco DNA Advantage и Cisco ONE Advantage, позволяващи на клиентите да разполагат с единно унифицирано решение, което обхваща рутерите от серията ISR4000 и съответно ASR1000 и ISR1000.

Лицензните нива са структурирани така, че да подпомагат растежа в бизнес нуждите, позволявайки на клиента да премине от основна функционалност, Cisco DNA Essentials, към пълна функционалност с Cisco DNA Advantage и разширяване, включващо оптимизация и анализ на WAN с Cisco ONE Advantage. Това осигурява пълна гъвкавост за преместване на един и същ лиценз през крайните точки въз основа на нарастващите изисквания към мрежата и сигурността, растеж на честотната лента на базата на растежа на потребителите и приложенията в сайтовете, както и възможността за промяна на управлението на платформата от офиса към облака или обратно.

Cisco DNA лицензите се поддържат за всички ISR4000 платформи, използващи Cisco DNA Център, контролера и аналитичната платформа в сърцето на базираната на намерения мрежа на Cisco. За повече информация относно Cisco DNA Center и поддържаните платформи се обърнете към
https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

Виртуализация на мрежовите функции (NFV) на предприятието с ISR4000

Създаден за намаляване на разходите, без да се компрометират жизненоважните мрежови услуги, UCS E-Series интегрирани в рутери браншови блейд сървъри предоставят поддръжка за готова за виртуализация и приложно ориентирана платформа, която може да бъде интегрирана безпроблемно в платформата ISR4000. Клиентите вече могат да инсталират виртуализирани приложения на ISR4000 рутери чрез Cisco® Enterprise NFV Infrastructure Software (NFVIS) - инфраструктура за виртуализация, която интегрира управлението на целия жизнен цикъл на VM,

мониторинг, програмируемост на устройството и верижно обслужване в един, инсталируем пакет. За повече информация относно Enterprise NFV и NFVIS, моля, вижте на https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-functions-virtualization-nfv/index.html#~stickynav=2

Поддръжка за DC захранване

Платформите ISR4000 поддържат DC и AC захранвания като опции. По-конкретно, ISR 4331 има два отделни идентификатора - ISR4331/K9 и ISR4331-DC/ K9, които поддържат съответно променлив и постоянен ток, ISR4400 може независимо да поддържа променлив или постоянен ток на едно и също шаси. Докато 4300 поддържа между 24V и 60Vdc, 4400 поддържа между 48V и 60Vdc. 4331 осигурява мощност до 250W, докато 4400 осигурява до 437W. Важно е да се отбележи, че когато на рутера са инсталирани DC захранвания, не трябва да се използват модули, базирани на PoE.

Повече подробности за DC захранване и неговите възможности можете да намерите на посочения по-долу адрес
https://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr/FRUs_Modules.html#49534

Производителност и мащабируемост на продукта

Серията Cisco 4000 е изградена върху многоядрена CPU архитектура. Тя работи с модулен софтуер Cisco IOS XE, който позволява на платформата да използва в пълна степен предимството на разпределената многоядрена архитектура. Архитектурата на Cisco 4000 разделя операциите на контролната и информационната равнина и интегрира първата за индустрията равнина на услугите. Този дизайн предоставя пълнофункционални интегрирани услуги до Слой 7 при висока производителност с възможност за предоставяне на подходящи за приложенията мрежови услуги, като същевременно поддържа стабилна платформа и високо ниво на работа в периоди на голям мрежов трафик.

ISR 4000 се състои от 3 серии рутери - серия ISR 4400, серия 4300 и серия ISR 4200, чиито нива на производителност са представени на диаграмата по-долу.

[redacted]

[redacted]

Общото за новата Серия 4000 е, че всички платформи се предлагат с фиксирани максимални нива на производителност. Едно фиксирано базово ниво на производителност се доставя като фабрично по подразбиране с опционален лиценз за производителност при поискване за увеличаване на пропускателната способност на базата. Този сценарий дава възможност за внедряване във високоскоростна WAN среда чрез лицензиране по заявка за удвояване, или за една от платформите - утрояване на капацитета на рутера без никакви хардуерни надграждания.

Всички 4000 платформи имат фиксираните нива на производителност, зададени в рамките на действителния капацитет, в резултат на което производителността не е задължително да се влошава, когато услугата е добавена в конфигурацията. Тази настройка предлага определена производителност, като елиминира предположенията на мрежовия администратор при планиране на нови услуги.

За подробна информация относно производителността и мащабируемостта на платформата от серията ISR 4000, вижте Бяла книга за ефективност на адрес https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/white-paper-c11-734550.html

Boost лиценз за ISR 4000

В допълнение към Лиценза за производителност, клиентите вече могат да поръчат Booster (или Boost) лиценз, който позволява на рутера да изпълнява между пет или повече пъти в сравнение с пропускателната способност с Лиценз за производителност. За разлика от описаната по-горе детерминирана производителност, в режим Booster рутерът не осигурява детерминираното ниво на производителност, както е предвидено при работа с лиценз по подразбиране или с лиценз за производителност.

Лицензът Boost осигурява ниво над лиценза за производителност, което позволява на клиентите напълно да премахнат ограниченията в производителността на ISR4000. Това ще накара ISR 4000 платформите да работят на изцяло нови нива, което ще позволи 4+ Gbps за IP маршрутизация (CEF) на ISR от серията 4400. За внедрявания с използване на криптиране, пропускателната способност на IPSec с AES 256 се увеличава до 250 Mbps в най-ниската платформа до 10 Gbps при ISR4461.

Поддръжка на интерфейси и модули на ISR 4000

Серията рутери (ISRs) за интегрирани услуги Cisco 4000 са модулни рутери с LAN и WAN връзка. Рутерите осигуряват слотове за мрежов интерфейсен модул (NIM) и слотове за подобрен сервизен модул (SM-X), предлагащи богат набор от модули, като LAN, WAN и безжични интерфейси плюс набор от Изчислителни машини (Compute engines) за вградени услуги.

За пълния списък на поддържаните модули от серията ISR4000 вижте Списъка с интерфейси и модули на адрес https://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/relevant-interfaces-and- modules.html.

Софтуерно дефинирана WAN със серията ISR4000

Серията ISR 4000 е оптимизирана за софтуерно дефинирана WAN (SD-WAN). За предприятията това означава, че критичните за бизнеса приложения работят по-бързо, с по-голяма надеждност и намалени оперативни разходи (OpEx). SDWAN постига това, като прави всички браншови центрове и центрове за данни да имат възможност да наблюдават, контролират, преместват и отчитат потоци от данни за приложения, като например специфичен уеб (HTTP) трафик. Серията ISR 4000 има възможност за задълбочена проверка на пакети и може точно да идентифицира и контролира хиляди различни приложения, включително клиентски вътрешни корпоративни приложения.

Цялата SD-WAN реализация върху ISR4000 може да бъде осъществена чрез управление на крайното устройство или от облака, или от офиса чрез възходящи нива на лицензи, базирани на пропускателна способност. Всички лицензи, които поддържат SD-WAN, независимо дали са офисни или в облак, са активирани чрез използване на абонаментни лицензи. Тези лицензи за абонамент дават възможност на всички клиенти безпроблемно да преминават между управление от офиса или от облак, ако е необходимо. Лицензните нива са структурирани да подпомагат растежа на бизнес нуждите чрез прости абонаменти, които помагат за опростяване на преминаването към базирани на намерения мрежи за WAN.

Абонаментите за SDWAN са представени от три лиценза за абонамент - **Cisco DNA Essentials, DNA Advantage и Cisco DNA Premier**, всеки от които е с разширена функционалност. **Cisco DNA Essentials** обхваща всички видове свързаност и управление на жизнения цикъл на рутера, поддържа видимост на мрежата и приложенията, съчетана с базова сигурност на обекта и обмена на данни. **Cisco DNA Advantage** осигурява разширени топологии на WAN, политики, ориентирани към приложенията политики, поддържани от подобрена мрежова сигурност. **Cisco DNA Premier** осигурява облачно свързване с неограничена сегментация, разширена оптимизация на приложенията и мрежови анализи с разширена защита от заплахи.

За повече информация относно Cisco SDWAN, вижте https://www.cisco.com/c/en/us/products/software/one-wan-subscription/index.html

Ползите са огромни;

1. Критичните за бизнеса приложения вече не трябва да се конкурират помежду си или с трафик, който трябва да се обслужва по най-добрия начин.
2. Корпоративната мрежа става по-надеждна, защото могат да се използват множество пътища.
3. Разходите са значително намалени, тъй като двойните MPLS връзки могат да бъдат заменени с комбинация от MPLS и Интернет.
4. Времето за въвеждане на нови отдалечени обекти драстично се намалява, тъй като SD-WAN поддържа бързо внедрявани DSL и 3G / 4G LTE връзки толкова лесно, колкото и MPLS.
5. При тези връзки сигурността е гарантирана с помощта на защитена автоматична VPN технология, използвана от правителства и финансови организации по целия свят.

От гледна точка на платформата, серията ISR 4000 има:

1. Разделени равнини за контрол и данни за вградена система за предотвратяване на атаки за Отказ на услуга (DoS) и Система за предотвратяване на проникване (IPS) и вградена защитна стена.
2. SaaS приложенията могат да имат локално кеширано съдържание. Кеширането е автоматично и се конкурира директно с технологията Akamai за получаване на информация.
3. Скоростта на действие на приложението се увеличава значително с помощта на вградена технология за ускоряване, която може да кешира локално на ниво байт.

Решения за сигурност на Cisco за серия ISR4000

Cisco WAN MACsec

Маршрутизаторите на Cisco поддържат широк спектър от непрекъснато подобрявани защитни функции на рутерите ISR4000. Cisco WAN MACsec се поддържа на рутерите от серията ISR4000, използвайки модул NIM-2GE-CU-SFP. WAN MACsec осигурява решение за криптиране на мрежова линия през транспортни услуги на Слой 2 на Ethernet и може да се използва извън мрежите на офиса, независимо дали става дума за транспортни връзки Metro Ethernet или за връзка между центрове за данни (DCI). MACsec също така осигурява WAN връзки, които използват Ethernet като носител на медия слоя за връзки. За повече информация вижте документацията на адрес https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2016/WP-WAN-MACsecDep-Aug2016.pdf

Анализ на Cisco на заплахата срещу криптирането

Бързото покачване на криптирания трафик променя пейзажа на заплахата. Тъй като все повече предприятия стават дигитални, значителен брой услуги и приложения използват криптиране като основен метод за защита на информацията. Анализът на заплахата срещу криптирането (ETA) е функция, която позволява на клиентите да правят криптографски оценки и да идентифицират злонамерени съобщения в криптиран трафик чрез пасивен мониторинг. Използването на информация за събития, които се случват вътре в потока или вътрешна поточна телеметрия за идентифициране на зловредна комуникация в криптиран трафик означава, че Анализът на заплахата срещу криптирането може да поддържа интегритета на криптирания поток, без да е необходимо групово декриптиране. За повече информация и поддръжката на платформата вижте https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network- security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf

Cisco Snort IPS и Cisco Umbrella Branch

Cisco® Snort® IPS за Серията рутери за интегрирани услуги Cisco 4000 (ISR) предлага леко решение за защита от заплахи, което използва признатата в индустрията технология с отворен код за предотвратяване на проникване Snort Intrusion Prevention System (IPS). То е перфектно за клиенти, които търсят рентабилно решение, предоставящо единно решение както за усъвършенствани възможности за маршрутизация, така и за интегрирана защита от заплахи, за да помогне спазването на регулаторните изисквания.

Cisco Umbrella Branch е облачна услуга за сигурност за Cisco рутери за интегрирани услуги (ISR). Тя осигурява първия слой на защита срещу заплахи в браншовите офиси. Освен това предлага и най-простият и бърз начин за защита на всяко устройство във вашата браншова мрежа. Вие получавате видимост и усилване на DNS слоя, така че можете да блокирате заявки към злонамерени домейни и IP адреси, преди да се осъществи връзка.

Когато активирате MACsec, ще трябва да осигурите лицензи за сигурност и HSEC, за да спазите федералните разпоредби за контрол на износа. Когато клиентите желаят да активират ETA, лицензът за сигурност (SEC) трябва да бъде активиран. Активирането на Snort се нуждае от лиценз за сигурност (SEC) и лиценз за абонамент. Активирането на Cisco Umbrella Branch се нуждае от лиценз на Umbrella Branch и лиценз за абонамент.

КП2

Намаляване на оперативните разходи с помощта на Cisco ISR

Поддръжка за моделиране на данни

Предприятията и доставчиците на услуги (SP) желаят да намалят оперативните разходи (opex) на своите мрежи и да увеличат гъвкавостта и скоростта, с която предоставят нови услуги чрез инвестиции в софтуерно дефинирани мрежи (SDN) и виртуализация на мрежовите функции (NFV). Cisco рутерите осигуряват поддръжка за Netconf и YANG моделиране на данни с увеличаване на обхвата на модела в следващите версии.

Надстройки за поддръжка на софтуера (SMU)

Сега маршрутизаторите ISR4000 осигуряват Надстройки за поддръжка на софтуера (SMU) [7]. Надстройките за поддръжка на софтуера (SMU) е пакет, който може да бъде инсталиран в система, за да предостави корекции с пачове или сигурна резолюция на изготвено изображение. SMU пакет се предоставя на базата на издание и на компонент и е специфичен за платформата. SMU е независим и самостоятелен пакет и няма никакви предпоставки или зависимости. Моля, вижте https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-16-6/config-mgmt-xe-16-6-book/cm- smu.html for additional details

Network Plug and Play

Network Plug and Play помага да се автоматизира вграждането на нови устройства във вашата мрежа чрез прилагане на конфигурационни настройки без ръчна намеса. С помощта на централно управляван контролер се намалява времето, необходимо на новото устройство да се присъедини към вашата мрежа и да стане функционално. За повече информация относно Plug and Play (PnP), моля, вижте https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/release/notes/pnp-connect-release-notes.html

Лицензиране и пакетиране на Cisco IOS софтуер

Универсално изображение на IOS XE и XE-SDWAN

С платформата се доставя единично универсално изображение на Cisco IOS XE, включващо всички функции. Разширените функции могат да бъдат разрешени чрез просто активиране на софтуерен лиценз на универсално изображение. Технологичните пакети и лицензи за функции, активирани чрез лицензи за право на използване, опростяват доставката на софтуер и намаляват оперативните разходи за внедряване на нови функции.

Началната поддръжка на IOS версия 16.9.1 SDWAN се предлага за IOS изображение рутера от серията ISR4000. Функциите SDWAN се предоставят чрез отделно изображение, XE-SDWAN изображение. Докато изображението Universal IOS-XE осигурява функции за маршрутизиране, изображението XE-SDWAN осигурява поддръжка за софтуерно-дефинирани WAN решения, базирани в офиса или облака. Унифицирани комуникации за XE-SDWAN ще се поддържат в следващите версии.

При поръчка на ISR рутер, клиентът може да избере изображение IOS-XE или XE-SDWAN. С изображение IOS-XE клиентите могат да изберат лицензиране, основаващо се на абонамент, или за вечно лицензиране. С изображение XE-SDWAN клиентите могат да поръчват само лицензиране за абонамент. Вижте ръководството за поръчка на Cisco DNA на https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/dna-center/nb-09-dna-1-x-ordering-guide-cte-en-latest.pdf.

[7] Поддържа се от IOS-XE16.6.1 за всички рутери от серията ISR4000 и ASR1000

Четири основни технологични лиценза са налични в серията Cisco 4000 и използват изображение IOS-XE; тези лицензи могат да бъдат активирани чрез процеса на активиране на Cisco софтуер, идентифициран на https://www.cisco.com/go/sa.

Налични са следните лицензи:

- IP база: Този технологичен пакет се предлага по подразбиране.
- Опит на приложение (APPX): Този лиценз включва и данни характеристики за ефективността на приложението.
- Унифицирани комуникации (UC) [8]: Този лиценз включва гласови функции.
- Сигурност (SEC) или сигурност без криптиране на полезен товар (SEC-NPE): Този лиценз включва функции за защита на мрежова инфраструктура.

Серията Cisco 4000 има лиценз за използване при поискване за увеличаване на пропускателната способност на базата без хардуерни промени. Присъства и лиценз за висока сигурност (HSEC), който премахва ограниченията, налагани от ограниченията за износ на правителството на САЩ върху броя на криптираните тунели и криптирания поток. Лицензът HSECK[9] е отделно необходим лиценз за функция, за да имате пълна крипто функционалност. Без лиценза HSECK[9] ще бъдат достъпни само 1000 сигурни тунела и крипто честотна лента от 2509 Mbps.

За допълнителна информация и подробности относно лицензирането и опаковането на софтуер на Cisco IOS софтуер за серията Cisco 4000, моля, посетете https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg.pdf.

IOS-XE осигурява поддръжка както за постоянно, така и за абонаментно лицензиране. Абонаментно лицензиране с поддръжка на Cisco DNA Център се предлага с помощта на 3-те лиценза Cisco DNA Essentials, Cisco DNA Advantage и Cisco DNA Premier в съответствие с подобни лицензи, които предоставят поддръжка от страна на XE-SDWAN. Моля, вижте ръководството за поръчка на Cisco DNA на: https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/dna-center/nb-09-dna-1-x-ordering-guide-cte-en-latest.pdf.

Софтуерно дефинираните мрежи могат да се осигурят чрез три основни лиценза на серията Cisco 4000; тези лицензи могат да бъдат активирани чрез процеса на активиране на Cisco софтуер, идентифициран на https://www.cisco.com/go/sa с помощта на Cisco DNA Център или чрез портала за управление на vManage. Изображението XE-SDWAN осигурява собствена схема за лицензиране чрез лицензирането на Cisco DNA.

Налични са следните лицензи:

- **Cisco DNA Essentials** обхваща всички видове свързаност и управление на жизнения цикъл на рутера, поддържа видимост на мрежата и приложенията, съчетана с базова сигурност на обекта и обмена на данни.
- **Cisco DNA Advantage** осигурява разширени WAN топологии, ориентирани към приложенията политики, поддържани от подобрена мрежова сигурност.
- **Cisco DNA Premier** осигурява облачно свързване с неограничена сегментация, разширена оптимизация на приложенията и мрежови анализи с разширена защита от заплахи.

За повече информация, моля, вижте на https://www.cisco.com/c/dam/en/us/products/collateral/software/dna-software- routing-subscription.pdf

[8] Унифицирани комуникации не се поддържат от ISR4221

[9] Промяната в 250Mbps беше постигната във версия 16.8.1 на IOS-XE съгласно променените федерални разпоредби

Поддръжка на смарт лицензиране на софтуер за IOS-XE

IOS-XE поддържа смарт лицензиране, като се започне с изображение на версия 16.6.1 и Device Led Conversion с версия на изображението 16.9.1.

Смарт лицензирането на софтуер е опростена система за управление на лицензи, която осигурява видимост на собствеността и потреблението на лицензи от клиента. Лицензите се управляват чрез централен облачен портал на Cisco за смарт лицензиране (CSSM). Облачният портал поддържа отчет за това какво е купил клиентът и какво използва, като по този начин предупреждава клиента, ако не отговаря на изискванията. Клиентите могат да определят какви лицензи притежават и как се използват. Клиентите се възползват от възможността да обединят наличните лицензи, като по този начин осигуряват по-лесно използване на лицензи в подобни платформи, като по този начин намаляват оперативните разходи.

Въпреки че клиентите могат да закупят съществуващи SKU, те задължително трябва да създадат Смарт акаунт, когато използват Смарт лицензиране. Един или повече виртуални акаунта могат да бъдат създадени под Смарт акаунта, за да може организацията да раздели логически закупените лицензи. Device Led Conversion (DLC) позволява на клиента да конвертира всички съществуващи PAK и RTU лицензи на рутера в Смарт лиценз. За повече информация вижте на https://www.cisco.com/c/en/us/products/software/smart-accounts/software-licensing.html.

Пакети Cisco ISR 4000

Cisco ISR 4000 се предлага в няколко атрактивни пакета. Пакетите AX интегрират лицензите Cisco Wide Area Application Services (WAAS), Сигурност (SEC) и Данни (DATA) в един пакет, който е лесен за поръчване, конфигуриране и внедряване. За клиенти, които се интересуват и от глас, заедно с всички тези функции, AXV предлага една атрактивна опция. Вижте таблица 6 за подробности.

Таблица 5. Пакети с функции на Cisco ISR 4000

Пакети	Функции
Опит в приложението с Глас (AXV)	AX + Глас
Глас със Сигурност (VSEC)	Глас + Сигурност
Опит в приложението (AX)	IP База + Сигурност + разширени мрежови протоколи: L2TPv3, BFD, MPLS, VRF, VXLAN[10] (Чест. лента <100Mbps) Опит в приложението: PfRv3, WAAS с AppNav, NBAR2, AVC, IP SLA Хибридна облачна свързаност: LISP, OTV (за чест. лента <100Mbps), VPLS, EoMPLS Смарт уеб кеширане: Akamai Connect
Глас (V)	IP База + Унифицирани комуникации: CME, SRST, CUBE
Сигурност (SEC)	IP База + Разширена сигурност: Зоново-базирани защитни стени, IPSec VPN, EZVPN, DMVPN, FlexVPN

Бележка: ISR4221/K9 не поддържа UC (Voice), следователно няма V, VSEC, AXV пакети за ISR4221/K9

Повече информация относно пакети ISR AX има на https://www.cisco.com/go/ax.

Лицензионният модел на заплащане с растежа на бизнеса ви позволява да увеличите нивото на производителност на платформите от базово ниво на по-високо ниво. Така че можете да закупите на атрактивна входна цена и да увеличите нивото на ефективност с растежа на потребностите на вашия бизнес. Таблица 7 описва лицензите за ефективност.

[10] Поддържа се само на ISR4451

A1 България ЕАД

Таблица 6. Лицензи за ефективност на Cisco ISR 4000

Платформа	Лиценза за ефективност по заявка	Функции
ISR4461	FL-4460-PERF-K9	Увеличава ефективността от основна 1,5 Gbps до 3 Gbps
ISR4451	FL-44-PERF-K9	Увеличава ефективността от основна 1 Gbps до 2 Gbps
ISR4431	FL-44-PERF-K9	Увеличава ефективността от основна 500 Mbps до 1 Gbps
ISR4351	FL-4350-PERF-K9	Увеличава ефективността от основна 200 Mbps до 400 Mbps
ISR4331	FL-4330-PERF-K9	Увеличава ефективността от основна 100 Mbps до 300 Mbps
ISR4321	FL-4320-PERF-K9	Увеличава ефективността от основна 50 Mbps до 100 Mbps
ISR4221	FL-4220-PERF-K9	Увеличава ефективността от основна 35 Mbps до 75 Mbps

Таблица 7. Лиценза за ефективност Cisco ISR 4000 Booster (boost)

Парт. номер	Описание
FL-4220-BOOST-K9 (=)	Лиценза за ефективност Booster за рутер от Серия 4220
FL-4320-BOOST-K9 (=)	Лиценза за ефективност Booster за рутер от Серия 4320
FL-4330-BOOST-K9 (=)	Лиценза за ефективност Booster за рутер от Серия 4330
FL-4350-BOOST-K9 (=)	Лиценза за ефективност Booster за рутер от Серия 4350
FL-4430-BOOST-K9 (=)	Лиценза за ефективност Booster за рутер от Серия 4430
FL-44-BOOST-K9 (=)	Лиценза за ефективност Booster за рутер от Серия 4450
FL-4460-BOOST-K9 (=)	Лиценза за ефективност Booster за рутер от Серия 4460

Информация за поръчка

Серията Cisco ISR 4000 може да бъде поръчана и доставена. За да направите поръчка, вижте Таблица 8 по-долу и посетете Cisco Ordering Home Page.

Таблица 8. Информация за поръчка на серията Cisco ISR 4000

Наименование на продукта	Описание на продукта
ISR4461/K9	Cisco ISR 4461 с 4 вградени GE, 3 NIM слота, 1 ISC слот, 3 SM слота, 8 GB флаш памет по подразбиране, 2 GB DRAM по подразбиране (равнина на данните), 4 GB DRAM по подразбиране (равнина на контрола)
ISR4451-X/K9	Cisco ISR 4451 с 4 вградени GE, 3 NIM слота, 1 ISC слот, 2 SM слота, 8 GB флаш памет по подразбиране, 2 GB DRAM по подразбиране (равнина на данните), 4 GB DRAM по подразбиране (равнина на контрола)
ISR4431/K9	Cisco ISR 4431 с 4 вградени GE, 3 NIM слота, 1 ISC слот, 8GB флаш памет по подразбиране, 2 GB DRAM по подразбиране (равнина на данните), 4 GB DRAM по подразбиране (равнина на контрола)
ISR4351/K9	ISR 4351 с 3 вградени GE, 3 NIM слота, 1 ISC слот, 2 SM слота, 4 GB флаш памет по подразбиране, 4 GB DRAM по подразбиране
ISR4331/K9	ISR 4331 с 3 вградени GE, 2 NIM слота, 1 ISC слот, 1 SM слота, 4 GB флаш памет по подразбиране, 4 GB DRAM по подразбиране
ISR4321/K9	ISR 4321 с 2 вградени GE, 2 NIM слота, 1 ISC слот, 4 GB флаш памет по подразбиране, 4 GB DRAM по подразбиране
ISR4221/K9	ISR 4221 с 2 вградени GE, 2 NIM слота, 1 ISC слот, 8 GB флаш памет по подразбиране, 4 GB DRAM по подразбиране

За допълнителни номера на продукти, включително предложенията за пакети за серията Cisco 4000, моля свържете се с местния представител на Cisco. За да направите поръчка, посетете Cisco Ordering Home Page. За да изтеглите софтуера, посетете Cisco Software Center.

Опции за миграция на рутери с интегрирани услуги

Серията Cisco ISR 4000 е включена в стандартната Cisco Програма за миграция на технологии (TMP).

Вижте https://www.cisco.com/go/tmp и Вижте на https://www.cisco.com/go/tmp и се свържете с местния представител на на Cisco за подробности относно програмата.

Гаранционна информация

Рутерите за интегрирани услуги от серията Cisco ISR 4000 имат 90-дневна гаранция с ограничена отговорност.

Cisco и партньорски услуги за браншовия офис

Услугите на Cisco и нашите сертифицирани партньори ви помагат да трансформирате опита на бранша и да ускорите бизнес иновациите и растежа. Притежаваме експертен опит да създадем ясен, възпроизвеждащ оптимизиран отпечатък в браншовите офиси за различните технологии. Услугите за планиране и проектиране привеждат в съответствие технологията с вашите бизнес цели и могат да увеличат ефективността на използването. Техническите услуги ви помагат да подобрите оперативната ефективност, да спестите пари и да намалите риска. Услугите за оптимизация ви помагат непрекъснато да подобрявате ефективността и да успеете с новите технологии. За повече информация, моля посетете https://www.cisco.com/go/services.

ФИДЕС ИНТЕРКОНСУЛТ ООД СОФИЯ

A1 България ЕАД

Техническата поддръжка на Cisco SMARTnet® за серията Cisco ISR 4000 се предлага на базата на еднократен или годишен договор. Опциите за поддръжка варират от асистенция чрез Бюро за помощ до проактивна консултация на място. Всички договори за поддръжка включват:

- Основни актуализации на Cisco IOS софтуера за подобрения в протокола, сигурността, честотната лента и функциите;
- Права за пълен достъп до техническите библиотеки на Cisco.com за техническа помощ, електронна търговия и информация за продуктите:
- Достъп 24 часа на ден до най-големия специализиран персонал за техническа поддръжка

Cisco Капитал

Гъвкави решения за плащане, които ще помогнат да постигнете вашите цели

Cisco Капитал улеснява получаването на правилната технология за постигане на вашите цели, дава възможност за трансформация на бизнеса и ви помага да останете конкурентоспособни. Можем да ви помогнем да намалите общите разходи за собственост, да запазите капитала и да ускорите растежа. В повече от 100 държави нашите гъвкави разплащателни решения могат да ви помогнат да придобиете хардуер, софтуер, услуги и допълващо оборудване на трети страни с лесни и предвидими плащания. Научи повече.

За повече информация

За повече информация относно серията Cisco ISR 4000, посетете https://www.cisco.com/go/ISR4K или се свържете с местния представител на Cisco.

История на документа

Нова или преработена тема	Описано в	Дата
Промяна 4461 от 2RU на 3RU	Раздел размери	04 декември 2018 г.
Добавени 4461 и SD-WAN		13 ноември 2018 г.
Добавена е поддръжка за Cisco SD-WAN с IOS XE SD-WAN, жерсия 16.9.1 на софтуера. Добавено Анализ на цриптирания трафик, както и информация за поддръжка на Boost Performance Licensing.	Информация за поръчка	08 август 2018 г.
Добавен е нов модел от серията ISR 4000 - ISR 4221. Актуализирани всички свързани модули, памети, лицензи и пакети, имащи отношение към ISR 4221.	Функции и предимства	23 август 2017 г.

Главен офис в Америка
Cisco Systems, Inc.
San Jose, CA

Главен офис в Азия-Тихи океан
Cisco Systems (USA) Pte. Ltd.
Singapore

Главен офис в Европа
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco има над 200 офиса по света. Номерата на телефоните и факсовете са изписани в сайта на Cisco https://www.cisco.com/go/offices.

Подписаният Огнян Петков Кирилов удостоверявам верността на извършения от мен превод от английски на български език на приложения документ – "Серия рутери за интегрирани услуги Cisco 4000". Преводът се състои от 26 (двадесет и шест) страници.

Преводач: Огнян Петков Кирилов [redacted]

„СИДЕС ИНТЕРКОНСУЛТ" ООД

cisco

Data Sheet

Cisco 4000 Family Integrated Services Router

ВЯРНО С ОРИГИНАЛА

Table of Contents

ВЯРНО С ОРИГИНАЛА

Cisco® 4000 Family Integrated Services Routers (ISRs) form an Software Defined WAN platform that delivers the performance, security, and convergence capabilities that today's branch offices need.

Product Overview

The Cisco 4000 Family Integrated Services Router (ISR) revolutionizes WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, it specifically addresses the growing need for application-aware networking in distributed enterprise sites. These locations tend to have lean IT resources. But they often also have a growing need for direct communication with both private data centers and public clouds across diverse links, including Multiprotocol Label Switching (MPLS) VPNs and the Internet.

The Cisco 4000 Family contains the following platforms: the 4461, 4451, 4431, 4351, 4331, 4321 and 4221 ISRs.

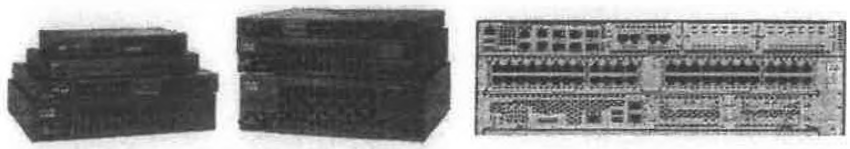


Figure 1.
Cisco 4000 Series Integrated Services Routers

Features and Benefits

Cisco 4000 Family ISRs provide you with Cisco® Software Defined WAN (SDWAN) software features and a converged branch infrastructure. Along with superior throughput, these capabilities form the building blocks of next-generation branch-office WAN solutions.

Cisco Software Defined WAN

Cisco SDWAN is a set of intelligent software services that allow you to reliably and securely connect users, devices, and branch office locations across a diverse set of WAN transport links. SDWAN-enabled routers like the ISR 4000 dynamically route traffic across the "best" link based on up-to-the-minute application and network conditions for great application experiences. You get tight control over application performance, bandwidth usage, data privacy, and availability of your WAN links - control that you need as your branches conduct greater volumes of mission-critical business.

Cisco Converged Branch Infrastructure

The Cisco 4000 Series ISRs consolidate many must-have IT functions, including network, compute, and storage resources. The high-performance, integrated routers run multiple concurrent services, including encryption, traffic management, and WAN optimization, without slowing your data throughput. And you can activate new services on demand through a simple licensing change.

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Cisco Intent Based Networking and Digital Network Architecture (Cisco DNA)

The last few years has seen a rapid transformation and adoption of digital technologies. This puts pressure on the on the Network teams supporting this changing infrastructure - especially when provisioning, managing, monitoring and troubleshooting these diverse devices. Additionally innovations such as Software Defined WAN (SDWAN), Network Function Virtualization (NFV), Open APIs and Cloud Management show great promise in transforming Organizations IT networks. This transformation raises further questions and challenges for the IT teams.

The Cisco Digital Network Architecture (Cisco DNA) is an open, extensible, software-driven architecture that provides for faster innovation, helping to generate deeper insights, and deliver exceptional experiences across many different applications. Cisco DNA relies on intent-based networking, a revolutionary approach in networking that helps organizations automate, simplify, and secure the network.

The intent-based Cisco DNA network is:

- Informed by Context: Interprets every byte of data that flows across it, resulting in better security, more customized experiences, and faster operations.
- Powered by Intent: Translates your intent into the right network configuration, making it possible to manage and provision multiple devices and things in minutes.
- Driven by Intuition: Continually learns from the massive amounts of data flowing through it and turns that data into actionable insight. Helps you solve issues before they become problems and learn from every incident.

Cisco DNA Center provides a centralized management dashboard across your entire network — the branch, campus, data center, and cloud. Rather than relying on box-by-box management, you can design, provision, and set policy end-to-end from the single Cisco DNA Center interface. This allows you to respond to organizational needs faster and to simplify day-to-day operations. Cisco DNA Analytics and Assurance and Cisco Network Data Platform (NDP) help you get the most from your network by continuously collecting and putting insights into action. Cisco DNA is open, extensible, and programmable at every layer. It integrates Cisco and third-party technology, open APIs, and a developer platform, to support a rich ecosystem of network-enabled applications.

Table 1 breaks out many of the features and benefits of the Cisco 4000 Family that create a Software Define WAN (SDWAN) and a converged branch infrastructure.

Table 1. Cisco 4000 Family ISR General Feature Highlights

Business Requirement(s)	Feature/Solution
Performance • Throughput • Service reliability	• Concurrent software services at speeds up to 2 Gbps. Backplane architecture supports high-bandwidth module-to-module communication at speeds up to 10 Gbps. • A distributed multicore architecture with the industry's first internal services plane. • Remote installation of application-aware services, which run identically to their counterparts in dedicated appliances.
Lower WAN expenditures	• Embedded SDWAN solution for creating lower-cost, business-class Internet connections.
Pay-as-you-grow • Performance upgrade model • Investment protection • CapEx budget management	• Router capacity can be increased with a remote performance-on-demand license upgrade (no hardware upgrade) for exceptional savings.
Superior and secure user application experiences	• ISR-AX "Application Experience" software bundle with advanced routing and network monitoring services. • Dynamic Multipoint VPN (DMVPN), zone-based firewalls, Intrusion Prevention (Snort & Umbrella Branch) and Content Management using Cisco Cloud Web security & OpenDNS protecting data,

ВЯРНО С ОРИГИНАЛА

Business Requirement(s)	Feature/Solution
	providing authentication credentials, and transmissions not backhauled through the data center. • Secure boot feature performs hardware-based authentication of the bootloader software to prevent malicious or unintended software from booting on the system. • Code signing verifies digital signatures of executables prior to loading to prevent execution of altered or corrupted code. • Hardware authentication protects against hardware counterfeiting by using an on-board tamper-proof silicon, including field replaceable modules. If authentication fails, the module is not allowed to boot.
IT consolidation, space savings, and improved Total Cost of Ownership (TCO)	• Single converged branch platform integrates routing, switching, virtual server, storage, security, unified communications, WAN optimization, and performance management tools.
Business continuity and increased resiliency	• ISR 4400 Series models (4461, 4451, and 4431 ISRs) support dual integrated power supplies for backup. The entire ISR 4000 Family supports optional power supply capable of delivering additional PoE power to endpoints. • Modular network interfaces with diverse connection options for load-balancing and network resiliency. • Modular interfaces with online removal and insertion (OIR) for module upgrades without network disruption. • Cisco Unified Survivable Remote Site Telephony (SRST), which serves as a resiliency complement to Cisco Hosted Collaboration Solution (HCS), a Cisco cloud-based UC service. • Support for multiple, diverse access links: T1/E1, T3/E3, Serial, xDSL, Gigabit and Ten-Gigabit Ethernet.
Lower telephony costs with VoIP and rich media experiences	• High-performance analog/digital gateway, allowing VoIP over less expensive Session Initiation Protocol (SIP) trunks. • Integrated IP PBX (Cisco Unified Communications Express) and Session Border Controller (Cisco Unified Border Element, or CUBE).
Easier manageability and support	• Single, universal software image for all features and performance-on-demand licensing flexibility. • No additional services and support needed for compute and storage. • Supported by Cisco and third-party management tools, with programmability and automation.

Platform Architecture

Table 2 lists the primary hardware architectural features and benefits of the Cisco 4000 Family. The routers run modular Cisco IOS XE Software, widely deployed in the world's most demanding networks. The software's comprehensive portfolio of services spans multiple technology areas, including security, WAN optimization, app and network Quality of Service (QoS), and embedded management.

Table 2. Architectural Highlights

Architectural Features	Benefits/Description
Multicore processors	• High-performance multicore processors support high-speed WAN connections. The data plane uses an emulated Flow Processor (FP) that delivers Application-Specific Integrated Circuit (ASIC)-like performance that does not degrade as services are added.
Embedded IP Security (IPsec) VPN hardware acceleration	• Increases scalability. When combined with an optional Cisco IOS XE Software Security license, enables WAN link security and VPN services.

ВЯРНО С ОРИГИНАЛА

Architectural Features	Benefits/Description
Integrated Gigabit Ethernet ports	• The Cisco 4000 Family provides up to four built-in 10/100/1000 Ethernet ports for WAN or LAN. • Based on the platform, some of the 10/100/1000 Ethernet ports can support Small Form-Factor Pluggable (SFP)-based connectivity in addition to RJ-45 connections, enabling fiber or copper connectivity. • Optionally, depending on the platform, up to 30W PoE+ can be enabled on two of the built-in front panel Gigabit Ethernet interfaces to provide power to external devices such as fourth-generation (4G) LTE routers. • An additional dedicated Gigabit Ethernet port is provided for device management[1].
USB-based console access	• A mini type-B USB console port[2] supports management connectivity when traditional serial ports are not available. • Traditional console and auxiliary ports are also available
Optional integrated power supply for distribution of PoE	• An optional upgrade to the internal power supply provides inline power (802.3af-compliant PoE or 802.3at-compliant PoE+) to optional integrated switch modules. • Redundant PoE conversion modules provide an additional layer of fault tolerance.
Optional integrated Redundant Power Supply (RPS)	• For the ISR 4400 Series, power redundancy is available by installing an optional integrated RPS for decreasing network downtime and protecting the network from power failures. • Optional PoE boost mode increases total PoE capacity to up to 1000W.
Cisco Enhanced Services Module (SM-X)	• Each service-module slot offers high data-throughput capability of up to 10 Gbps toward the system and up to 1 Gbps to other module slots. • Support for both single- and double-wide service modules provides flexibility in deployment options. • An SM-X slot can be converted into a Network Interface Module (NIM) slot using an optional carrier card. • Service modules support Online Insertion and Removal (OIR), avoiding network disruption when installing new or replacement modules[1].
Cisco Network Interface Modules (NIMs)[3]	• Up to three integrated NIM slots on the Cisco 4000 Family allow for flexible configurations. • Each NIM slot offers options of up to two 2Gbps connections. One towards the route processor and one for direct module to module communication. The ISR 4221 has only one 1Gbps connection to the Route Processor • NIMs support OIR. • Special NIMs add support Solid-State Drives (SSDs) and Hard Disk Drives (HDDs)[1].
Cisco Integrated Services Card (ISC) slot on motherboard	• Integrated Services Card natively supports the new Cisco High-Density Packet Voice Digital Signal Processor Modules (PVDM4s), providing greater-density rich-media voice. • Each Integrated Services Card slot connects to the system architecture through an up-to 2-Gbps link. • Future modules can be hosted on the Integrated Services Card slot, improving system functions.
Flash memory support	• A single flash memory slot is available to support high-speed storage densities, upgradable to up to 32 GB. The ISR4221 ships with a fixed 8GB Flash • Two USB type A 2.0 ports provide capabilities for convenient storage[1].

[1] Not supported on ISR4221

[2] ISR4221 supports shared Console & Auxiliary ports

[3] Unified Communications (UC) and UC based NIM's are not supported

ВЯРНО С ОРИГИНАЛА

Architectural Features	Benefits/Description
DRAM	• For the ISR 4400 Series, the default control-plane memory is 4 GB, upgradable to 16 GB to provide additional scalability for control-plane features. The default data-plane memory is 2 GB. • For the ISR 4300 Series, the default memory is 4 GB, upgradable to 16 GB (only 8GB for 4321) to provide additional scalability. • The ISR 4200 Series comes with 4GB Fixed DRAM

Managing your Cisco ISR 4000 Family ISRs

The Cisco network management applications listed at the top of Table 3 are standalone products that can be purchased or downloaded to manage your Cisco network devices. The applications are built specifically for the different operational phases; select those that best fit your needs. Those management capabilities listed under the "Cisco IOS Software XE Embedded Management" heading are directly integrated into the routers' software operating system.

Table 3. Cisco DNA Center

Operational Phase	Application	Description
Device staging and configuration	WebUI	• A GUI-based device-management tool for Cisco IOS and Cisco IOS XE Software-based access routers. This tool simplifies routing, firewall, VPN, unified communications, and WAN and LAN configuration through easy-to-use wizards.
Network-wide deployment, configuration, monitoring, and troubleshooting	Cisco Prime™ Infrastructure	• Offers comprehensive lifecycle management of wired and wireless access, campus, and branch-office networks; rich visibility into end-user connectivity, and application performance assurance. • Provides wired lifecycle functions such as inventory, configuration, and image management; automated deployment, compliance reporting, integrated best practices; and reporting.
Staging, deployment, and changes to configuration and image files	Cisco Configuration Engine	• A secure network management product that provides zero-touch image and configuration distribution through centralized, template-based management.
Context-aware security configuration and monitoring	Cisco Prime Security Manager	• Management tool for configuring and managing context-aware security. The application supports both single- and multi-device manager form factors. • Provides the ability to write and enforce the granular context-aware security policies.
Cisco Wide Area Application Service (WAAS) management	Cisco WAAS Central Manager	• The management tool for the WAAS[1]*(WAN optimization and application acceleration) integrated service. It provides a centralized mechanism for configuring WAAS features, reporting, and monitoring.

Cisco IOS XE Software Embedded Management Capabilities	
Feature	**Description**
Cisco IOS Embedded Event Manager (EEM)	• A distributed and customized approach to event detection and recovery. • Offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
Cisco IOS XE IP Service-Level Agreements (IP SLAs)	• Helps assure the performance of new business-critical IP applications as well as IP services that use data and voice in an IP network.
SNMP, Remote Monitoring (RMON), syslog, NetFlow, IP Flow Information Export (IPFix)	• Network monitoring and accounting tools.

[1] It is suggested to use AppNav with an External WAAS device for the ISR4221

Product Specifications

Table 4 lists the general product specifications for the Cisco 4000 Family routers.

Table 4. Specifications of Cisco 4000 Family Integrated Services Routers

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Aggregate Throughput (Default)	1.5Gbps	1 Gbps	500 Mbps	200 Mbps	100 Mbps	50 Mbps	35Mbps
Aggregate Throughput (Performance License)	3Gbps	2 Gbps	1 Gbps	400 Mbps	300 Mbps	100 Mbps	75 Mbps
Aggregate CEF Only[5] Throughput (Boost License)	Over 7Gbps	Over 4Gbps	Over 4Gbps	Over 2Gbps	Over 2Gbps	1.5Gbps	1.2Gbps
Total onboard WAN or LAN 10/100/1000 ports	4	4	4	3	3	2	2
Total onboard WAN or LAN 10Gbps ports	2	-	-	-	-	-	-
RJ-45-based ports	4	4	4	3	2	2	2
SFP-based ports	4	4	4	3	2	1	1

[5] Using onboard Gigabit Ethernet Interfaces

ВЯРНО С ОРИГИНАЛА

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Enhanced service-module slots	3	2	0	2	1	0	0
Doublewide service-module slots	2	1 (assumes no singlewide SM-X modules installed)	0	1 (assumes no singlewide SM-X modules installed)	0	0	0
NIM slots	3	3	3	3	2	2	2
OIR (all I/O modules)	Yes	Yes	Yes	Yes	Yes	Yes	No
Onboard ISC slot	1	1	1	1	1	1	No
Default memory double-data-rate 3 (DDR3) error-correction-code (ECC) DRAM (Combined control/services/data planes)	NA	NA	NA	4 GB	4 GB	4 GB	4GB
Maximum memory DDR3 ECC DRAM (Combined control/services/data planes)	NA	NA	NA	16 GB	16 GB	8 GB	4GB
Default memory DDR3 ECC DRAM (data plane)	4 GB	2 GB	2 GB	NA	NA	NA	NA
Maximum memory DDR3 ECC DRAM (data plane)	4 GB	2 GB	2 GB	NA	NA	NA	NA
Default memory DDR3 ECC DRAM (control/services plane)	8 GB	4 GB	4 GB	NA	NA	NA	NA

ВЯРНО С ОРИГИНАЛА

A1

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Maximum memory DDR3 ECC DRAM (control/services plane)	32 GB	16 GB	16 GB	NA	NA	NA	NA
Default flash memory	8 GB	8 GB	8 GB	4 GB	4 GB	4 GB	8GB
Maximum flash memory	32 GB	32 GB	32 GB	16 GB	16 GB	8 GB	8GB
External USB 2.0 slots (type A)	2	2	2	2	1	1	1
USB console port -type B mini (up to 115.2 kbps)	1	1	1	1	1	1	0
Serial console port - RJ45 (up to 115.2 kbps)	1	1	1	1	1	1	1 (combo CON/AUX port)
Serial auxiliary port - RJ45 (up to 115.2 kbps)	1	1	1	1	1	1	1 (combo CON/AUX port)
Power-supply options	Internal: AC, DC and PoE	Internal: AC, DC and PoE	Internal: AC, DC, and PoE	Internal: AC, DC and PoE	Internal: AC,DC and PoE	External: AC and PoE	External AC only
Redundant power supply	Internal: AC, DC and PoE	Internal: AC, DC and PoE	Internal: AC, DC, and PoE	N/A	N/A	N/A	NA
Power Specifications							
AC input voltage	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging	100 to 240 VAC autoranging
DC Input Voltage							
Input Voltage	48 – 60V	48 – 60V	48 – 60V	NA	24 – 60V	NA	NA
Input Current	12A Max	12A Max	12A Max	NA	14 - 5A	NA	NA
AC input frequency	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz
AC input current range, AC power supply (maximum)	7.1 to 3.0A	7.1 to 3.0A	3 to 1.3A	7.1 to 3.0A	3 to 1.3A	1.5 to 0.6A	1.5 to 0.6A
AC input surge current	60 A peak and less than 5 Arms per half cycle	<50 A	60 A peak and less than 5 Arms per half cycle	60 A peak and less than 12 Arms per half cycle	60 A peak and less than 5 Arms per half cycle	90 A peak and less than 3 Arms per half cycle	90 A peak and less than 3 Arms per half cycle
Typical power	[redacted]	158	65	48	42	36	24

ВЯРНО С ОРИГИНАЛА

A1 ...ария ЕАД

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
modules) (watts)							
Maximum power with AC power supply (watts)	1000W (no PoE)	450 (no PoE)	250 (no PoE)	430	250	125	90
Maximum power with DC power supply (watts)	437 (no PoE)	437 (no PoE)	437 (no PoE)	437 (no PoE)	250 (no PoE)		
Maximum power with PoE power supply (platform only) (watts)	1000 with PoE redundant 1450 with PoE boost no redundancy	1000 with PoE redundant 1450 with PoE boost no redundancy	500 with PoE redundant 1000 with PoE boost no redundancy	990	530	260	NA (No PoE Support)
Maximum endpoint PoE power available from PoE power supply (watts)	500 W with optional redundancy	500 W with optional redundancy	250 W with optional redundancy	500	250	120	NA (No PoE Support)
Maximum endpoint PoE power capacity with PoE boost (watts)	950 W no redundancy	950 W no redundancy	500 W no redundancy	N/A	N/A	N/A	NA (No PoE Support)
Sizes and Weights							
Dimensions (H x W x D)	3.5 x 17.25 x 18.5 in 88.9 x 438.15 x 469.9 mm)	3.5 x 17.25 x 18.5 in (88.9 x 438.15 x 469.9 mm)	1.73 x 17.25 x 19.97 in (43.9 x 438.15 x 507.2 mm)	3.5 x 17.25 x 18.5 in (88.9 x 438.15 x 469.9 mm)	1.75 x 17.25 x 17.25 in (44.45 x 438.15 x 438.15 mm)	1.75 x 14.55 x 11.60 in (44.55 x 369.57 x 294.64 mm)	1.72 x 12.7 x 10" (43.7 x 322.6 x 254 mm)

ВЯРНО С ОРИГИНАЛА

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
External Power Supply Dimensions (H x W x D)	N/A	N/A	N/A	N/A	N/A	2.95 x 1.18 x 6.10 in (75 x 30 x 155 mm)	37 x 73 x 152 mm (Phihong mfg PN: AA90U-120A-R) 36.5 x 67 x 155 mm (Delta mfg PN: ADP90GR BA)
Shipping Box Dimensions (H x W x D)	9.75 x 22.25 x 26 in (24.76 x 56.51 x 66.04 mm)	9.75 x 22.25 x 26 in (24.76 x 56.51 x 66.04 mm)	7.88 x 22.25 x 28.75 in (200.2 x 565.1 x 730.25 mm)	9.75 x 22.25 x 26 in (24.76 x 56.51 x 66.04 mm)	7.125 x 22.75 x 22.5 in (180.98 x 577.85 x 571.5 mm)	7.0 x 21.5 x 16.125 in (177.8 x 546.1 x 409.6 mm)	4.13 x 18.25 x 12.94" (104.9 x 463.6 x 328.7 mm)
Rack height	3 Rack Units (3RU)	2 Rack Units (2RU)	1 Rack Units (1RU)	2 Rack Units (2RU)	1 Rack Unit (1RU)	1 Rack Unit (1RU)	1 Rack Unit (1RU)
Rack-mount 19in. (48.3 cm) EIA	Included	Included	Included	Included	Included	Included	Optional
Rack-mount 23in. (58.4 cm) EIA	Optional	Optional	Optional	Optional	Optional	N/A	NA
Wall-mount	No	No	Yes	No	Yes	Mounting holes under chassis	Yes
Weight with 1, 450-WAC power supply (no modules).		28.8 lb (13.1 kg)	N/A	28.8 lb (13.1 kg)	N/A	N/A	NA
Weight with 1 1,000-WAC power supply+ 1 PoE power module (no other modules)		30.6 lb (13.9 kg)	N/A	29.0 lb (13.2 kg)	N/A	N/A	NA
Weight with AC PS (no modules)		N/A	18.5 lb (8.4 kg)	N/A	13.5 lb (6.2 kg)	7.7 lb (3.5 kg) + 1.2 lb (0.66 kg) external PS	7.1 lb (3.22kg)
Weight with DC PS (no modules)		28.8lb (13.1kg)	28.8lb (13.1kg)	28.8lb (13.1kg)	13.5 lb (6.2 kg)		
Weight with AC PS with POE (no modules)		N/A	18.6 lb (8.4 kg)	N/A	14.1 lb (6.4 kg)	N/A	NA
Typical weight (fully loaded with modules)		42.7 lb (19.4 kg)	22.4 lb (10.2 kg)	37.7 lb (17.1 kg)	16.1 lb (7.3 kg)	9.14 lb (4.2 kg) + 1.2 lb (0.66 kg) external PS	8.11 lb (3.68kg)
Packaging	[redacted]	6.4 lb (2.9 kg)	5.9 lb (2.7 kg)	6.4 lb (2.9 kg)	4.6 lb (2.1 kg)	2.2 lb (1 kg)	1.28 lb (0.58kg)

ВЯРНО С ОРИГИНАЛА

A1 [redacted] ЕАД [redacted] КП 2

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Weight							
Airflow	I/O side to bezel side	I/O side to bezel side	I/O side to bezel side	I/O side to bezel side	I/O side to bezel side	Right I/O side to Left I/O side	I/O side to bezel side
MTBF (Hours)	480770	480770	512970	566310	587250	593270	593270
Environmental Specifications							
Operating Conditions							
Temperature	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)	32 to 104°F (0 to 40°C)
Altitude (China)	0 – 6,560 ft. (0 – 2,000 m)	0 – 6,560 ft. (0 – 2,000 m)	0 – 6,560 ft. (0 – 2,000 m)	0 – 6,560 ft. (0 – 2,000 m)	0 – 6,560 ft. (0 – 2,000 m)	0 – 6,560 ft. (0 – 2,000 m)	0 – 6,560 ft. (0 – 2,000 m)
Altitude (Rest of the world)	0 – 10,000 ft. (0 – 3,050 m)	0 – 10,000 ft. (0 – 3,050 m)	0 – 10,000 ft. (0 – 3,050 m)	0 – 10,000 ft. (0 – 3,050 m)	0 – 10,000 ft. (0 – 3,050 m)	0 – 10,000 ft. (0 – 3,050 m)	0 – 10,000 ft. (0 – 3,050 m)
Short Term Temperature upto 6560ft per NEBS GR-63-CORE	NA	NA	NA	NA	32° to 131° (0° to 55° C) (for ISR4331-DC version)	NA	NA
Relative humidity	5% to 85%	5% to 85%	5% to 85%	5% to 85%	5% to 85%	5% to 85%	5% to 85%
Short-term humidity	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air	5% to 90%, not to exceed 0.024 kg water/kg of dry air
Acoustics: Sound pressure (Typical/ maximum)	50.6/73.1 dBA	50.6/73.1 dBA	54.3/79.1 dBA	50.6/73.1 dBA	52.8/74.8 dBA	24.2/51.9 dBA	28.5/53 dBA

ВЯРНО С ОРИГИНАЛА

A1 я ЕАД

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
Acoustics: Sound power (Typical/ maximum)	58.2/78.8 dBA	58.2/78.8 dBA	57.2/80.8 dBA	58.2/78.8 dBA	61.2/81.6 dBA	31.9/59.9 dBA	41 / 68 dBA
Nonoperating Conditions							
Temperature	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)
Relative humidity	5% to 95%	5% to 95%	5% to 95%	5% to 95%	5% to 95%	5% to 95%	5% to 95%
Altitude	15,584 ft (4750m)	15,584 ft (4750m)	15,584 ft (4750m)	15,584 ft (4750m)	15,584 ft (4750m)	15,584 ft (4750m)	15,584 ft (4750m)
Regulatory and Compliance							
Safety	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1	UL 60950-1 CAN/CSA C22.2 No. 60950-1 EN 60950-1 AS/NZS 60950-1 IEC 60950-1
EMC	47 CFR, Part 15 ICES-003 Class A EN55032 Class A CISPR32 Class A AS/NZS CISPR 32 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 KN22, KN24	47 CFR, Part 15 ICES-003 Class A EN55032 Class A CISPR32 Class A AS/NZS CISPR 32 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 KN22, KN24	47 CFR, Part 15 ICES-003 Class A EN55032 Class A CISPR32 Class A AS/NZS CISPR 32 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 KN22, KN24	47 CFR, Part 15 ICES-003 Class A EN55032 Class A CISPR32 Class A AS/NZS CISPR 32 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 KN22, KN24	47 CFR, Part 15 ICES-003 Class A EN55032 Class A CISPR32 Class A AS/NZS CISPR 32 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 KN22, KN24 EN 50121-1 EN61000-6-4 EN 50121-4	ICES-003 Class A EN55032 Class A CISPR32 Class A AS/NZS CISPR 32 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 KN22, KN24	ICES-003 Class A EN55032 Class A CISPR32 Class A AS/NZS CISPR 32 Class A VCCI V-3 CNS 13438 EN 300-386 EN 61000 (Immunity) EN 55024, CISPR 24 KN22, KN24
Telecom	T1 IC CS-03:2004	T1 IC CS-03:2004 TIA-968-	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101	TIA-968-B CS-03 ANSI T1.101

ВЯРНО С ОРИГИНАЛА

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
	TIA-968-B:2009 HKTA 2028:2010 HKTA 2017:2010 HKTA 2015: 2006 G.703:2001 ID0002:2007 IS6100:2004 DSPR Gray Book:2000 DSPR Technical Condition: 2004 E1 AS/ACIF S016: 2001 AS/ACIF S038: 2001 G.703:2001 TBR 4:1995 TBR 12:1993 TBR 13:1996 RRA 2009-38 (RRL 2005-96) IDA TS DLCN:2011 IDA TS ISDN PRA:2005 IS6100: 2004 PTC 220:2008 Ethernet IEEE 802.3 ANSA X3.263	B:2009 HKTA 2028:2010 HKTA 2017:2010 HKTA 2015: 2006 G.703:2001 ID0002:2007 IS6100:2004 DSPR Gray Book:2000 DSPR Technical Condition: 2004 E1 AS/ACIF S016: 2001 AS/ACIF S038: 2001 G.703:2001 TBR 4:1995 TBR 12:1993 TBR 13:1996 RRA 2009-38 (RRL 2005-96) IDA TS DLCN:2011 IDA TS ISDN PRA:2005 IS6100: 2004 PTC 220:2008 Ethernet IEEE 802.3 ANSA X3.263	ITU-T G.823, G.824 IEEE 802.3 RTTE Directive Homologation requirements vary by country and interface type. For specific country information, refer to the online approvals data base at: https://www.ciscofax.com/.	ITU-T G.823, G.824 IEEE 802.3 RTTE Directive Homologation requirements vary by country and interface type. For specific country information, refer to the online approvals data base at: https://www.ciscofax.com/.	ITU-T G.823, G.824 IEEE 802.3 RTTE Directive Homologation requirements vary by country and interface type. For specific country information, refer to the online approvals data base at: https://www.ciscofax.com/.	ITU-T G.823, G.824 IEEE 802.3 RTTE Directive Homologation requirements vary by country and interface type. For specific country information, refer to the online approvals data base at: https://www.ciscofax.com/	ITU-T G.823, G.824 IEEE 802.3 RTTE Directive Homologation requirements vary by country and interface type. For specific country information, refer to the online approvals data base at: https://www.ciscofax.com/.

Cisco IOS XE Software	
Protocols	IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Technical Specifications	Cisco 4461	Cisco 4451	Cisco 4431	Cisco 4351	Cisco 4331	Cisco 4321	Cisco 4221
	Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), RSVP, CDP, ERSPAN, IPSLA, Call Home, EEM, IKE, ACL, EVC, DHCP, FR, DNS, LISP, OTV[6], HSRP, RADIUS, AAA, AVC, Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IP sec, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE802.1ag, and IEEE802.3ah						
Encapsulations	Generic routing encapsulation (GRE), Ethernet, 802.1q VLAN, Point-to-Point Protocol (PPP), Multilink Point-to-Point Protocol (MLPPP), Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16), High-Level Data Link Control (HDLC), Serial (RS-232, RS-449, X.21, V.35, and EIA-530), and PPP over Ethernet (PPPoE)						
Traffic management	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing, and NBAR.						
Cryptographic Algorithms	Encryption: DES, 3DES, AES-128 or AES-256 (in CBC and GCM modes); Authentication: RSA (748/1024/2048 bit), ECDSA (256/384 bit); Integrity: MD5, SHA, SHA-256, SHA-384, SHA-512						

Services plane: Enabling the Branch-in-a-Box

All Cisco ISR 4000 routers contain processing cores built-in as standard to allow full-featured services to run on-board. This includes the full-featured Cisco WAAS engine that provides application acceleration and highly responsive virtual desktop experience. The technology is known as Cisco Service Containers and it uses a standard hypervisor to allow x64 based applications to run.

The 4000 series routers can be fitted with Solid State Drives (SSD) and server cards for local storage and computing capability. The Cisco UCS-E server cards are available with 8-core Intel Xeon processors with up to 48GB of high speed DDR3 memory and three drives built in offering RAID 0, 1 and 5. This immense amount of compute power can eliminate the need for any dedicated servers at branch sites. UCS-E cards can be configured and managed using VMware vCenter and pooled with Data Center compute resources.

[6] Supported only on the 4451 for Bandwidths <100Mbps

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Software Subscription through Cisco DNA Licensing

The ISR4000 series supports software based subscription using Cisco DNA based licensing. Three Cisco DNA based software subscription licenses are available for the WAN portfolio: Cisco DNA Essentials, Cisco DNA Advantage and Cisco ONE Advantage allowing customers to have a single unified solution that spans across the ISR4000 series routers and its ASR1000 and ISR1000 counterparts

The license tiers are structured to support the growth in business needs enabling the customer to move from basic functionality using the Cisco DNA Essentials to full-functionality with the Cisco DNA Advantage and expanding that to include WAN Optimization and Analytics on the Cisco ONE Advantage. This provides complete flexibility to move the same license across end-points based on growing network and security requirements, growth in bandwidth based on user and application growth at the sites as also the ability to change the management of the platform from on-prem to cloud or vice-versa.

Cisco DNA Licenses are supported for all ISR4000 platforms using the Cisco DNA Center, the controller and analytics platform at the heart of Cisco's intent-based network. For more information on the Cisco DNA Center and supported platforms, please refer to https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html

Enterprise NFV on ISR4000

Built to reduce costs without compromising vital network services, the UCS E-Series router-integrated branch blade servers provide support for a Virtualization-ready and Application-centric platform that can be seamlessly integrated on the ISR4000 platform. Customers can now install virtualized applications on the ISR4000 routers through the Cisco® Enterprise NFV Infrastructure Software (NFVIS) – a virtualization infrastructure that integrates full VM lifecycle management, monitoring, device programmability, and service chaining in a single, installable package. For more information on Enterprise NFV and NFVIS, please refer to the link at https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-functions-virtualization-nfv/index.html#~stickynav=2

Support for DC Power

ISR4000 platforms support both DC and AC Power Supplies as options. Specifically, the ISR 4331 has two separate product SKU's – the ISR4331/K9 and the ISR4331-DC/K9 which support AC and DC Power respectively, The ISR4400 can independently support an AC or a DC Power supply on the same chassis. While the 4300 supports between 24V and 60Vdc, the 4400 supports between 48V and 60Vdc. The 4331 provides for upto 250W of power rating while the 4400 provides upto 437W. It is important to note that when DC Power supplies are installed on the router, PoE based modules may not be used.

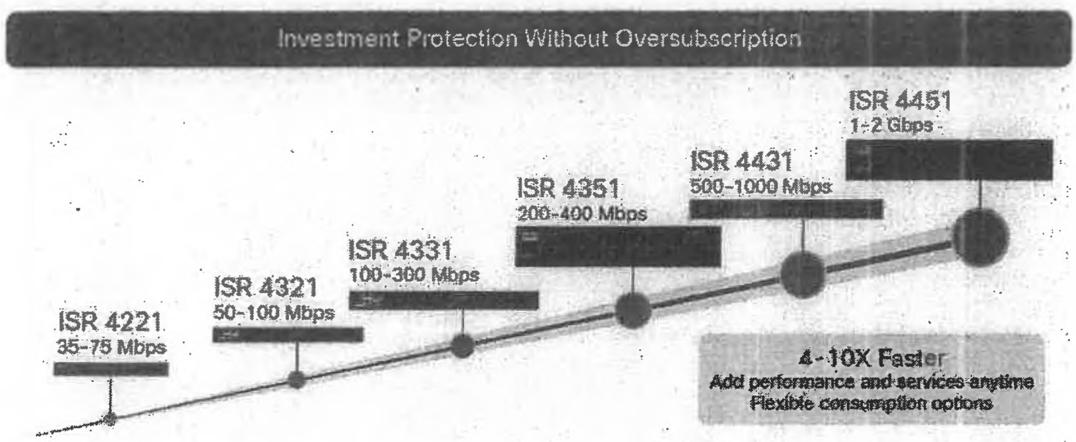
More details about the DC Power supplies and its capabilities can be found at the below url https://www.cisco.com/c/en/us/td/docs/routers/access/4400/hardware/installation/guide4400-4300/C4400_isr/FRUs_Modules.html#49534

Product Performance and Scalability

The Cisco 4000 Family is built on a multicore CPU architecture. It runs modular Cisco IOS XE Software, which allows the platform to use to full advantage a distributed multicore architecture. The architecture of the Cisco 4000 separates control- and data-plane operations and integrates an industry-first services plane. This design delivers full-featured integrated services up to Layer 7 at high performance with the ability to deliver application-aware network services while maintaining a stable platform and a high level of performance during periods of heavy network traffic.

The ISR 4000 consists of 3 series of Routers – the ISR 4400 series, the 4300 series and ISR 4200 series whose performance levels maybe represented by the chart below

ВЯРНО С ОРИГИНАЛА



Common for the new 4000 Family is that all platforms come with fixed maximum performance levels. One fixed base performance level is delivered as factory default with an optional performance-on-demand license to increase the base forwarding throughput. This scenario enables deployment in high-speed WAN environments through performance-on-demand licensing to double or, for one of the platforms, triple the router capacity without any hardware upgrades.

All 4000 platforms have their fixed performance levels set well within actual capacity, with the result that performance does not necessarily degrade when a service is added to the configuration. This setup provides a deterministic performance, eliminating a network administrator's guesswork when planning for new services.

For a more detailed document on ISR 4000 Series Performance and Platform Scalability, please refer to the Performance Whitepaper at https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/white-paper-c11-734550.html

ISR 4000 Boost License

In addition to the Performance License, customers may now order a Booster (or Boost) License that allows the router to perform between five or more times than that of the throughput with Performance License. In contrast to the deterministic performance described above, in the Booster mode, the router does not provide the deterministic level of performance as provided when operating with the default license or with the Performance license.

The Boost License provides a license tier above the Performance License allowing customers to completely remove the ISR4000's performance limiters. This will make the ISR 4000 platforms perform at entirely new performance levels, allowing for 4+ Gbps of IP Routing (CEF) performance on the 4400 series ISRs. For deployments using encryption, IPSec throughput with AES 256 increases to 250Mbps on the lowest platform up to 10Gbps on the ISR4461.

ВЯРНО С ОРИГИНАЛА

ISR 4000 Interfaces and Modules Support

The Cisco 4000 Series Integrated Services Routers (ISRs) are modular routers with LAN and WAN connectivity. The routers provide for Network Interface Module (NIM) slots and Enhanced service module (SM-X) slots offering a rich set of Modules, such as LAN, WAN and Wireless Interfaces plus a range of Compute engines for embedded services

For the complete list of supported modules on the ISR4000 Series refer to the Interfaces and Modules sheet at https://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/relevant-interfaces-and-modules.html.

Software defined WAN with the ISR4000 Series

The ISR 4000 series is optimized for the Software Defined WAN (SD-WAN). For enterprises this means that business critical applications run faster, with more reliability and reduced Operational Expenditure (OpEx). The SDWAN achieves this by making all branches and Data Centers have the ability to monitor, control, move and report on streams of application data such as specific web (HTTP) traffic for example. The ISR 4000 series has deep packet inspection capability and can accurately identify and control thousands of different applications including custom in-house enterprise applications.

The entire SD-WAN implementation on the ISR4000 is maybe implemented by managing the end device either from the Cloud or On-Premise through ascending levels of throughput based licenses. All licenses that support SD-WAN, whether On-Premise or on Cloud are all enabled using Subscription Licenses. These subscription licenses enable all customers to seamlessly transition between On-Premise and Cloud management as needed. The license tiers are structured to support the growth in business needs through simple subscriptions that help simplify the journey to intent-based networking for the WAN.

The SDWAN subscriptions are aligned across three subscription licenses of **Cisco DNA Essentials, DNA Advantage and Cisco DNA Premier,** each expanding functionally. The **Cisco DNA Essentials** covers all types of connectivity & router life cycle management, support for Network & application visibility coupled with basic premise and transport security. The **Cisco DNA Advantage** provides for Advanced WAN topologies, Application aware policies supported by enhanced network security. The **Cisco DNA Premier** provides for Cloud connectivity with unlimited segmentation, Advanced Application optimization & Network Analytics, secured by advanced threat protection

For more information on Cisco SDWAN please refer to https://www.cisco.com/c/en/us/products/software/one-wan-subscription/index.html

The benefits are immense;

1. Business-critical applications no longer have to contend each other or with traffic that should be served on best effort basis.
2. The Enterprise network becomes more reliable because multiple paths can be used.
3. Costs are greatly reduced because dual MPLS links can be replaced with a mix of MPLS and Internet.
4. The time to bring up new remote sites is dramatically reduced because the SD-WAN supports rapidly deployed DSL and 3G/4G LTE connections as easily as MPLS.
5. Security is assured across these connections using a zero-touch secure VPN technology used by governments and finance organizations worldwide.

ВЯРНО С ОРИГИНАЛА

From a platform perspective, the ISR 4000 series has

1. Separated control and data planes for Denial of Service (DoS) attack prevention and Intrusion Prevention System (IPS) and firewall capability built-in.
2. SaaS applications can have content locally cached. The caching is automatic and peers directly with Akamai technology to obtain intelligence.
3. Application performance speed is greatly increased using in-built application acceleration technology that can locally cache at a byte-level.

Cisco Security Solutions for the ISR4000 Series

Cisco WAN MACsec,

Cisco routers support a wide-range of ever enhancing security features on the ISR4000 routers. Cisco WAN MACsec is supported on the ISR4000 series routers using the NIM-2GE-CU-SFP module. WAN MACsec provides a line-rate network encryption solution over Layer 2 Ethernet transport services and can be leveraged outside campus networks, whether it be over Metro Ethernet transport or Data Center Interconnect (DCI) links. MACsec also secures WAN connections that are leveraging Ethernet as the link-layer media. For more information refer to the whitepaper at https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2016/WP-WAN-MACsecDep-Aug2016.pdf

Cisco Encrypted Threat Analytics

The rapid rise in encrypted traffic is changing the threat landscape. As more businesses become digital, a significant number of services and applications are using encryption as the primary method of securing information. Encrypted Threat Analytics (ETA) is a functionality that allows customers to do cryptographic assessments and identify malware communications in encrypted traffic through passive monitoring. Using information about events that occur inside of a flow or intraflow telemetry to identify malware communication in encrypted traffic means Encrypted Traffic Analytics can maintain the integrity of the encrypted flow without the need for bulk decryption. For more information and platform support refer to https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf

Cisco Snort IPS and Cisco Umbrella Branch

Cisco® Snort® IPS for Cisco 4000 Series Integrated Services Routers (ISRs) offers a lightweight threat defense solution that uses industry-recognized Snort open-source Intrusion Prevention System (IPS) technology. It is perfect for customers who are looking for a cost-effective solution that provides one box for both advanced routing capabilities and integrated threat defense security to help comply with regulatory requirements.

Cisco Umbrella Branch is a cloud-delivered security service for the Cisco Integrated Services Router (ISR). It provides the first layer of defense against threats at branch offices. And it offers the simplest, fastest way to protect every device on your branch network. You gain visibility and enforcement at the DNS layer, so you can block requests to malicious domains and IPs before a connection is ever made.

When enabling MACsec, you will need to procure the Security and HSEC licenses to stay within the limits of federal export control regulations. When customers wish to enable ETA, the Security (SEC) license needs to be enabled. Enabling Snort needs a Security (SEC) license and a signature subscription license. Enabling Cisco Umbrella Branch needs an Umbrella Branch license and a subscription license.

Reducing Operational Costs using Cisco ISR

Support for Data Modelling

Enterprises and Service Providers (SP's) wish to drive down the operational cost (opex) of their networks and increase the agility and speed with which they deliver new services furthered by investments in Software Defined Networking (SDN) and Network Function Virtualization (NFV). Cisco routers provide support for Netconf and YANG data-modelling with increasing model coverage in successive releases

Software Maintenance Upgrades (SMU)

The ISR4000 routers now support Software Maintenance Upgrades (SMU)[7]. The Software Maintenance Upgrade (SMU) is a package that can be installed on a system to provide a patch fix or security resolution to a released image. An SMU package is provided on a per release and per component basis and is specific to the platform. An SMU is an independent and self-sufficient package and it does not have any prerequisites or dependencies. Please refer to https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/config-mgmt/configuration/xe-16-6/config-mgmt-xe-16-6-book/cm-smu.html for additional details

Network Plug and Play

Network Plug and Play helps automate the onboarding of new devices on your network by applying configuration settings without manual intervention. With the ease of a centrally managed controller, it reduces the time a new device takes to join your network and become functional. For more information on Plug and Play (PnP), please refer to https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/release/notes/pnp-connect-release-notes.html

Cisco IOS Software Licensing and Packaging

Universal IOS XE and XE-SDWAN Image

A single Cisco IOS XE Universal image encompassing all functions is delivered with the platform. Advanced features can be enabled by simply activating a software license on the Universal image. Technology packages and feature licenses, enabled through right-to-use licenses, simplify software delivery and decrease the operational costs of deploying new features.

Beginning IOS version 16.9.1, SDWAN support is provided for IOS image on the ISR4000 series router. The SDWAN features are provisioned through a separate image, the XE-SDWAN image. While the Universal IOS-XE image provides for routing features, the XE-SDWAN image provides support for OnPrem or Cloud based Software Defined WAN solutions. Unified Communications for XE-SDWAN will be supported in upcoming releases

When ordering an ISR router, a customer may choose either of IOS-XE or XE-SDWAN image. With IOS-XE image, customers may opt for subscription based licensing or for perpetual licensing. With XE-SDWAN image, customers may order only subscription licensing. Refer to Cisco DNA Ordering Guide at https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/dna-center/nb-09-dna-1-x-ordering-guide-cte-en-latest.pdf.

[7] Supported from IOS-XE16.6.1 for all ISR4000 and ASR1000 series routers

ВЯРНО С ОРИГИНАЛА

A1 ... ария ЕАД

Four major technology licenses are available on the Cisco 4000 Family and use the IOS-XE image; these licenses can be activated through the Cisco software activation process identified at https://www.cisco.com/go/sa. The following licenses are available:

- IP Base: This technology package is available as default.
- Application Experience (APPX): This license includes data and application performance features.
- Unified Communications (UC)[8]: This license includes voice features.
- Security (SEC) or Security with No Payload Encryption (SEC-NPE): This license includes features for securing network infrastructure.

The Cisco 4000 Series has a performance-on-demand license to increase the base forwarding throughput with no hardware changes. Also present is the High Security (HSEC) license, which removes the curtailment enforced by the U.S. government export restrictions on the encrypted tunnel count and encrypted throughput. The HSECK9 license is a separately required license for a feature to have full crypto functionality. Without the HSECK9 license, only 1000 secure tunnels and 250[9] Mbps of crypto bandwidth would be available.

For additional information and details about Cisco IOS Software licensing and packaging on the Cisco 4000 Family, please visit https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg.pdf.

IOS-XE provides support for both perpetual and subscription licensing. Subscription Licensing with support for Cisco DNA Center is offered using the 3-Licenses of Cisco DNA Essentials, Cisco DNA Advantage and Cisco DNA Premier in-line with similar licenses that provide support on the XE-SDWAN side. Please refer to Cisco DNA Ordering Gide at: https://www.cisco.com/c/dam/en/us/products/collateral/cloud-systems-management/dna-center/nb-09-dna-1-x-ordering-guide-cte-en-latest.pdf.

Software Defined Networks maybe provisioned through three major licenses on the Cisco 4000 Family; these licenses can be activated through the Cisco software activation process identified at https://www.cisco.com/go/sa using the Cisco DNA Center or through the vManage management portal. The XE-SDWAN image provides for its own licensing schema through the Cisco DNA Licensing

The following licenses are available:

- **Cisco DNA Essentials** covers all types of connectivity & router life cycle management, support for Network & application visibility coupled with basic premise and transport security
- **Cisco DNA Advantage** provides for Advanced WAN topologies, Application aware policies supported by enhanced network security
- The **Cisco DNA Premier** provides for Cloud connectivity with unlimited segmentation, Advanced Application optimization & Network Analytics, secured by advanced threat protection

For more information please refer to https://www.cisco.com/c/dam/en/us/products/collateral/software/dna-software-routing-subscription.pdf

[redacted]

[8] Unified Communications is not supported by ISR4221

[9] The change to 250Mbps was achieved in the IOS-XE version 16.8.1 pursuant to revised Federal regulations

ВЯРНО С ОРИГИНАЛА

А1 България ЕАД [redacted]

[redacted]

Smart Software Licensing Support for IOS-XE

IOS-XE supports Smart Licensing beginning with image version 16.6.1 and Device Led Conversion with image version 16.9.1. Smart Software licensing is a simplified license management system that delivers visibility into customer license ownership and consumption. Licenses are managed through a central Cisco Smart License cloud portal (CSSM). The cloud portal maintains an account of what the customer has bought and what they are using, thus alerting the customer if they go out of compliance. Customers can determine what licenses they own and how they are being used. Customers benefit from being able to pool available licenses thus providing for a more straightforward license usage across like-platforms, thus decreasing operational costs.

While customers can purchase existing SKU's, they must mandatorily create a Smart Account when implementing Smart Licensing. One or more Virtual Accounts maybe created under the Smart Account to enable the organization to logically segregate the purchased licenses. Device Led Conversion (DLC) allows the customer to convert all existing PAK and RTU licenses on the router into a Smart License. For more information, refer to the link at https://www.cisco.com/c/en/us/products/software/smart-accounts/software-licensing.html.

Cisco ISR 4000 Bundles

Cisco ISR 4000 is available is several attractive bundles. The AX bundles integrate Cisco Wide Area Application Services (WAAS), Security (SEC), and Data (DATA) licenses into a single bundle that is simple to order, configure, and deploy. For customers who are also interested in voice along with all of these features, AXV presents an attractive option. See Table 6 for details.

Table 5. Cisco ISR 4000 Feature Bundles

Bundles	Features
Application Experience with Voice (AXV)	AX + Voice
Voice with Security (VSEC)	Voice + Security
Application Experience (AX)	IP Base + Security + advanced networking protocols: L2TPv3, BFD, MPLS, VRF, VXLAN[10] (Bandwidth <100Mbps) Application Experience: PfRv3, WAAS with AppNav, NBAR2, AVC, IP SLA Hybrid Cloud Connectivity: LISP, OTV (for Bandwidth <100Mbps), VPLS, EoMPLS Intelligent Web Caching: Akamai Connect
Voice (V)	IP Base + Unified Communications: CME, SRST, CUBE
Security (SEC)	IP Base + Advanced Security: Zone Based Firewall, IPSec VPN, EZVPN, DMVPN, FlexVPN

Note: ISR4221/K9 does not support UC (Voice), hence no V, VSEC, AXV bundles for ISR4221/K9

More information on ISR AX bundles is available at https://www.cisco.com/go/ax.

A pay-as-you-grow licensing model lets you increase the performance level for the platforms from the base level to a higher level. So you can purchase at an attractive entry-level price point and increase the performance level as your business demand grows. Table 7 describes the performance licenses.

[10] Supported only on the ISR4451

ВЯРНО С ОРИГИНАЛА

A1 ... ЕАД

Table 6. Cisco ISR 4000 Performance Licenses

Platform	Performance-on-Demand License	Features
ISR4461	FL-4460-PERF-K9	Increases the performance from base performance 1.5 Gbps to 3 Gbps
ISR4451	FL-44-PERF-K9	Increases the performance from base performance 1 Gbps to 2 Gbps
ISR4431	FL-44-PERF-K9	Increases the performance from base performance 500 Mbps to 1 Gbps
ISR4351	FL-4350-PERF-K9	Increases the performance from base performance 200 Mbps to 400 Mbps
ISR4331	FL-4330-PERF-K9	Increases the performance from base performance 100 Mbps to 300 Mbps
ISR4321	FL-4320-PERF-K9	Increases the performance from base performance 50 Mbps to 100 Mbps
ISR4221	FL-4220-PERF-K9	Increases the performance from base performance 35 Mbps to 75 Mbps

Table 7. Cisco ISR 4000 Booster (boost) Performance Licenses

Part number	Description
FL-4220-BOOST-K9 (=)	Booster Performance License for 4220 Series Router
FL-4320-BOOST-K9 (=)	Booster Performance License for 4320 Series Router
FL-4330-BOOST-K9 (=)	Booster Performance License for 4330 Series Router
FL-4350-BOOST-K9 (=)	Booster Performance License for 4350 Series Router
FL-4430-BOOST-K9 (=)	Booster Performance License for 4430 Series Router
FL-44-BOOST-K9 (=)	Booster Performance License for 4450 Series Router
FL-4460-BOOST-K9 (=)	Booster Performance License for 4460 Series Router

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Ordering Information

The Cisco ISR 4000 Family is orderable and shipping. To place an order, refer to Table 8 below and visit the Cisco Ordering Home Page.

Table 8. Cisco ISR 4000 Series Ordering Information

Product Name	Product Description
ISR4461/K9	Cisco ISR 4461 with 4 onboard GE, 3 NIM slots, 1 ISC slot, 3 SM slots, 8 GB Flash Memory default, 2 GB DRAM default (data plane), 4 GB DRAM default (control plane)
ISR4451-X/K9	ISR 4451 with 4 onboard GE, 3 NIM slots, 1 ISC slot, 2 SM slots, 8 GB Flash Memory default, 2 GB DRAM default (data plane), 4 GB DRAM default (control plane)
ISR4431/K9	ISR 4431 with 4 onboard GE, 3 NIM slots, 1 ISC slot, 8GB Flash Memory default, 2 GB DRAM default (data plane), 4 GB DRAM default (control plane)
ISR4351/K9	ISR 4351 with 3 onboard GE, 3 NIM slots, 1 ISC slot, 2 SM slots, 4 GB Flash Memory default, 4 GB DRAM default
ISR4331/K9	ISR 4331 with 3 onboard GE, 2 NIM slots, 1 ISC slot, 1 SM slots, 4 GB Flash Memory default, 4 GB DRAM default
ISR4321/K9	ISR 4321 with 2 onboard GE, 2 NIM slots, 1 ISC slot, 4 GB Flash Memory default, 4 GB DRAM default
ISR4221/K9	ISR 4221 with 2 onboard GE, 2 NIM slots, 1 ISC slot, 8 GB Flash Memory default, 4 GB DRAM default

For additional product numbers, including the Cisco 4000 Family bundle offerings, please contact your local Cisco account representative. To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center.

Integrated Services Router Migration Options

The Cisco ISR 4000 Family is included in the standard Cisco Technology Migration Program (TMP). Refer to https://www.cisco.com/go/tmp and contact your local Cisco account representative for program details.

Warranty Information

The Cisco ISR 4000 Series Integrated Services Routers have a 90-day limited liability warranty.

Cisco and Partner Services for the Branch Office

Services from Cisco and our certified partners help you transform the branch-office experience and accelerate business innovation and growth. We have the expertise to create a clear, replicable, optimized branch-office footprint across technologies. Planning and design services align technology with your business goals and can increase deployment efficiency. Technical services help you improve operational efficiency, save money, and mitigate risk. Optimization services help you continuously improve performance and succeed with new technologies. For more information, please visit https://www.cisco.com/go/services.

ВЯРНО С ОРИГИНАЛА

A1

Cisco SMARTnet® technical support for the Cisco ISR 4000 Family is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation. All support contracts include:

- Major Cisco IOS Software updates for protocol, security, bandwidth, and feature improvements
- Full access rights to Cisco.com technical libraries for technical assistance, electronic commerce, and product information
- Access 24 hours a day to the industry's largest dedicated technical support staff

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For More Information

For more information about the Cisco ISR 4000 Family, visit https://www.cisco.com/go/ISR4K or contact your local Cisco account representative.

Document History

New or revised topic	Described In	Date
Change 4461 from 2RU to 3RU	Sizing Section	December 4, 2018
Added 4461 and SD-WAN		November 13, 2018
Added support for Cisco SD-WAN with IOS XE SD-WAN, 16.9.1 software release. Added Encrypted Traffic Analytics as well as Boost Performance Licensing support information.	Ordering Information	August 8, 2018
Added new ISR 4000 Series model, the ISR 4221. Updated all related modules, memory, licenses and bundles support related to the ISR 4221.	Features and Benefits	August 23, 2017

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

Превод от английски език

CISCO
Мост към възможното

Информационен лист
Cisco публичен

Рутери за агрегирани услуги Cisco Серия ASR 1000

София 1504, ул. "Св. Климент Охридски" №4
тел.: 02/ 946 13 92; тел./факс: 02/ 943 86 65
e-mail: office@fides.bg
www.fides.bg

Съдържание

Преглед на продукта

Рутерите за агрегиране на Cisco® Серия ASR 1000 осигуряват WAN платформа, дефинирана от софтуер, която обединява множество WAN връзки и мрежови услуги, включително криптиране и управление на трафика, и ги препраща през WAN връзки със скорост от 2,5 до 200 Gbps. Рутерите съдържат както хардуерна, така и софтуерна резервираност в един водещ в индустрията дизайн с висока достъпност.

Последните допълнения към серията Cisco ASR 1000 са рутерите Cisco ASR 1002-HX и Cisco ASR 1001-HX. И двата нови рутера поддържат до 100 Gbps в 2-Рак единица (2RU) и 60 Gbps във формат-1-Рак единица (1RU) съответно. ASR 1002-HX има 8 вградени 10 Gigabit Ethernet (GE) порта и 8 1 GE порта, със слот за адаптер за Ethernet Port (EPA) за разширяване. ASR 1001-HX има 4 вградени 10 GE порта, 8 1 GE порта и 4 конфигурируеми порта 10 GE или 1 GE. Процесорът 3 на рутера от сериоята Cisco ASR 1000 е най-новото попълнение към модулните машини на равнината на управление в серията Cisco ASR 1000. Процесорът 3 на рутера добавя още опции за по-висока производителност, памет и съхранение към серията ASR 1000.

Серията Cisco ASR 1000 поддържа Cisco IOS® XE софтуер, модулна операционна система с модулно пакетиране, висока скорост и голяма гъвкавост. Процесорите с вградени услуги от серията Cisco ASR 1000 (ESP), които са базирани на технологията на процесора Cisco Flow, ускоряват много усъвършенствани функции, като например крипто базирана сигурност на достъпа; Транслация на мрежови адреси (NAT), защита от заплахи чрез Cisco зоново-базирана защитна стена (ZBFW), инспекция на дълбоки пакети (DPI), Cisco обединен граничен елемент (CUBE) и разнообразен набор от функции на взаимосвързани Центрове за данни (DCI). Тези услуги са внедрени в софтуера на Cisco IOS XE, без да е необходима допълнителна хардуерна поддръжка.

Рутерите от серията ASR 1000 се намират в края на вашия корпоративен център за данни или голям офис, свързвайки се с WAN, както и в Точките на присъствие при доставчиците на услуги (POPs). Серията Cisco ASR 1000 ще бъде в полза за следните видове клиенти:

- Предприятията, които изпитват експлозивен мрежов трафик като мобилност, облачни мрежи и използване на видео и с нарастващо използване на сътрудничество; Cisco ASR консолидират тези различни потоци от трафик и прилагат към тях управление на трафика и резервирани възможности, за да поддържат консистентна производителност между фирмените сайтове и облачните локации;
- Доставчиците на мрежови услуги, които трябва да доставят на бизнес клиентите високоефективни услуги, като DCI и агрегиране на сървърите на браншовите офиси; Доставчиците на услуги могат, също така, да използват мултисервизните рутери, за да разгърнат хоствани и управлявани услуги за бизнеса и мултимедийни услуги към гражданите.
- Съществуващите клиенти на рутерите от серията Cisco 7200 (в края на продажбата), които търсят проста миграция към нова мултисервисна платформа, която осигурява по-висока производителност със същия дизайн.

[redacted] [redacted] [redacted]

 [redacted] [redacted] [redacted]

[redacted] рия ЕАД
от 27
КП2

Характеристики и предимства

Рутерите от серията Cisco ASR 1000 имат модулен, но интегриран дизайн, така че мрежовите оператори мога да увеличат мрежовия си капацитет и услуги без хардуерна надстройка. С гъвкавостта на големия връзки максималните скорости и цената, не е необходимо да преоценявате никоя мрежова локация.

Освен това имате възможност да закупите модели „-X“ и „-HX“, така че можете да увеличите пропускателнат способност, като просто закупите лицензи за надграждане, докато нараства вашия бизнес, за да увеличават динамично скоростта на мрежата си.

Софтуерно дефинирана WAN на Cisco

Възможностите на Cisco SD-WAN могат да бъдат активирана на платформите от серията Cisco ASR 1000 IOS-XE. Cisco SD-WAN предлага изцяло нов начин за управление и опериране на вашата WA инфраструктура. Cisco SD-WAN е облачно доставена архитектура, която предлага сигурни, гъвкави и богат услуги със следните ключови предимства:

- **По-добро потребителско изживяване:** Възможността за инсталиране на приложения за минути в всяка платформа, с консистентно потребителско изживяване. Осигурява предсказуем производителност за приложения, намиращи се в центъра за данни или в облака.
- **По-голяма гъвкавост:** По-бързо, по-лесно внедряване и работа на вашата WAN и постигане на по бърза производителност, като използвате по-малка честотна лента. Добавя нови услуги, генериращ приходи за минути, а не за месеци.
- **Разширена защита от заплахи:** Свържете защитено потребителите си с приложенията за минути защитавайте данните си от WAN едж до облака. Сигурна сегментация за критични активи многослойна, устойчива сигурност, която криптира всички данни.

SD-WAN интегрирана сигурност

За да се свържат ефективно с множество облачни инфраструктури, много бизнес клиенти искат да създада SD-WAN инфраструктура, която използва директен достъп до Интернет (DIA). Това може да спести разходи да намали сложността, като намали WAN трафика до вашите центрове за данни; въпреки това свързването н браншове директно към Интернет без подходящите контроли за сигурност излага мрежата ви на заплахи уязвимости.

С платформата Cisco SD-WAN и платформите от серия ASR 1000 можете да интегрирате директно системат за сигурност на браншовата DIA с тези интегрирани възможности за сигурност:

- Приложно ориентирана защитната стена на предприятието
- Прилагане на DNS слой (Umbrella)

А с интеграцията за сигурност на Cisco SD-WAN ще намалите сложността, като имате единен интерфейс з управление (vManage) както за мрежата, така и за сигурността.

За повече информация относно Cisco SD-WAN и vManage вижте: https://www.cisco.com/go/sd-wan.

[redacted]

[redacted] ия ЕАД
[redacted] я от 27
КП2

Унифицирана защита на достъпа и многофакторна автентификация

Моделът за сигурност "Нулево доверие" позволява сигурни връзки към всички приложения (независимо дали за в офиси или в облака) на базата на надеждността на потребителите и устройствата.

Таблица 1 обобщава характеристиките и предимствата на рутерите от серията ASR 1000 на Cisco.

Таблица 1. Характеристики и предимства на рутерите от серията ASR 1000 на Cisco.

Характеристика	Полза
Висока достъпност	
Резервирани хардуерни компоненти и захранвания	• Тези компоненти осигуряват непрекъснатост на системата и бизнеса. • ASR 1006, ASR 1006-X, ASR 1009-X и ASR 1013 имат резервирани маршрутни процесори и ESP. • ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, и ASR1004 имат резервирани елементи в софтуера на Cisco IOS XE.
Вътрешна резервираност на устройствата	• Резервираният хардуер, комбиниран с модулен софтуер, ограничава грешките и предотвратява повреди в системата. • Резервираността при рутерите се активира чрез сдвояване на рутери, които действат като резервно копие един за друг. Рутерите предлагат 99,999 процента („пет деветки") наличност за непрекъснато високопроизводително потребителско преживяване с приложенията.
Поддръжка за актуализиране на софтуера без прекъсване на услугата (ISSU)	• Не е необходимо да планирате прозорци за престой; промените се правят, докато системата продължава да работи, при наличие на непрекъснато маршрутизиране.
Режим на суб-пакет за софтуера на Cisco IOS XE	• Можете да надстроите отделни софтуерни компоненти за по-малко време.
Мащабируем капацитет и производителност	
Платформа базирана на процесора Cisco Flow	• Усъвършенстваните услуги могат да работят с високи скорости без нужда от допълнителен хардуер или блейдове.
Хардуерно ускорение	• Функции като качество на услугата (QoS), криптография и списъци за контрол на достъпа (ACL) се обработват в хардуера.
Разделяне на контролната и пренасочващата равнина	• Можете да мащабирате равнините за управление и данни независимо една от друга.
Защита на инвестициите	
Модулност на софтуера	• Можете да смесвате и подбирате услугите, които най-добре отговарят на вашите бизнес нужди; няма да "губите" инвестиции за способности, които не са ви необходими.
Заплащане с растежа на бизнеса с моделите „-X"	• Когато имате нужда от по-голяма производителност, просто го активирате с промяна в лиценза за софтуер, вместо да се налага да харчите капитали за допълнителен хардуер.
Cisco адаптери за споделени портове (SPA)	• Можете да използвате повторно вашата инвестиция в мрежовите Вх./Изх. за всички платформи.
Cisco Мрежови интерфейсни модули (NIM)	• Можете да използвате повторно вашата инвестиция в мрежовите Вх./Изх. за всички [redacted]

[redacted] ней [redacted] азени.

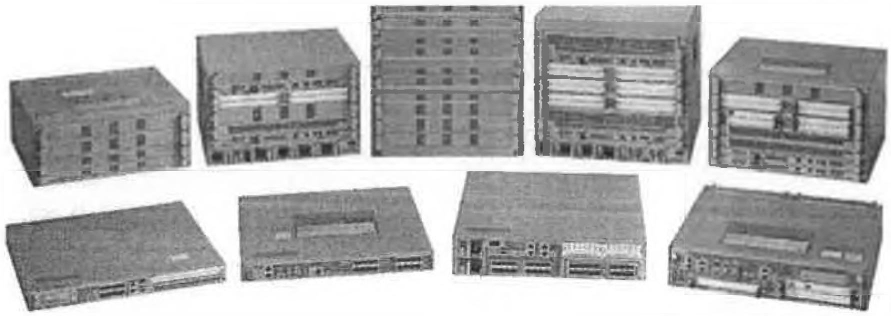
«ФИДЕС ИНТЕРКОМСУЛТ» ООД

А1 България ЕАД

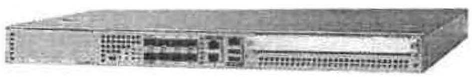
Продуктово портфолио

Серията Cisco ASR 1000 съдържа 8 модела с различни типове Вх./Изх. свързаност и слотове, и различни максимални скорости на пропускане (Фигура 1). Всички модели използват иновативния и мощен процесор Cisco Flow и поддържат един и същ набор от функции, базирани на операционната система Cisco IOS XE. Цялото това сходство опростява управлението и операциите.

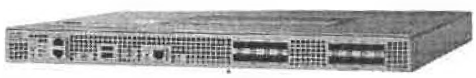
- Рутер Cisco ASR 1001-X (Фигура 2)
- Рутер Cisco ASR 1002-X
- Рутер Cisco ASR 1001-HX (Фигура 3)
- Рутер Cisco ASR 1002-HX (Фигура 4)
- Рутер Cisco ASR 1004
- Рутер Cisco ASR 1006
- Рутер Cisco ASR 1006-X
- Рутер Cisco ASR 1009-X
- Рутер Cisco ASR 1013



Фигура 1.
Рутери за агрегирани услуги Cisco Серия ASR 1000



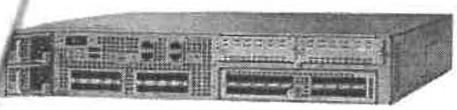
Фигура 2.
Рутер Cisco ASR 1001-X



Фигура 3.
Рутер Cisco ASR 1001-HX

[redacted]

[redacted]



Фигура 4.
Рутер Cisco ASR 1002-HX

Лицензиране на софтуера

Абонамент за софтуер чрез Cisco DNA лицензиране

Серията ASR 1000 поддържа софтуерно базиран абонамент, използвайки лицензиране на базата на Cisco DNA. За портфолиото на WAN са достъпни два лиценза за абонамент за софтуер на базата на Cisco DNA: Cisco DNA Advantage и Cisco DNA Premier позволяват на клиентите да разполагат с единно унифицирано решение, обхващащо рутерите от серията ASR 1000 и тези от ISR 1000 и ISR 4000.

Лицензните нива са структурирани така, че да подпомагат растежа в бизнес нуждите, позволявайки на клиента да премине от основна функционалност, Cisco DNA Essentials, към пълна функционалност с Cisco DNA Advantage и да го разширят, така че да включват оптимизация и анализ на WAN на Cisco DNA Premier. Това осигурява пълна гъвкавост за преместване на един и същ лиценз през крайните точки въз основа на нарастващите изисквания към мрежата и сигурността, растеж на честотната лента на базата на растежа на потребителите и приложенията в обектите, както и възможността за промяна на управлението на платформата от офиса към облака или обратно.

Cisco DNA лицензите се поддържат за платформи ASR 1000 с помощта на Cisco DNA Център, контролера и платформата за анализи в сърцето на базираната на намерения мрежа на Cisco. За повече информация относно Cisco DNA Център и поддържаните платформи, моля, вижте на https://www.cisco.com/c/en/us/products/cloud-systems- management/dna-center/index.html.

Софтуер Cisco ONE

Софтуерът Cisco ONE™ предлага ценен и гъвкав начин за закупуване на софтуер за достъп до WAN и домейните на центровете за данни. На всеки етап от жизнения цикъл на продукта софтуерът Cisco ONE помага за по-лесно закупуване, управление и надграждане на вашия мрежов и инфраструктурен софтуер. Софтуерът Cisco ONE предоставя:

- Гъвкави лицензионни модели за плавно разпределение на разходите за софтуер на клиентите във времето
- Защита на инвестициите за закупуване на софтуер чрез преносимост на лицензи с активирани софтуерни услуги
- Достъп до актуализации, надстройки и нова технология от Cisco чрез услуги за поддръжка на софтуер на Cisco® (SWSS)

Cisco ONE за WAN дава на организациите широки възможности за браншовите офиси и периферията на предприятието. Cisco ONE Foundation за WAN свързва и осигурява вашия браншови офис, като същевременно оптимизира разходите. Cisco ONE WAN Collaboration интегрира глас и видео във вашия браншови офис и в периферията на мрежата.

За да активирате услугите на рутерите от серията ASC 1000 серия са необходими лицензи за софтуерните функции. Понастоящем са налични два вида лицензи за функции. Някои услуги изискват само лиценз за право на използване (RTU), докато други услуги изискват както лиценз за RTU, така и един или повече ензи за брой сесии. Всички лицензи на серията Cisco ASR 1000 са базирани на доверието, което ачава, че лицензите не се валидират чрез активиране на продукта или лицензен ключ.

...а рутерите Cisco ASR 1000 е необходим един от следните пет пакета:

- Cisco ASR 1000 IQS XE UNIVERSAL - БЕЗ КРИПТИРАНЕ НА ИНФОРМАЦИЯТА
- Cisco ASR 1000 IOS XE UNIVERSAL
- Cisco ASR 1000 IOS XE UNIVERSAL БЕЗ Законно прихващане
- Cisco ASR 1000 IOS XE UNIVERSAL - БЕЗ КРИПТИРАНЕ НА ИНФОРМАЦИЯТА БЕЗ законно

прихващане За да активирате набор от необходими функции, се изисква един от следните три технологични пакета:

  - Лиценз за Cisco ASR 1000 IP Base
  - Лиценз за IP услуги с Cisco ASR 1000 Advanced
  - Лиценз услуги с Cisco ASR 1000 Advanced

Варианти за използване на серията Cisco ASR 1000

Таблици 2 и 3 описват примери за използване от предприятия и доставчици на услуги съответно.

Таблица 2. Приложения на серията Cisco ASR 1000 в предприятия

Сценарий за внедряване	Описание	Характеристики на системата
WAN едж: Гарантира приложения с висок приоритет чрез създаване на виртуален „стъклен таван" за приложения с по-нисък приоритет. Подобрява потребителското изживяване.	• Прилага модулни QoS CLI (MQC) политики за VLAN или тунели • Ограничава арбитрарното събиране на трафик с нисък приоритет до определена честотна лента • Класифицира въз основа на диференцирана кодова точка на услугите (DSCP), мрежово-базирано разпознаване на приложения (NBAR) и Cisco IOS Cisco IOS FPM (FPM) в много йерархии, една за висок приоритет и една за нисък приоритет	• Прилага гъвкави йерархии • Поддържа 464 000 опашки от данни, чакащи за обработка • Позволява на всички опашки да имат минимална, максимална и извънредна честотна лента с приоритетно разпространение
Мултисервизен, мащабируем и сигурен разпределител: **IP Security (IPsec) VPN агрегационни скали за изпълнение на новите изисквания за честотна лента на IP VPN доставчиците на услуги.**	• Намалява капиталовите разходи (CapEx) и експлоатационните разходи (OpEx), като мигрира и консолидира към по-малко рутери от серията Cisco ASR 1000. • Защитава инвестициите чрез лесен преход към много по-високо ниво на криптиране, предлагайки поддръжка за криптиране до 78 Gbps с 200-Gbps Cisco ASR 1000 Серия ESP (ASR1000-ESP200) • Предлага по-лесно управление чрез вградени услуги за сигурност в процесора Cisco Flow, без да се изискват допълнителни сервизни модули или блейдове • Оптимизиран за QoS и IP Multicast приложения	• Поддържа хиляди сайтове • Поддържа 8 000 IPsec тунела • Предлага ефективност на криптиране до 78 Gbps и некриптографска поддръжка на преминаващата информация до 200 Gbps с процесора за вградени услуги на серията Cisco ASR 1000 200 Gbps (ASR1000-ESP200)

[redacted]

[redacted]

[redacted]

АТБ България ЕАД
София
КП2

...ценарий за внедряване	Описание	Характеристики на системата
Вградена високоскоростна защитна стена: **С политиката на зоново-базирана защитна стена, серията Cisco ASR 1000 действа като скрита и пълна бариера между всеки интерфейс, който не е част от същата зона. Трябва да се конкретизира изричната политика за двойка зони (използвайки езика на Cisco за политиките; т.е. MQC) във всяка посока между всяка двойка зони. Политиката установява в рамките на рутера вида на проверка на състоянието (слой 4, слой 7 или приложение) и параметрите на сесията, които да се прилагат за всяка двойка зони.** **Пример: Ще бъде необходима изрична политика, позволяваща на HTTP и Системата за имена на домейни (DNS) да преминават границата на интернет-демилитаризираната зона (DMZ).**	• Защитната стена е вградена в процесора на Cisco Flow; не са необходими допълнителни сервизни блейдове или модули • Няколко гигабита от честотната лента се маршрутизират, докато в същото време рутерът изпълнява зоново базирана политика за защитната стена и други основни функции като QoS, IPv4, IPv6, NetFlow и други • Серията Cisco ASR 1000 осигурява регистриране на всички състояния на сесиите на защитната стена към приложения за управление на мрежата, способни да приемат относително огромни количества потока от данни. Приложения на трети страни могат да обработват данните от сесията	• Осигурява работа на защитната стена от 2,5 до 200 Gbps, в зависимост от използвания ESP • Предлага високоскоростна регистрация от 40 000 сесии в секунда с NetFlow Версия 9
Управляван CPE: Това внедряване наираншова архитектура предлага мощна инвестиционна защита с услуги и мащаб.	• Оборудваното оборудване за клиентски офиси (CPE) помага на браншовите офиси да се насочват правилно през различни видове Ethernet, за да спазват Споразуменията за ниво на услугата (SLA) • Това приложение криптира няколко гигабита от честотна лента без допълнителни сервизни блейдове или модули • Управляваният CPE оптимизира WAN, за да маршрутизира около частични повреди в мрежата на доставчика на услуги, за по-добро гарантиране на критичните приложения • Това приложение предлага малки форм-фактори (1 Рак единица [1RU] за Cisco ASR 1001-X и ASR 1001-HX и 2RU за рутерите Cisco ASR 1002-HX и ASR 1002-X) • Бележка: ISSU не се поддържа на Cisco ASR 1001-X, ASR 1001-HX, ASR 1002-HX, ASR 1002-X или ASR 1004 Управляваният CPE предлага достъпност, дори когато софтуерът Cisco IOS е отпаднал	• Предлага първа за индустрията резервирана поддръжка на софтуера, без допълнителен хардуерен модул, на Cisco ASR 1001-X, ASR 1001-HX, ASR 1002-HX, ASR 1002-X и ASR 1004; резервираността на хардуера и ISSU се поддържат на Cisco ASR 1006 и ASR 1013 • Предлага мощна защитна стена и NAT производителност от 2,5 до 200 Gbps и поддържа криптиране от 1,8 до 78 Gbps в допълнение към оптимизацията на WAN и гласовите функции

Таблица 3. Приложения на серията Cisco ASR 1000 в провайдерите на услуги

Сценарий за внедряване	Описание	Характеристики на системата
Широколентов L2TP концентратор за достъп (LAC) или L2TP мрежов сървър (LNS): **Решението предлага протокол на тунелиране Слой 2 (L2TP) директен протокол от крайна точка до тунел (PPPoX) или IP сесии с изисквания за честотна лента в ATM STM-1, Fast Ethernet, Gigabit Ethernet и 10 Gigabit Ethernet диапазон.**	• Приложението е идеално за тройно възпроизвеждане (данни, глас и видео) на пазара на едро • Предлага интегрирана доставка на услуги • Поддържат се защитна стена за потребителя, сесиен граничен контролер (SBC) и др.	• Осигурява много висока мащабируемост до 64 000 абонати и до 16 000 тунела

...ия ЕАД
София
КП2

Сценарий за внедряване	Описание	Характеристики на системата
От страната на доставчика на услуги Слой 3 VPN (L3VPN) от страната на доставчика: **Пример: Можете да внедрите решението от към страната на разпределен доставчик или на доставчик в глобални VPN мрежи със изисквания за честотна лента като асиметрична DSL (ADSL), T1 / E1, STM-1, STM-4, Fast Ethernet, Gigabit Ethernet и т.н.**	• Приложението предоставя интегрални услуги в процесора на Cisco Flow • Осигурява криптиране, FPM, NBAR, SBC, IP Multicast и др.	• Предлага отлична мултикаст функция • Мащаб до 8 000 случая на виртуално транзитиране на маршрути (VRF), 1 милион етикета на Протокола за дистрибуция на етикети (LDP) и 4000 списъка за контрол на достъпа (ACL) • Поддържа до 4 милиона маршрута IPv4 • Поддържа до 4 милиона маршрута IPv6
От страната на доставчика на услуги Маршрутен рефлектор от висок клас: **Можете да използвате решението като маршрутен рефлектор за поддръжка на честотна лента от 40 Gbps.**	• Приложението осигурява висока мащабируемост • То предлага модулен дизайн на процесора на рутера и ESP с резервираност на хардуера и софтуера	• Мащабира до 29 милиона маршрута IPv4 • Поддържа 64 000 съседства на Слой 3
Пример за глас и мултимедия от следващо поколение: Cisco Unified Border Element Enterprise Edition (ENT издание): **Приложението SBC (наречено Cisco Unified Border Element [ENT издание]) изпълнява функциите на шлюз за глас и видео едновременно със стандартните IP данни за услуги. Не се изисква уред или допълнителен блейд за услуги.** **Протоколите за контрол и медийните протоколи работят прозрачно в сложна гласова архитектура. За повече информация вижте информационния лист CUBE на https://www.cisco.com/go/cube.**	• Защитените и верифицирани връзки с магистралната линия с Протокол за започване на сесия (SIP) позволяват на доставчиците на услуги да предлагат гласови и видео услуги в реално време • WAN едж е по-лесен за управление, тъй като има само една изходна и една входна точка за достъп до Интернет или услуги от доставчика на услуги • Контролната равнина е отделена от равнината за предаване на данни, така че процесите на сигнализиране и управление са отделени от обработката на медиите • Приложението CUBE SBC може да се използва за SIP магистрални видео и/ или аудио услуги, осигурени от доставчици на услуги или за достъпни по Интернет SIP линейни услуги към Унифицираният мениджър на комуникации на Cisco	• Подпомага SBC със сигурност, QoS, IPv4 и IPv6 (IP Unicast и IP Multicast едновременно) • Поддържа 16 000 едновременни гласови повиквания и мултимедийни данни до 200 Gbps с активирано отчитане, защитна стена и качество на разговорите • Интегриран е с входяща инфраструктура с висока достъпност и транслация на Протокола за конфигурация на динамичен хост (DHCP)

Спецификация на продукта

Таблица 4 сравнява различните маршрутизатори на Cisco ASR 1000, а Таблица 5 сравнява различните спецификации на процесорния модула. За сравнения на ESP на Cisco ASR, вижте ESP datasheet. За сравнение на маршрутните процесори на ASR, вижте RP datasheet. За сравнение на SPA интерфейсните процесори на SPA, вижте SPA/SIP datasheet.

...ария ЕАД
СОФИЯ
КП 2

аблица 4. Серия Cisco ASR 1000: Сравнение на шасита и спецификации

Модел	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
Физически спецификации **Бележка:** Дълбочината се отнася за размер на шасито от ръб до ръб и не включва издатини като дръжки за карти, дръжки на захранващия блок и скоби за управление на кабелите. Вижте приложимото ръководство за инсталиране на хардуер за допълнителни подробности.	Височина: 1.71 in. (43.43 mm) Ширина: 17.3 in. (439.42 mm) Дълбочина: 18.17 18.17 in. (461.5 mm) Тегло: • 25 lb (11.35 kg) пълно натоварване **Бележка:** Рутерът Cisco ASR 1001-X има интегрирани маршрутен процесор, ESP, и SIP	Височина: 3.5 in. (88.9 mm) Ширина: 17.2 in. (437.4 mm) Дълбочина: 18.15 in. (461.0 mm) Тегло: • 38.25 lb(17.36 kg) (с двойно AC захранване и SPA капаци) • 39.05 lb (17.72 kg) (с двойно AC захранване и SPA капаци)) • Няма включени SPA **Бележка:** Cisco ASR 1002-X е с интегрирани маршрутен процесор, ESP и SIP	Височина: 1.71 in. (43.43 mm) Ширина: 17.3 in. (439.42 mm) Дълбочина: 18.38 in. (466.85 mm) Тегло: • 23 lb (10.44 kg) с двойно AC захранва • не • 22.5 lb (10.21 kg) с двойно DC захранване	Височина: 3.5 in. (88.9 mm) Ширина: 17.3 in. (439.4 mm) Дълбочина: 19.25 in. (489.0 mm) Weight: • 34 lb (15.45 kg) (с двойно AC захранване) • 34 lb (15.45 kg) (с двойно DC захранване)	Височина: 7 in. (177.8 mm) Ширина: 17.2 in. (437.4 mm) Дълбочина: 18.15 in. (461.0 mm) Тегло: • 68.7 lb (31.16 kg) (с двойно AC захранване, капаци за свободни SPA, серия ASR 1000 10-Gbps ESP [ASR1000 - ESP10] или серия ASR 1000 40-Gbps ESP [ASR1000-ESP-40], серия Cisco ASR 1000 рутерен процесор 1 [RP1] [ASR1000-RP1], два серия Cisco ASR 1000 10-Gbps SIPs [ASR1000-SIP10] или серия ASR1000 40-Gbps SIPs	Височина: 10.5 in. (266.7 mm) Ширина: 17.2 in. (437.4 mm) Дълбочина: 18.15 in. (461.0 mm) Тегло: • 98.70 lb (44.77 kg) (с двойно AC захранване, SPA, рутерен процесор или два Cisco серия ASR 1000 10-Gbps ESPs [ASR1000-ESP10] или серия ASR 1000 40-Gbps ESPs [ASR1000-ESP-40] или серия ASR1000 100-Gbps ESPs [ASR1000-ESP100], два серия Cisco ASR 1000 RP1s [ASR1000- RP1], три Cisco	Височина: 10.47 in. (265.9 mm) Ширина: 17.2 in. (437.4 mm) Дълбочина: 18.15 in. (461.0 mm) Тегло: • 36.5 lb празен • 112 lb (50.91 kg) (с два вентилаторни модула, три AC захранващи блока, три свободни гнезда за захранване, два серия Cisco ASR1000 100-Gbps ESPs [ASR1000-ESP100] или два серия Cisco ASR1000 100-Gbps ESPs [ASR1000-ESP100-X] или два серия ASR1000 200-Gbps ESPs [ASR1000-ESP200-X], два Cisco	• Височина: 15.72 in. (399.3 mm) • Ширина: 17.2 in. (437.4 mm) • Дълбочина: 18.15 in. (461.0 mm) • Тегло: • 50 lb празен • 154 lb (70 kg) (с два вентилаторни модула, четири AC захранващи блока, две свободни гнезда за захранване, два серия Cisco ASR1000 100-Gbps ESPs [ASR1000-ESP100] или два серия Cisco ASR1000 100-Gbps ESPs [ASR1000-ESP100-X] или два серия ASR1000 200-Gbps ESPs [ASR1000-ESP200-X], два Cisco ASR1000	• Височина: 22.8 in. (579.1 mm) • Ширина: 17.2 in. (437.4 mm) • Дълбочина: 18.15 in. (461.0 mm) • Тегло: • 184.0 lb (83.46 kg) (с резервно AC захранване, SPA, рутерен процесор или капаци за свободни SIP, два серия Cisco ASR 1000 40-Gbps ESPs [ASR1000-ESP40] или серия ASR1000 100-Gbps ESPs [ASR1000-ESP100] или серия ASR1000 100-Gbps ESPs [ASR1000-ESP100-X] или серия ASR1000 200-Gbps ESPs [ASR1000-ESP200],

[redacted]

[redacted]

ЕАД
т 27

КП2

Модел	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					[ASR1000-SIP-40], и без SPA)	серия ASR 1000 10-Gbps SIPs [ASR1000-SIP10] или серия ASR1000 40-Gbps SIPs [ASR1000-SIP-40], и без SPA)	0 серия ASR 1000 RP2s [ASR1000-RP2], два серия Cisco ASR 1000 100-Gbps MIPs [ASR1000-MIP100], четири свободни EPA и без EPA)	серия 200-Gbps ESPs [ASR1000-ESP200-X], два серия Cisco ASR 1000 RP2s [ASR1000-RP2], три серия Cisco ASR 1000 100-Gbps MIPs [ASR1000-MIP100], шест празни EPA , и без EPA)	два серия Cisco ASR 1000 RP2s [ASR1000-RP2], шест серия Cisco ASR 1000 40-Gbps SIPs [ASR1000-SIP40], и без SPA)
Памет по подразбиране	8-GB DRAM споделена между рутерните процесори, ESP и SIP	4-GB DRAM споделена между рутерните процесори, ESP и SIP	8-GB DRAM споделена между рутерните процесори, ESP и MIP	16-GB DRAM споделена между рутерните процесори, ESP и MIP	4-GB DRAM RP1 8-GB DRAM RP2	4-GB DRAM RP1 8-GB DRAM RP2	8-GB DRAM RP2 8-GB DRAM RP3	8-GB DRAM RP2 8-GB DRAM RP3	8-GB DRAM RP2 8-GB DRAM RP3
Брой поддържани SIP или Ethernet линейни карти	Интегрирани в шасито	Интегрирани в шасито	Интегрирани в шасито	Интегрирани в шасито	2	3	2	3	6
Споделени портови адаптери	1 SPA слот с единична височина	3 SPA слота	Няма	Няма	8 SPA слота	12 SPA слота	8 SPA слота	12 SPA слота	24 SPA слота
Адаптери за Ethernet портове	Няма	Няма	Няма	1 EPA слот	Няма	Няма	4 EPA слота	6 EPA слота	12 EPA слота
Серия Cisco ASR 1000 ESP:	Интегрирани в шасито	Интегрирани в шасито	Интегрирани в шасито	Интегрирани в шасито	1 ESP слот	2 ESP слота	2 ESP слота	2 ESP слота	2 ESP слота
Рутерен процесор	Интегриран в шасито: Cisco ASR 1001-X	Интегриран в шасито: Cisco ASR 1002-X	Интегриран в шасито: СерияCisco ASR 1001-HX	Интегриран в шасито: Cisco ASR 1002-HX	1 слот за рутерен процесор	2 слота за рутерен процесор	2 слота за рутерен процесор	2 слота за рутерен процесор	2 слота за рутерен процесор

[redacted]

[redacted]

[redacted] [redacted]

СОФИЯ
КП2

одел	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
	Серия рутерен процесор с четири-ядрен процесор	Серия рутерен процесор с четири-ядрен процесор	Рутерен процесор	Серия Рутерен процесор					
Резервираност	Софтуер: Да	Софтуер: Да	Софтуер: Да	Софтуер: Да	Софтуер: Да	Хардуер: Да	Хардуер: Да	Хардуер: Да	Хардуер: Да
Вградени Gigabit Ethernet портове	Да: 6 Gigabit Ethernet Малък форм фактор включваеми (SFP) порта	Да: 6 Gigabit Ethernet SFP порта	Да: 8 Gigabit Ethernet SFP порта, плюс опционални 4 конфигуруеми 1GE/10GE порта	Да: 8 Gigabit Ethernet SFP порта	0	0	0	0	0
Вградени 10 Gigabit Ethernet портове	Да: Два 10 Gigabit Ethernet Малък форм фактор плюс включваеми (SFP+) порта Бележка: Вградените 10-GB портове не могат да бъдат понижени до скорост 1-GB	Не	Да, четири 10 Gigabit Ethernet Малък форм фактор плюс включваеми (SFP+) порта, плюс опционални 4 конфигуруеми 1GE/10GE порта	Да: Осем 10 Gigabit Ethernet Малък форм фактор плюс включваеми (SFP+) порта Бележка: Вградените 10-GB портове не могат да бъдат понижени до скорост 1-GB	Не	Не	Не	Не	Не
Мрежов интерфейсен модул	Да	Не	Не	Да	Не	Не	Не	Не	Не

«ФИДЕС ИНТЕРНЕЙШЪНЪЛ»

ЕАД

КП2

Таблица 5. Сравнение и спецификации на процесорния модул серия Cisco ASR 1000

Cisco ASR 1000 Серия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
ESP поддръжка	Cisco ASR 1000 серия 2.5- Gbps ESP (по подразбиране) Надграждащ се чрез лиценз за активирана функция на софтуер до 5, 10 или 20 Gbps	Cisco ASR 1002-XESP с 5-Gbps (по подразбиране) Надграждащ се чрез лиценз за активирана функция на софтуер до 10, 20 или 36 Gbps	Вградена ESP с до 60 Gbps пропускателна способност	Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100) еквивалент	Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10), некриптиран Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10- N), Cisco ASR 1000 серия 20-Gbps ESP (ASR1000-ESP20), и Cisco ASR 1000 серия 40-Gbps ESP (ASR1000-ESP40)	Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10), некриптиран Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10-N), Cisco ASR 1000 серия 20- Gbps ESP (ASR1000-ESP20), Cisco ASR 1000 серия 40- Gbps ESP (ASR1000-ESP40), и Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100)	Cisco ASR 1000 серия 40-Gbps ESP (ASR1000-ESP40), Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100), Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100-X) и ASR 1000 серия 200-Gbps ESP (ASR1000-ESP200- X)	Cisco ASR 1000 серия 40- Gbps ESP (ASR1000-ESP40), Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100), Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100-X), и Cisco ASR 1000 серия 200-Gbps ESP (ASR1000-ESP200) и Cisco ASR 1000 серия 200-Gbps ESP (ASR1000-ESP200-X)	Cisco ASR 1000 серия 40-Gbps ESP (ASR1000 - ESP40), Cisco AS R 1000 серия 100-Gbps ESP (ASR1000 - ESP100), Cisco AS R 1000 серия 100-Gbps ESP (ASR1000 - ESP100-X), и Cisco ASR 1000 серия 200-Gbps ESP (ASR1000 - ESP200)
ESP честотна лента	2.5 до 20 Gbps	5 до 36 Gbps	60 Gbps	100 Gbps	10 до 40 Gbps	10 до 100 Gbps	40 до 100 Gbps	40 до 200 Gbps	40 до 200 Gbps
ESP памет	Споделете една и съща контролна памет на рутерния процесор	Споделете една и съща контролна памет на рутерния процесор	Споделете една и съща контролна памет на рутерния процесор	Споделете една и съща контролна памет на рутерния процесор	Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10)	Cisco ASR 1000 серия 10- Gbps ESP (ASR1000-ESP10) и ASR 1000 серия 10-Gbps ESP (ASR1000-	Cisco ASR 1000 серия 40- Gbps ESP (ASR1000-ESP40): 8-GB	Cisco ASR 1000 серия 40- Gbps ESP (ASR1000-ESP40): 8- GB DRAM Cisco ASR 1000	Cisco ASR 1000 серия 40- Gbps ESP (ASR1000-ESP40): 8- GB DRAM

Cisco ASR 1000 Серия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					и Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10) 2-GB DRAM по подразбиране; 2-GB DRAM максимум Cisco ASR 1000 серия 20-Gbps ESP (ASR1000-ESP20) 4-GB DRAM по подразбиране; 4-GB DRAM максимум	ESP10): 2-GB DRAM по подразбиране; 2-GB DRAM максимум Cisco ASR 1000 серия 20- Gbps ESP (ASR1000-ESP20): 4-GB DRAM по подразбиране; 4-GB DRAM максимум Cisco ASR 1000 серия 40-Gbps ESP (ASR1000-ESP40): 8-GB DRAM Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100): 16-GB DRAM	DRAM Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100): 16-GB DRAM Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100- X): 32-GB DRAM Cisco ASR 1000 серия 200-Gbps ESP (ASR1000-ESP200- X): 64- GB DRAM	серия 100-Gbps ESP (ASR1000-ESP100): 16-GB DRAM Cisco ASR 1000 серия 200-Gbps ESP (ASR1000-ESP200): 32-GB DRAM Cisco ASR 1000 серия 100-Gbps ESP (ASR1000-ESP100-X): 32-GB DRAM Cisco ASR 1000 серия 200-Gbps ESP (ASR1000-ESP200-X): 64-GB DRAM	Cisco ASR 1000 серия 100- Gbps ESP (ASR1000-ESP100): 16-GB DRAM Cisco ASR 1000 серия 200- Gbps ESP (ASR1000-ESP200): 32-GB DRAM Cisco ASR 1000 серия 100- Gbps ESP (ASR1000-ESP100- X): 32-GB DRAM
Линейни карти за SIP и Ethernet	Интегрирани в шасито: не се включват	Интегрирани в шасито: не се включват	Интегрирани в шасито: не се включват	Интегрирани в шасито: не се включват	Поддържа Cisco ASR 1000 серия 10-Gbps SIP карта на носителя (ASR10 00-SIP10), Cisco ASR 1000 серия 40-Gbps SIP	Поддържа Cisco ASR 1000 серия 10- Gbps SIP карта на носителя (ASR1000-SIP10), Cisco ASR 1000 серия 40- Gbps SIP карта на носителя (ASR1000-SIP40), и ASR 1000 фиксиран Ethernet	Поддържа Cisco ASR 1000 серия 40-Gbps SIP карта на носителя (ASR1000-SIP40), Cisco ASR 1000 серия MIP 100-Gbps карта на носителя (ASR100 0-	Поддържа Cisco ASR 1000 серия 40- Gbps SIP карта на носителя (ASR1000-SIP40), Cisco ASR 1000 серия MIP 100-Gbps карта на носителя (ASR1000- MIP 100), и ASR 1000 фиксиран Ethernet	Поддържа Cisco ASR 1000 серия 40-Gbps SIP карта на носителя (ASR1000-SIP40), Cisco ASR1000 серия MIP 100-Gbps карта на носителя (ASR1000-MIP100), и ASR

[redacted]

[redacted]

[redacted]

[redacted]

Cisco ASR 1000 Серия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					карта на носителя (ASR1000-SIP40), и ASR 1000 линейни карти за фиксиран Ethernet; два 10 GE + двадесет 1 GE линейни карти (ASR10 00-2T+20X1GE); и шест 10 GE линейни карти (ASR10 00-6TGE)	линейна карта; две 10 GE + двадесет 1 GE линейни карти (ASR1000-2T+20X1G E), и шест 10 GE линейни карти (ASR1000-6TGE)	MIP100), и ASR 1000 линейни карти за фиксиран Ethernet; два 10 GE + двадесет 1 GE линейни карти (ASR100 0-2T+20X1GE); и шест 10 GE линейни карти (ASR100 0-6TGE)	линейна карта; две 10 GE + двадесет 1 GE (ASR1000-2T+20X1GE) линейни карти; и шест 10 GE линейни карти (ASR1000-6TGE)	1000 линейни карти за фиксиран Ethernet; два 10 GE + двадесет 1 GE (ASR1000 - 2T+20X1 GE) линейни карти; и шест 10 GE линейни карти (ASR1000-6TGE)
Вградено хардуерно базирано криптиране (най-високата пропускателна стойност е за пакети от 1400B)	Да: До 8-Gbps криптиран поток	Да: До 4-Gbps криптиран поток	Да: До 16-Gbps криптиран поток	Да: До 25-Gbps криптиран поток	Да: На Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10) с до 4 Gbps и на Cisco ASR 1000 серия 20-Gbps ESP (ASR1000-ESP20) с до 8-Gbps криптиран поток **Бележка:** Не се поддържа на устройства без крипто	Да: На Cisco ASR 1000 серия 10- Gbps ESP (ASR1000-ESP10) с до 4-Gbps криптиран поток, Cisco ASR 1000 серия 20- Gbps ESP (ASR1000-ESP20) с до 8-Gbps криптиран поток, Cisco ASR 1000 серия 40- Gbps ESP (ASR1000-ESP40) с до 11-Gbps криптиран поток,	Да: На Cisco ASR 1000 Серия 40-Gbps ESP (ASR1000-ESP40) с до 11- Gbps криптиран поток, Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100) с до 29- Gbps криптиран поток, Cisco ASR 1000	Да: На Cisco ASR 1000 Серия 40-Gbps ESP (ASR1000-ESP40) с до 11-Gbps криптиран поток, Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100) с до 29-Gbps криптиран поток, Cisco ASR 1000 Серия 200-Gbps ESP (ASR1000-ESP200) с до 78-Gbps криптиран	Да: На Cisco ASR 1000 Серия 40-Gbps ESP (ASR1000-ESP40) с до 11-Gbps криптиран поток, Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100) с до 29-Gbps криптиран поток, и Cisco ASR 1000 Серия 200-Gbps ESP (ASR1000-ESP200) с до

КП2

Cisco ASR 1000 Серия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					Cisco ASR 1000 серия 10-Gbps ESP (ASR1000-ESP10- N)	и Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100) с до 29-Gbps криптиран поток **Бележка:** Не се поддържа на устройства без крипто Cisco ASR 1000 Серия 10- Gbps ESP (ASR1000-ESP10-N)	Серия 100-Gbps ESP (ASR100 0-ESP100-X) с до 142- Gbps криптиран поток и Cisco ASR 1000 Серия 200-Gbps ESP (ASR100 0-ESP200-X) с до 197- Gbps криптиран поток	поток, Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100-X) с до 142-Gbps криптиран поток и Cisco ASR 2000 Серия 100-Gbps ESP (ASR1000-ESP200-X) с до 197-Gbps криптиран поток	78-Gbps криптиран поток, Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100-X) с до 142-Gbps криптиран поток
Минимално издание на софтуера Cisco IOS XE	Cisco IOS XE софтуер издание 3.12.0	Cisco IOS XE софтуер издание 3.7.0S	Cisco IOS XE софтуер издание 16.3.1S	Cisco IOS XE софтуер издание 16.2.1S	Cisco IOS XE софтуер издание 2.1	Също като за Cisco ASR 1002 без Cisco ASR 1000 Серия 40- Gbps ESP (ASR1000-ESP40) изисква Cisco IOS XE софтуер издание 3.1.0S **Бележка:** Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100) изисква Cisco IOS XE	Cisco IOS XE софтуер издание 3.16.0 **Бележка:** Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100-X) и Cisco ASR 1000 Серия 200- Gbps ESP (ASR100 0- ESP200-	Cisco IOS XE софтуер издание 3.16.0 **Бележка:** Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100-X) и Cisco ASR 1000 Серия 200-Gbps ESP (ASR1000-ESP200-X) изисква Cisco IOS XE софтуер издание 17 2	Cisco ASR 1000 Серия 40-Gbps ESP (ASR1000-ESP40) изисква Cisco IOS XE софтуер издание 3.1.0S, ASR 1000 Серия 100-Gbps ESP (ASR1000 - ESP100) изисква Cisco IOS XE софтуер издание 3.7.0S, и ASR 1000 Серия

Cisco ASR 1000 Серия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
						софтуер издание 3.7.0S.	X) изисква Cisco IOS XE софтуер издание 17.2		200-Gbps ESP (ASR1000-ESP200) изисква Cisco IOS XE софтуер издание 3.10.0S **Бележка:** Cisco ASR 1000 Серия 100-Gbps ESP (ASR1000-ESP100- X) изисква Cisco IOS XE софтуер издание 17.2
Монтиране в рак	Да: 19-инчов	Да: 19-инчов	Да: 19-инчов	Да: 19-инчов	Да: 19-инчов	Да: 19-инчов	Да: 19-инчов	Да: 19-инчов	Да: 19-инчов
Стенен монтаж	Не	Не	Не	Не	Не	Не	Не	Не	Не
Външна USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет	поддържа 1-GB USB флаш памет
Резервно ел. захранване	Да: Двойно захранване по подразбиране; опция за AC или DC захранване **Бележка:** Не се поддържа микс от едно AC и едно DC захранване.	Също като за Cisco ASR 1002	Да: Двойно захранване по подразбиране; опция за AC или DC захранване **Бележка:** Не се поддържа микс от едно AC и едно DC захранване.	Да: Двойно захранване по подразбиране; опция за AC или DC захранване **Бележка:** Не се поддържа микс от едно AC и едно DC захранване.	Също като за Cisco ASR 1002	Също като за Cisco ASR 1002	Да: Двойно захранване по подразбиране, разширяващо се до общо шест, в зависимост от предпочитанията за конфигурация и резервираност; опция или 1100W AC или 950W DC **Бележка:**	Да: Двойно захранване по подразбиране, разширяващо се до общо шест, в зависимост от предпочитанията за конфигурация и резервираност, опция или 1100W AC или 950W DC **Бележка:** Микс от AC и DC захранване	Да: Четворно захранване (резервиран и двойки) по подразбиране; опция за AC или DC захранване **Бележка:** Не се поддържа микс от AC и DC захранване.

:isco ASR 1000 Серия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
							Не се поддържа микс от AC и DC захранване.	не се поддържа	
Входна мощност	Глобален диапазон на AC вход (85 до 264 VAC) Глобален диапазон на DC вход (-40 до - 72V; 48V номинално)	Също като за Cisco ASR 1002	Глобален диапазон на AC вход (85 до 264 VAC) Глобален диапазон на DC (-40 до - 72V; -48V номинално)	Глобален диапазон на AC вход (85 до 264 VAC) Глобален диапазон на DC (-40 до - 72V; - 48V номинално)	Също като за Cisco ASR 1002	Също като за Cisco ASR 1002	Глобален диапазон на AC вход (85 до 264 VAC) Глобален диапазон на DC (-40 до - 72V; -48V номинално)	Глобален диапазон на AC вход (85 до 264 VAC) Глобален диапазон на DC (-40 до - 72V; -48V номинално)	Глобален диапазон на AC (180 до 264V; 240V; 60 или 50 Hz номинално) Глобален диапазон на DC (-40,5 до - 72V; -48V номинално)
Консумирана мощност	• Максимум (DC): 242W • Максимум (AC): 250W • Максимум (изход) 250W	• Максимум (DC): 590W • Максимум (AC): 560W • Максимум (изход): 470W	• Максимум (DC): 360W • Максимум (AC): 360W • Максимум (изход) 360W	• Максимум (DC): 500W • Максимум (AC): 500W • Максимум (изход) 500W	• Максимум (DC): 1020 W • Максимум (AC): 960W • Максимум (изход) 765W	• Максимум (DC): 1700W • Максимум (AC): 1600W • Максимум (изход) 1275W Или • Максимум (DC): 2100W • Максимум (AC-ел. мрежа): 2000W • Максимум (изход) 1695W	• Максимум (DC): 4600W • Максимум (AC): 4500W • Максимум (изход) 4030W	• Максимум (DC): 5200W • Максимум (AC): 5100W • Максимум (изход) 4575W	• Максимум (DC): 4200W • Максимум (AC-ел. мрежа): 4000W • Максимум (изход): 3390W
Въздушен поток	Отпред назад	Отпред назад	Отпред назад	Отпред назад	Отпред назад	Отпред назад	Отпред назад	Отпред назад	Отпред назад
Работна температура (номинална)	32 до 104°F (0 до 40°C)	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X
Работна температу[redacted] кратко срочна)	32 до 122°F (0 [redacted]	Също като за [redacted]co ASR [redacted]1-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X

[redacted]

КП2

…co ASR 1000 …рия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
Работна влажност (номинална) (относителна влажност)	10 до 85%	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X
Работна влажност (краткосрочна)	5 до 90%	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1002
Температура на съхраняване	-40 до 150°F (-40 до 70°C)	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X
Влажност на съхраняване (относителна влажност)	5 до 95%	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X
Работна надморска височина	-500 до 10,000 фута (-152 до 3048 метра)	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X
Стандарти за изграждане на мрежово оборудване (NEBS)	GR-1089 и GR-63	GR-1089 и GR-63	GR-1089 и GR-63	GR-1089 и GR-63	GR-1089 и GR-63	GR-1089 и GR-63	GR-1089 и GR-63	GR-1089 и GR-63	GR-1089 и GR-63
EMC стандарти	• FCC 47 CFR • част 15 клас A • VCCI клас A • AS/NSZ клас A • ICES-003 Клас A • EN55022 /CISPR 22 Оборудване за информационни технологии. • (Излъчване)	Също като за Cisco ASR 1001-X	**Излъчвания** • FCC 47CFR15 Клас A • AS/NZS CISPR 22 • CISPR 22 Клас A • EN55022 Клас A • ICES-003 Клас A • VCCI клас A • CNS- 13438 Клас A • EN61000-3-2	**Излъчвания** • FCC 47CFR15 Клас A • AS/NZS CISPR 22 • CISPR 22 Клас A • EN55022 Клас A • ICES-003 Клас A • VCCI клас A • CNS- 13438 Клас A • EN61000-3-2	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X	Също като за Cisco ASR 1001-X

ЕАД София КП2

...o ASR ...00 ...рия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
	• EN55024 /CISPR 24 Информация за технологично оборудване • (Устойчивост) • EN300 386 Информация за телекомуникационно оборудване • (EMC) • EN50082 - 1/EN610 00-6-1 Общ стандарт за имунитет		• EN61000- 3-3 • Устойчивост • IEC/EN61000-4-2 Устойчивост на електростатични разряди • IEC/EN61000-4-3 Устойчивост на излъчвания • IEC/EN61000-4-4 EFT-B Устойчивост • IEC/EN61000-4-5 Пик • IEC/EN61000-4-6 Устойчивост на кондуктивни смущения • IEC/EN61000-4-8 Устойчивост на магнитното поле на захранващата честота • IEC/EN61000-4-11 Спадове на напрежението, кратки прекъсвания вариране на напрежението **ETSI/EN** • EN55022/ CISPR 22 Оборудване за информационни технологии (Емисии) • EN55022/ CISPR 24 Оборудване за информационни технологии (Устойчивост) • EN300386 Телекомуникации	• EN61000-3-3 **Устойчивост** • IEC/EN61000-4-2 Устойчивост на електростатични разряди • IEC/EN61000-4-3 Устойчивост на излъчвания • IEC/EN61000-4-4 EFT-B Устойчивост • IEC/EN610 00-4-5 Пик • IEC/EN61000-4-6 Устойчивост на кондуктивни смущения • IEC/EN610 00-4-8 Устойчивост на магнитното поле на захранващата честота • IEC/EN610 00-4-11 Спадове на напрежението, кратки прекъсвания вариране на напрежението **ETSI/EN** • EN55022/ CISPR 22 Оборудване за информационни технологии (Емисии) • EN55022/ CISPR 24 Оборудване за информационни технологии					

Cisco ASR 1000 Серия	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
			Мрежово оборудване • EN50082-1/EN6100 0-6-1 Общ стандарт за имунитет	(Устойчивост) • EN300 386 Телекомуникационно мрежово оборудване • EN50082-1/EN6100 0-6-1 Общ стандарт за имунитет					
Стандарти за безопасност	UL60950-1 CSA C22.2 No. 60950 -1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 6095 0-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL6095 0-1 CSA C22.2 No. 609 50-1-03 EN 60950- 1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950- 1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950 -1 CSA C22.2 No. 6095 0-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950- 1 CSA C22.2 No. 6095 0-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1

Информация за поръчка

Cisco ONE софтуер за WAN е наличен за ASR 1000 серия.

Софтуерът Cisco ONE предлага цялостно решение, което осигурява оптимално изживяване при всяка връзка, като същевременно ви помага да извлечете максимума от вашата WAN инвестиция със сигурна, устойчива на повреди свързаност.

Ползи:

- Свържете браншовите офиси и главния офис сигурно и на оптимална цена, като подобрите производителността на приложението чрез техники за ускоряване на протокола и техники за оптимизация, които разтоварват WAN.
- Интегрирайте глас и видео в браншовите офиси и главния офис, за да увеличите производителността.

За информация за поръчване на софтуера Cisco ONE за ASR 1000 серия, идете на https://www.cisco.com/c/en/us/products/software/one-wan/wan-part-numbers.html.

Устойчивост на околната среда на Cisco

Информация за политиките и инициативите на Cisco за устойчивост на околната среда за нашите прод[redacted] решения, операции и разширени операции или верига на доставки е предоставена в раздела "Устойчивост на околната среда" в доклада за Корпоративна социална отговорност (CSR) на Cisco.

[redacted]

…България ЕАД
София
КП2

Референтните връзки към информация по ключови теми за устойчивост на околната среда (споменати в раздела „Устойчивост на околната среда“ в доклада CSR) са дадени в следната таблица:

Тема относно устойчивостта	Препратка
Информация относно законите и разпоредбите за съдържанието на материалите в продуктите	Материали
Информация относно закони и разпоредби за електронните отпадъците, включително продукти, батерии и опаковки	Съответствие с WEEE

Cisco предоставя достъп до данните за опаковките само за информация. Тя може да не отразява най-актуалните правни разработки и Cisco не твърди и не гарантира, че е пълна, точна или актуална. Тази информация подлежи на промяна без предупреждение.

Поддръжка за софтуерно дефинирана WAN на Cisco

Серията ISR 1000 е оптимизирана за софтуерно дефинирана WAN (SD-WAN). За предприятията това означава, че критичните за бизнеса приложения работят по-бързо, с по-голяма надеждност и намалени оперативни разходи (OpEx). Cisco SDWAN постига това, като прави всички браншови центрове и центрове за данни да имат възможност да наблюдават, контролират, преместват и отчитат потоци от данни за приложения, като например специфичен уеб (HTTP) трафик.
Серията ISR 1000 има възможност за задълбочена проверка на пакети и може точно да идентифицира и контролира хиляди различни приложения, включително клиентски вътрешни корпоративни приложения.

Цялата SD-WAN реализация върху ASR 1000 може да бъде осъществена чрез управление на крайното устройство от облака или от офиса чрез възходящи нива на лицензи, базирани на пропускателна способност. Всички лицензи, които поддържат Cisco SD-WAN, независимо дали са офисни или в облак, са активирани чрез използване на абонаментни лицензи. Тези лицензи за абонамент дават възможност на всички клиенти безпроблемно да преминават между управление от офиса или от облак, ако е необходимо. Лицензните нива така са структурирани, че да подпомагат растежа на бизнес нуждите чрез прости абонаменти, които помагат за опростяване на преминаването към базирани на намерения мрежи за WAN.

Абонаментите за SD-WAN са представени от три лиценза за абонамент - **Cisco DNA Essentials, Cisco DNA Advantage и Cisco DNA Premier**, всеки от които разширява функционалността. **Cisco DNA Essentials за серията ISR 1000 и ISR 4000** обхваща всички видове свързаност и управление на жизнения цикъл на рутера, поддържа видимост на мрежата и приложенията, съчетана с базова сигурност на обекта и обмена на данни. Серията ASR 1000 поддържа две нива на Cisco DNA, Cisco DNA Advantage и Cisco DNA Premier. **Cisco DNA Advantage** осигурява разширени топологии на WAN, политики, ориентирани към приложенията политики, поддържани от подобрена мрежова сигурност. **Cisco DNA Premier** осигурява облачно свързване с неограничена сегментация, разширена оптимизация на приложенията и мрежови анализи с разширена защита от заплахи.

За повече информация относно Cisco SD-WAN, вижте https://www.cisco.com/c/en/us/products/software/one-wan-subscription/index.html.

За да направите поръчка, посетете Cisco Commerce Workspace.

За да започнете работа с серията Cisco ASR 1000, вижте подробните номера на продуктите и описанията в следните таблици:

- Таблица 6: Шаси
- Таблица 7: Процесорни модули
- [redacted]ица 8: Интерфейси и модули

за софтуерно изображение, лиценз за функции и надстройки, и за повече подробности за пакетите от серията Cisco ASR 1000 и как да поръчате Cisco ASR 1000 Серия, вижте Cisco ASR 1000 Ordering Guide.

Таблица 6. Информация за поръчка на шаси за серия Cisco ASR 1000

Номер на продукта	Описание на продукта
Шаси за серия Cisco ASR 1000	
ASR1001-X	Cisco ASR 1001-X Система, крипто, 6 вградени GE, двоен P/S
ASR1001-X=	Cisco ASR 1001-X Система, крипто, 6 вградени GE, двоен P/S, резерва
ASR 1001-HX	Cisco ASR1001-HX Система, 8x10GE+8x1GE, 2xP/S, опция за крипто, резерва
ASR 1001-HX=	Cisco ASR1001-HX Система, 8x10GE+8x1GE, 2xP/S, опция за крипто, резерва
ASR1002-HX	Cisco ASR 1002-HX Система, 4x10GE+4x1GE вградени, двоен P/S, опция за крипто
ASR1002-HX=	Cisco ASR 1002-HX Система, 4x10GE+4x1GE вградени, двоен P/S, опция за крипто, резерва
ASR1002-X	Cisco ASR 1002-X Система, крипто, 6 вградени GE, двоен P/S
ASR1002-X=	Cisco ASR 1002-X Система, крипто, 6 вградени GE, двоен P/S, резерва
ASR1004	Шаси Cisco ASR 1004, двоен P/S
ASR1004=	Шаси Cisco ASR 1004, двоен P/S, резерва
ASR1006	Шаси Cisco ASR 1006, двоен P/S
ASR1006=	Шаси Cisco ASR 1006, двоен P/S, резерва
ASR1006-X	Шаси Cisco ASR 1006-X
ASR1006-X=	Шаси Cisco ASR 1006-X, резерва
ASR1009-X	Шаси Cisco ASR 1009-X
ASR1009-X=	Шаси Cisco ASR 1009-X, резерва
ASR1013	Шаси Cisco ASR 1013, резервиран P/S
ASR1013=	Шаси Cisco ASR 1013, резервиран P/S, резерва
Серия Cisco ASR 1000 Опции за USB памет	
MEMUSB-1024FT	1 GB USB Флаш токен за серия Cisco ASR 1000
MEMUSB-1024FT=	1 GB USB Флаш токен за серия Cisco ASR 1000, резерва

Таблица 7. Информация за поръчка на процесорни модули

Номер на продукта	Описание на продукта
Процесор за вградени услуги на серията Cisco ASR 1000	
ASR1000-ESP20	Процесор за вградени услуги на Cisco ASR 1000, 20 Gb
ASR1000-ESP20=	Процесор за вградени услуги на Cisco ASR 1000, 20 Gb, резерва
ASR1000-ESP40	Процесор за вградени услуги на Cisco ASR 1000, 40 Gb
ASR1000-ESP40=	Процесор за вградени услуги на Cisco ASR 1000, 40 Gb, резерва
ASR1000-ESP100	Процесор за вградени услуги на Cisco ASR 1000, 100 Gb
ASR1000-ESP100=	Процесор за вградени услуги на Cisco ASR 1000, 100 Gb, резерва
ASR1000-ESP200	Процесор за вградени услуги на Cisco ASR 1000, 200 Gb
ASR1000-ESP200=	Процесор за вградени услуги на Cisco ASR 1000, 200 Gb, резерва
ASR1000-ESP100-X	Процесор за вградени услуги на Cisco ASR 1000, 100 Gb
ASR1000-ESP100-X=	Процесор за вградени услуги на Cisco ASR 1000, 100 Gb, резерва
ASR1000-ESP200-X	Процесор за вградени услуги на Cisco ASR 1000, 200 Gb
ASR1000-ESP200-X=	Процесор за вградени услуги на Cisco ASR 1000, 200 Gb, резерва
Рутерен процесор за серията Cisco ASR 1000	
ASR1000-RP2	Cisco ASR 1000 Рутерен процесор 2
ASR1000-RP2=	Cisco ASR 1000 Рутерен процесор 2, резерва
ASR1000-RP3	Cisco ASR 1000 Рутерен процесор 3
ASR1000-RP3=	Cisco ASR 1000 Рутерен процесор 3, резерва
ASR1000-RP3-32G-2P	Cisco ASR1000 RP3 w/ 32 GB, 2 пакета
ASR1000-RP3-64G-2P	Cisco ASR1000 RP3 w/ 64 GB, 2 пакета

[redacted]

КП2

Таблица 8. Информация за поръчка на интерфейси и модули

Номер на продукта	Описание на продукта
Cisco ASR 1000 Серия SPA Интерфейсен процесор и Ethernet линейни карти	
ASR1000-SIP40	Cisco ASR 1000 SPA Интерфейсен процесор 40
ASR1000-SIP40=	Cisco ASR 1000 SPA Интерфейсен процесор 40, резерва
ASR1000-6TGE	Cisco ASR 1000 линейни карти за фиксиран Ethernet, 6X10GE
ASR1000-6TGE=	Cisco ASR 1000 линейни карти за фиксиран Ethernet, 6X10GE, резерва
ASR1000-2T+20X1GE	Cisco ASR 1000 линейни карти за фиксиран Ethernet, 2X10GE + 20X1GE
ASR1000-2T+20X1GE=	Cisco ASR 1000 линейни карти за фиксиран Ethernet, 2X10GE + 20X1GE, резерва
ASR1000-MIP100	Cisco ASR 1000 Ethernet линейни карти, 100 Gb Модулен интерфейс процесор
ASR1000-MIP100=	Cisco ASR 1000 Ethernet линейни карти, 100 Gb Модулен интерфейс процесор, резерва
EPA-1X100GE	Cisco ASR 1000 1x100GE Адаптери за Ethernet порт
EPA-1X100GE=	Cisco ASR 1000 1x100GE Адаптери за Ethernet порт, резерва
EPA-2X40GE	Cisco ASR 1000 2x40GE Адаптери за Ethernet порт (Native QSFP)
EPA-2X40GE=	Cisco ASR 1000 2x40GE Адаптери за Ethernet порт (Native QSFP), резерва
EPA-1X40GE	Cisco ASR 1000 1x40GE Адаптери за Ethernet порт (2 физически QSFP порта - опционален лиценз за активиране на 2-ри порт)
EPA-1X40GE=	Cisco ASR 1000 1x40GE Адаптери за Ethernet порт (2 физически QSFP порта - опционален лиценз за активиране на 2-ри порт), резерва
L-FLA1-EPA-1X40GE	Cisco ASR 1000 1x40GE Лиценз за е-Доставка порт за EPA-1X40GE
EPA-QSFP-1X100GE	Cisco ASR 1000 1x100GE QSFP Адаптери за Ethernet порт
EPA-QSFP-1X100GE=	Cisco ASR 1000 1x100GE QSFP Адаптери за Ethernet порт, резерва
EPA-CPAK-2X40GE	Cisco ASR 1000 2x40GE Адаптери за Ethernet порт (оптичен кабел)
EPA-CPAK-2X40GE=	Cisco ASR 1000 2x40GE Адаптери за Ethernet порт (оптичен кабел), резерва
EPA-10X10GE	Cisco ASR 1000 10x10GE Адаптери за Ethernet порт
EPA-10X10GE=	Cisco ASR 1000 10x10GE Адаптери за Ethernet порт, резерва
EPA-18X1GE	Cisco ASR 1000 18x1GE Адаптери за Ethernet порт
EPA-18X1GE=	Cisco ASR 1000 18x1GE Адаптери за Ethernet порт, резерва

[redacted]

СОФИЯ КП2

Начини за надграждане

Рутерите серия Cisco ASR 1000 са включени в стандартната програма на Cisco за миграция на технологии. Вижте на https://www.cisco.com/go/tmp и се свържете с местния представител на на Cisco за подробности относно програмата.

Cisco услуги.

Cisco услугите карат мрежите, приложенията и хората, които ги използват, работят по-добре заедно.

Cisco и нашите сертифицирани партньори могат да помогнат за успешното внедряване във вашето предприятие на WAN едж с широко портфолио от услуги, базирани на доказани методологии. Можем да ви помогнем да установите сигурна, устойчива WAN архитектура и успешно да интегрирате технологиите за сигурност и Cisco унифицирани комуникации с честотна лента за поддръжка на видео, колаборация, решения за браншови офиси и растеж в съответствие с вашите бизнес цели.

Подходът за жизнен цикъл на Cisco за услуги определя необходимите дейности във всяка фаза от жизнения цикъл на решението. Услугите по планиране и проектиране ускоряват приемането на решение. Спечелилата награди техническа поддръжка увеличава оперативната ефективност. Услугите за оптимизация подобряват производителността, устойчивостта, стабилността и предвидимостта и подготвят вашата мрежа и екипи за промяна. За повече информация, моля посетете https://www.cisco.com/go/services.

Cisco Капитал

Гъвкави решения за плащане, които ще помогнат да постигнете вашите цели

Cisco Капитал улеснява получаването на правилната технология за постигане на вашите цели, дава възможност за трансформация на бизнеса и ви помага да останете конкурентоспособни. Можем да ви помогнем да намалите общите разходи за собственост, да запазите капитала и да ускорите растежа. В повече от 100 държави нашите гъвкави разплащателни решения могат да ви помогнат да придобиете хардуер, софтуер, услуги и допълващо оборудване на трети страни с лесни и предвидими плащания. Научете повече.

За повече информация

За повече информация относно серията Cisco ASR 1000 посетете https://www.cisco.com/go/asr1000 или се свържете с местния представител на Cisco. За информация относно пакетите от серията Cisco ASR 1000, вижте Cisco ASR 1000 Ordering Guide.

Главен офис в Америка
Cisco Systems, Inc.
San Jose, CA

Главен офис в Азия-Тихи океан
Cisco Systems (USA) Pte. Ltd.
Singapore

Главен офис в Европа
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco има над 200 офиса по света. Номерата на телефоните и факсовете са изписани в сайта на Cisco https://www.cisco.com/go/offices.

Подписаният Огнян Петков Кирилов удостоверявам верността на извършения от мен превод от английски на български език на приложения документ – "Рутери за агрегирани услуги Серия Cisco ASR 1000". Преводът се състои от 27 (двадесет и седем) страници.

Преводач: Огнян Петков Кирилов

Отпечатано в СА[redacted]

C 8-7316[redacted] 05[redacted]

ЕАД

[redacted]

КП2

[redacted]

Cisco
The bridge to possible

Data sheet
Cisco public

Cisco ASR 1000 Series Aggregation Services Routers

[redacted]

[redacted]

[redacted]

ВЯРНО С ОРИГИНАЛА

А1 [redacted] КП2

[redacted]

Contents

[redacted]

[redacted]

ВЯРНО С ОРИГИНАЛА

A1 [redacted] ЕАД

Product overview

Cisco® ASR 1000 Series Aggregation Services Routers provide a Software Defined WAN platform that aggregates multiple WAN connections and network services including encryption and traffic management, and forward them across WAN connections at line speeds from 2.5 to 200 Gbps. The routers contain both hardware and software redundancy in an industry-leading high-availability design.

The latest additions to the Cisco ASR 1000 Series are the Cisco ASR 1002-HX Router and the Cisco ASR 1001-HX Router. Both new routers support up to 100 Gbps in a 2-Rack-Unit (2RU) and 60 Gbps in a 1-Rack-Unit (1RU) form factor, respectively. The ASR 1002-HX has 8 built-in 10 Gigabit Ethernet (GE) ports and 8 1 GE ports, with the Ethernet Port Adapter (EPA) slot for expansion. The ASR 1001-HX has 4 built-in 10 GE ports, 8 1 GE ports, and 4 configurable 10 GE or 1 GE ports. The Cisco ASR 1000 Series Route Processor 3 is the newest addition to the modular control plane engines in the Cisco ASR 1000 Series. The Route Processor 3 adds more options for higher performance, memory, and storage to the ASR 1000 Series.

The Cisco ASR 1000 Series supports Cisco IOS® XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The Cisco ASR 1000 Series Embedded Services Processors (ESPs), which are based on Cisco Flow Processor technology, accelerate many advanced features such as crypto-based access security; Network Address Translation (NAT), thread defense with Cisco Zone-Based Firewall (ZBFW), Deep Packet Inspection (DPI), Cisco Unified Border Element (CUBE), and a diverse set of Data-Center-Interconnect (DCI) features. These services are implemented in Cisco IOS XE Software without the need for additional hardware support.

Cisco ASR 1000 Series routers sit at the edge of your enterprise data center or large office connecting to the WAN, as well as in service provider Points Of Presence (POPs). The Cisco ASR 1000 Series will benefit the following types of customers:

- Enterprises experiencing explosive network traffic as mobility, cloud networking, and video and collaboration usage increase: Cisco ASRs consolidate these various traffic streams and apply traffic management and redundancy properties to them to maintain consistent performance among enterprise sites and cloud locations.
- Network service providers needing to deliver high-performance services, such as DCI and branch-office server aggregation, to business customers: Service providers can also use the multiservice routers to deploy hosted and managed services to business and multimedia services to residential customers.
- Existing Cisco 7200 Series Router (end-of-sale) customers looking for simple migration to a new multiservice platform that delivers greater performance with the same design.

Features and benefits

The Cisco ASR 1000 Series Routers carry a modular yet integrated design, so network operators can increase their network capacity and services without a hardware upgrade. With flexibility in the number of connections, speed maximums, and price, you don't have to under- or overprovision for any network location.

Alternatively, you also have the option to buy "-X" and "-HX" models, so you can increase throughput by simply purchasing upgrade licenses as you grow to increase your network speed dynamically.

Cisco Software-Defined WAN

Cisco SD-WAN capability can be enabled on the Cisco ASR 1000 series platforms with IOS-XE. Cisco SD-WAN offers an entirely new way to manage and operate your WAN infrastructure. Cisco SD-WAN is a cloud delivered architecture that offers secure, flexible and rich services with the following key benefits:

- **Better user experience:** The ability to deploy applications in minutes, on any platform, with a consistent user experience. Deliver predictable performance for applications residing in the data center or in the cloud.
- **Greater agility:** Faster, easier deployment and operation of your WAN, and get faster performance using less bandwidth. Add new revenue generating services in minutes not months.
- **Advanced threat protection:** Securely connect your users to applications in minutes and protect your data from the WAN edge to the cloud. Secure segmentation for critical assets and multi-layer, robust security that encrypts all data.

SD-WAN Integrated Security

In order to efficiently connect to multiple cloud infrastructures many enterprise customers want to build an SD-WAN infrastructure that uses Direct Internet Access (DIA). This can save costs and reduce complexity by reducing WAN traffic backhauled to your data centers; however connecting branches directly to the internet without the right security controls exposes your network to threats and vulnerabilities.

With Cisco SD-WAN and the ASR 1000 series platforms, you have integrated security built-right-in for branch DIA security with these integrated security capabilities:

- Application aware enterprise firewall
- DNS layer enforcement (Umbrella)

And with Cisco SD-WAN security integration you will reduce complexity by having a single management interface (vManage) for both the network and security.

For more info on Cisco SD-WAN and vManage see: https://www.cisco.com/go/sd-wan.

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Unified access security and multi-factor authentication

Zero trust security model, allows secure connections to all applications (whether on premises or in the cloud) based on the trust worthiness of users and devices.

Table 1 summarizes the features and benefits of the Cisco ASR 1000 Series Routers.

Table 1. Features and benefits of Cisco ASR 1000 Series Routers

Feature	Benefit
High availability	
Redundant hardware components and power supplies	• These components provide system and business continuity. • The ASR 1006, ASR 1006-X, ASR 1009-X, and ASR 1013 have redundant route processors and ESPs. • The ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, and ASR1004 have redundant instances of Cisco IOS XE Software.
Stateful intrachassis redundancy	• Redundant hardware combined with modular software contains faults to prevent system wide failure. • Redundancy across routers is enabled by pairing routers that act as backup for each other. The routers offer 99.999-percent ("five-nines") availability for consistent, high-performance user application experiences.
In-Service Software Upgrade (ISSU) support	• You don't need to schedule downtime windows: changes are made while the system keeps on working, with nonstop routing availability.
Cisco IOS XE Software Sub-package Mode	• You can upgrade individual software components in less time.
Scalable capacity and throughput	
Cisco Flow Processor-based platform	• Advanced services can operate at high speeds without the need for additional hardware or blades.
Hardware acceleration	• Features such as Quality of Service (QoS), cryptography, and Access Control Lists (ACLs) are processed in hardware.
Control- and forwarding-plane separation	• You can scale control and data planes independently of each other.
Investment protection	
Software modularity	• You can mix and match the services that best meet your business needs; you won't "waste" investments on capabilities you don't need.
Pay-as-you-grow licensing with "-X" models	• When you need greater throughput, you simply activate it with a change in software license, rather than having to expend capital for additional hardware.
Cisco Shared Port Adapters (SPAs)	• You can reuse your investment in network I/O across platforms.
Cisco Network Interface Modules (NIMs)	• You can reuse your investment in network I/O across platforms.

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Product portfolio

The Cisco ASR 1000 Series contains 8 models with varying types of I/O connectivity and slots and different maximum throughput rates (Figure 1). All models use the innovative and powerful Cisco Flow Processor and support the same feature set based on the Cisco IOS XE Operating System. All this commonality simplifies management and operations.

- Cisco ASR 1001-X Router (Figure 2)
- Cisco ASR 1002-X Router
- Cisco ASR 1001-HX Router (Figure 3)
- Cisco ASR 1002-HX Router (Figure 4)
- Cisco ASR 1004 Router
- Cisco ASR 1006 Router
- Cisco ASR 1006-X Router
- Cisco ASR 1009-X Router
- Cisco ASR 1013 Router

Figure 1.
Cisco ASR 1000 Series Aggregation Services Routers

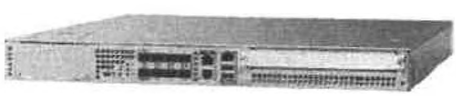


Figure 2.
Cisco ASR 1001-X Router

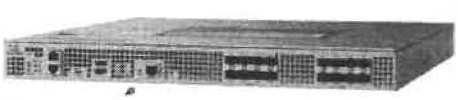


Figure 3.
Cisco ASR 1001-HX Router

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

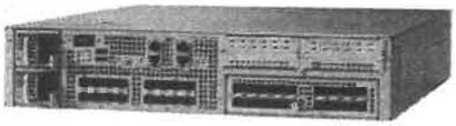


Figure 4.
Cisco ASR 1002-HX Router

Software licensing

Software subscription through Cisco DNA Licensing

The ASR 1000 series supports software based subscription using Cisco DNA based licensing. Two Cisco DNA based software subscription licenses are available for the WAN portfolio: Cisco DNA Advantage and Cisco DNA Premier allowing customers to have a single unified solution that spans across the ASR 1000 series routers and its ISR 1000 and ISR 4000 counterparts.

The license tiers are structured to support the growth in business needs enabling the customer to move from basic functionality at branch to full-functionality with the Cisco DNA Advantage and expanding that to include WAN Optimization and Analytics on the Cisco DNA Premier. This provides complete flexibility to move the same license across end-points based on growing network and security requirements, growth in bandwidth based on user and application growth at the sites as also the ability to change the management of the platform from on-prem to cloud or vice-versa.

Cisco DNA Licenses are supported for ASR 1000 platforms using the Cisco DNA Center, the controller and analytics platform at the heart of Cisco's intent-based network. For more information on the Cisco DNA Center and supported platforms, please refer to https://www.cisco.com/c/en/us/products/cloud-systems-management/dna-center/index.html.

Cisco ONE Software

Cisco ONE™ Software offers a valuable and flexible way to buy software for the WAN, access, and data center domains. At each stage in the product lifecycle, Cisco ONE Software helps make buying, managing, and upgrading your network and infrastructure software easier. Cisco ONE Software provides:

- Flexible licensing models to smoothly distribute customers' software spending over time
- Investment protection for software purchases through software services-enabled license portability
- Access to updates, upgrades, and new technology from Cisco through Cisco® Software Support Services (SWSS)

Cisco ONE for WAN gives organizations broad capabilities for branch offices and the enterprise edge: Cisco ONE Foundation for WAN connects and secures your branch office while optimizing for cost. Cisco ONE WAN Collaboration integrates voice and video into your branch office and network edge.

Software feature licenses are required to activate services on Cisco ASR 1000 Series Routers. Currently, two types of feature licenses are available. Certain services require only a Right-To-Use (RTU) license, whereas other services require both an RTU license and one or more number-of-sessions licenses. All the licenses on the Cisco ASR 1000 Series are honor-based, meaning that the licenses are not enforced through a product activation or license key.

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

For Cisco ASR 1000 Routers, one of the following five packages is required:

- Cisco ASR 1000 IOS XE UNIVERSAL - NO PAYLOAD ENCRYPTION
- Cisco ASR 1000 IOS XE UNIVERSAL
- Cisco ASR 1000 IOS XE UNIVERSAL WITHOUT Lawful Intercept
- Cisco ASR 1000 IOS XE UNIVERSAL - NO PAYLOAD ENCRYPTION WITHOUT Lawful Intercept

To enable a set of required features, one of the following three technology packages is required:

- Cisco ASR 1000 IP Base License
- Cisco ASR 1000 Advanced IP Services License
- Cisco ASR 1000 Advanced Services License

Cisco ASR 1000 Series use cases

Tables 2 and 3 describe enterprise and service provider application examples, respectively.

Table 2. Cisco ASR 1000 Series Enterprise Applications

Deployment scenario	Description	System characteristics
WAN edge: Guarantee high-priority applications by creating a virtual "glass ceiling" for lower-priority applications. Improve user experiences.	• Applies Modular QoS CLI (MQC) policies on VLANs or tunnels • Limits an arbitrary collection of low-priority traffic to a certain bandwidth • Classifies based on Differentiated Services Code Point (DSCP), Network-Based Application Recognition (NBAR), and Cisco IOS Cisco IOS FPM (FPM) into numerous hierarchies, one for high priority and one for low priority	• Implements flexible hierarchies • Supports 464,000 queues • Allows all queues to have a minimum, maximum, and excess bandwidth with priority propagation
Multiservice, scalable, and secure headend: **IP Security (IPsec) VPN aggregation scales to meet the new bandwidth demands of service provider IP VPNs.**	• Reduces Capital Expenditures (CapEx) and Operating Expenses (OpEx) by migrating and consolidating to fewer Cisco ASR 1000 Series Routers • Protects investment through easy transition to much higher encryption support, offering encryption support of up to 78 Gbps with the 200-Gbps Cisco ASR 1000 Series ESP (ASR1000-ESP200) • Offers easier management through embedded security services in the Cisco Flow Processor, with no additional service modules or blades required • Optimized for QoS and IP Multicast applications	• Supports thousands of sites • Supports 8,000 IPsec tunnels • Offers up to 78-Gbps encryption performance and up to 200-Gbps noncryptographic throughput support with the Cisco ASR 1000 Series 200-Gbps Embedded Services Processor (ASR1000-ESP200) engine

ВЯРНО С ОРИГИНАЛА

Deployment scenario	Description	System characteristics
Embedded high-speed firewall: **With the Zone-Based Policy Firewall, the Cisco ASR 1000 Series acts as an implicit and complete barrier between any interfaces not members of the same zone. An explicit zone-pair policy must be specified (using Cisco Policy Language; that is, MQC) in each direction between each zone pair. The policy establishes within the router the kind of stateful inspection (Layer 4, Layer 7, or application) and session parameters to apply to each zone pairing.** **Example: An explicit policy allowing HTTP and Domain Name System (DNS) to traverse the Internet-demilitarized zone (DMZ) zone boundary would be required.**	• The firewall is embedded in the Cisco Flow Processor; no additional service blades or modules are required • Multiple gigabits of bandwidth are routed while at the same time the router performs Zone-Based Policy Firewall and other baseline features such as QoS, IPv4, IPv6, NetFlow, and others • The Cisco ASR 1000 Series provides logging of all firewall session states off to network management applications capable of accepting relatively huge amounts of flow data. Third-party applications can handle the session data	• Provides firewall performance of 2.5 to 200 Gbps, depending on the ESP used • Offers high-speed logging of 40,000 sessions per second with NetFlow Version 9
Managed CPE: This implementation of branch-office architecture offers powerful investment protection with services and scale.	• Managed Customer Premises Equipment (CPE) helps branch offices route correctly over various types of Ethernet to comply with Service-Level Agreements (SLAs) • This application encrypts multiple gigabits of bandwidth without any additional service blades or modules • Managed CPE optimizes the WAN to route around brownouts in the service provider network to further guarantee mission-critical applications • This application offers small form factors (1 Rack Unit [1RU] for the Cisco ASR 1001-X and ASR 1001-HX and 2RUs for the Cisco ASR 1002-HX and ASR 1002-X Routers) • Note: ISSU is not supported on Cisco ASR 1001-X, ASR 1001-HX, ASR 1002-HX, ASR 1002-X, or ASR 1004. Managed CPE offers accessibility even when the Cisco IOS Software is down	• Offers first-in-industry software redundancy support, without any additional hardware module, on Cisco ASR 1001-X, ASR 1001-HX, ASR 1002-HX, ASR 1002-X, and ASR 1004; hardware redundancy and ISSU are supported on the Cisco ASR 1006 and ASR 1013 • Offers powerful firewall and NAT performance of 2.5 to 200 Gbps and 1.8- to 78-Gbps encryption support in addition to WAN optimization and voice features

Table 3. Cisco ASR 1000 Series service provider applications

Deployment scenario	Description	System characteristics
Broadband L2TP Access Concentrator (LAC) or L2TP Network Server (LNS): **The solution offers Layer 2 Tunneling Protocol (L2TP) endpoint-to-tunnel Point-to-Point Protocol (PPPoX) or IP sessions with bandwidth demands in the STM-1 ATM, Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet range.**	• The application is ideal for triple-play (data, voice, and video) wholesale deployments • It offers integral service delivery • Per-user firewall, Session Border Controller (SBC), etc. are supported	• Provides very high scalability of up to 64,000 subscribers and up to 16,000 tunnels

ВЯРНО С ОРИГИНАЛА

A1

Deployment scenario	Description	System characteristics
Service provider edge: Layer 3 VPN (L3VPN) provider edge: **Example: You can deploy the solution at the distributed provider edge or provider edge in global VPN networks for bandwidth demands such as asymmetric DSL (ADSL), T1/E1, STM-1, STM-4, Fast Ethernet, Gigabit Ethernet, etc.**	• The application provides integral services in the Cisco Flow Processor • It provides encryption, FPM, NBAR, SBC, IP Multicast, etc	• Offers excellent multicast performance • Scales to 8,000 Virtual Route Forwarding (VRF) instances, 1 million Label Distribution Protocol (LDP) labels, and 4,000 Access Control Lists (ACLs) • Supports up to 4 million IPv4 routes • Supports up to 4 million IPv6 routes
Service provider edge: High-end route reflector: **You can use the solution as a route reflector for bandwidth support of 40 Gbps.**	• The application provides high scalability • It offers a modular design of the route processor and ESP with hardware and software redundancy	• Scales up to 29 million IPv4 routes • Supports 64,000 Layer 3 adjacencies
Next-generation voice and multimedia example: Cisco Unified Border Element Enterprise Edition (ENT Edition): **The SBC application (named Cisco Unified Border Element [ENT Edition]) performs the voice and video gateway functions simultaneously with regular IP data services. No appliance or additional service blade is required. The control protocols and media protocols work transparently within a complex voice architecture. For more information, refer to the CUBE data sheet at https://www.cisco.com/go/cube.**	• Secure and authenticated Session Initiation Protocol (SIP) trunk connections enable service providers to offer real-time voice and video services • The WAN edge is simpler to manage because there is only one egress and one ingress point for access to Internet or service provider services • The control plane is separated from the data-forwarding plane, so the signaling and control processes are separate from media processing • The CUBE SBC application can be used for SIP trunk video and/or audio services provided by service providers or for Internet-accessible SIP line-side services to Cisco Unified Communications Manager	• Facilitates SBC with security, QoS, IPv4, and IPv6 (IP Unicast and IP Multicast simultaneously) • Supports 16,000 simultaneous voice calls and multimedia data of up to 200 Gbps with accounting, firewall, and call quality enabled • Integrated with inbox high-availability infrastructure and Dynamic Host Configuration Protocol (DHCP) Relay

Product specifications

Table 4 compares the different Cisco ASR 1000 Series Routers, and Table 5 compares the different processor module specifications. For comparisons of Cisco ASR ESPs, refer to the ESP datasheet. For comparisons of the ASR route processors, refer to the RP datasheet. For comparisons of the SPAs and SPA interface processors, refer to the SPA/SIP datasheet.

ВЯРНО С ОРИГИНАЛА

A1 ЕАД

Table 4. Cisco ASR 1000 Series: Chassis comparison and specifications

Model	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
Physical specifications **Note:** Depth applies to chassis edge-to-edge dimension and does not include protrusions such as card handles, power-supply handles, and cable management brackets. Refer to the applicable hardware installation guide for additional details.	Height: 1.71 in. (43.43 mm) Width: 17.3 in. (439.42 mm) Depth: 18.17 in. (461.5 mm) Weight: • 25 lb (11.35 kg) fully loaded **Note:** The Cisco ASR 1001-X Router has the route processor, ESP, and SIP integrated	Height: 3.5 in. (88.9 mm) Width: 17.2 in. (437.4 mm) Depth: 18.15 in. (461.0 mm) Weight: • 38.25 lb (17.36 kg) (with dual AC power supply and SPA blank covers) • 39.05 lb (17.72 kg) (with dual DC power supply and blank covers) • No SPAs included **Note:** The Cisco ASR 1002-X has the route processor, ESP, and SIP integrated	Height: 1.71 in. (43.43 mm) Width: 17.3 in. (439.42 mm) Depth: 18.38 in. (466.85 mm) Weight: • 23 lb (10.44 kg) with dual AC power supplies • 22.5 lb (10.21 kg) with dual DC power supplies	Height: 3.5 in. (88.9 mm) Width: 17.3 in. (439.4 mm) Depth: 19.25 in. (489.0 mm) Weight: • 34 lb (15.45 kg) (with dual AC power supplies) • 34 lb (15.45 kg) (with dual DC power supplies)	Height: 7 in. (177.8 mm) Width: 17.2 in. (437.4 mm) Depth: 18.15 in. (461.0 mm) Weight: • 68.7 lb (31.16 kg) (with dual AC power supply, SPA blank covers, Cisco ASR 1000 Series 10-Gbps ESP [ASR1000-ESP10] or ASR 1000 Series 40-Gbps ESP [ASR1000-ESP-40], Cisco ASR 1000 Series Route Processor 1 [RP1] [ASR1000-RP1], two Cisco ASR 1000 Series 10-Gbps SIPs [ASR1000-SIP10] or ASR1000 Series 40-Gbps SIPs	Height: 10.5 in. (266.7 mm) Width: 17.2 in. (437.4 mm) Depth: 18.15 in. (461.0 mm) Weight: • 98.70 lb (44.77 kg) (with dual AC power supply, SPA, route processor, two Cisco ASR 1000 Series 10-Gbps ESPs [ASR1000-ESP10] or ASR 1000 Series 40-Gbps ESPs [ASR1000-ESP-40] or ASR1000 Series 100-Gbps ESPs [ASR1000-ESP100], two Cisco ASR 1000 Series RP1s [ASR1000-RP1], three Cisco	Height: 10.47 in. (265.9 mm) Width: 17.2 in. (437.4 mm) Depth: 18.15 in. (461.0 mm) Weight: • 36.5 lb empty • 112 lb (50.91 kg) (with two fan modules, three AC power supplies, three power bay blanks, two Cisco ASR1000 Series 100-Gbps ESPs [ASR1000-ESP100] or two Cisco ASR1000 Series 100-Gbps ESPs [ASR1000-ESP100-X] or two Cisco ASR1000 Series 200-Gbps ESPs [ASR1000-ESP200-X], two Cisco	• Height: 15.72 in. (399.3 mm) • Width: 17.2 in. (437.4 mm) • Depth: 18.15 in. (461.0 mm) • Weight: • 50 lb empty • 154 lb (70 kg) (with three fan modules, four AC power supplies, two power bay blanks, two Cisco ASR1000 Series 100-Gbps ESPs [ASR1000-ESP100] or two Cisco ASR1000 Series 100-Gbps ESPs [ASR1000-ESP100-X] or two Cisco ASR1000 Series 200-Gbps ESPs [ASR1000-ESP200] or two Cisco ASR1000	• Height: 22.8 in. (579.1 mm) • Width: 17.2 in. (437.4 mm) • Depth: 18.15 in. (461.0 mm) • Weight: • 184.0 lb (83.46 kg) (with redundant AC power supply, SPA, route processor, SIP blank covers, two Cisco ASR 1000 Series 40-Gbps ESPs [ASR1000-ESP40] or ASR1000 Series 100-Gbps ESPs [ASR1000-ESP100] or ASR1000 Series 100-Gbps ESPs [ASR1000-ESP100-X] or ASR1000 Series 200-Gbps ESPs [ASR1000-ESP200]

ВЯРНО С ОРИГИНАЛА

Model	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					[ASR1000-SIP-40], and no SPAs)	ASR 1000 Series 10-Gbps SIPs [ASR1000-SIP10] or ASR1000 Series 40-Gbps SIPs [ASR1000-SIP-40], and no SPAs)	ASR 1000 Series RP2s [ASR1000-RP2], two Cisco ASR 1000 Series 100-Gbps MIPs [ASR1000-MIP100], four EPA blanks, and no EPAs)	0 Series 200-Gbps ESPs [ASR1000-ESP200-X], two Cisco ASR 1000 Series RP2s [ASR1000-RP2], three Cisco ASR 1000 Series 100-Gbps MIPs [ASR1000-MIP100], six EPA blanks, and no EPAs)	, two Cisco ASR 1000 Series RP2s [ASR1000-RP2], six Cisco ASR 1000 Series 40-Gbps SIPs [ASR1000-SIP40], and no SPAs)
Default memory	8-GB DRAM shared across route processor, ESP, and SIP	4-GB DRAM shared across route processor, ESP, and SIP	8-GB DRAM shared across route processor, ESP, and MIP	16-GB DRAM shared across route processor, ESP, and MIP	4-GB DRAM RP1 8-GB DRAM RP2	4-GB DRAM RP1 8-GB DRAM RP2	8-GB DRAM RP2 8-GB DRAM RP3	8-GB DRAM RP2 8-GB DRAM RP3	8-GB DRAM RP2 8-GB DRAM RP3
Number of SIPs or Ethernet line cards supported	Integrated in chassis	Integrated in chassis	Integrated in chassis	Integrated in chassis	2	3	2	3	6
Shared port adapters	1 single-height SPA slot	3 SPA slots	N/A	N/A	8 SPA slots	12 SPA slots	8 SPA slots	12 SPA slots	24 SPA slots
Ethernet port adapters	N/A	N/A	N/A	1 EPA slot	N/A	N/A	4 EPA slots	6 EPA slots	12 EPA slots
Cisco ASR 1000 Series ESP	Integrated in chassis	Integrated in chassis	Integrated in chassis	Integrated in chassis	1 ESP slot	2 ESP slots	2 ESP slots	2 ESP slots	2 ESP slots
Route processor	Integrated in the chassis: Cisco ASR 1001-X	Integrated in the chassis: Cisco ASR 1002-X	Integrated in the chassis: Cisco ASR 1001-HX Series	Integrated in the chassis: Cisco ASR 1002-HX	1 route-processor slot	2 route-processor slots	2 route-processor slots	2 route-processor slots	2 route-processor slots

ВЯРНО С ОРИГИНАЛА

Model	Cisco ASR 1001-X Series Route Processor with Quad Core Processor	Cisco ASR 1002-X Series Route Processor with Quad Core Processor	Cisco ASR 1001-HX Route Processor	Cisco ASR 1002-HX Series Route Processor	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
Redundancy	Software: Yes	Software: Yes	Software: Yes	Software: Yes	Software: Yes	Hardware: Yes	Hardware: Yes	Hardware: Yes	Hardware: Yes
Built-in Gigabit Ethernet ports	Yes: 6 Gigabit Ethernet Small Form-Factor Pluggable (SFP) ports	Yes: 6 Gigabit Ethernet SFP ports	Yes: 8 Gigabit Ethernet SFP ports, plus optional 4 configurable 1GE/10GE ports	Yes: 8 Gigabit Ethernet SFP ports	0	0	0	0	0
Built-in 10 Gigabit Ethernet port	Yes: Two 10 Gigabit Ethernet Small Form-Factor Plus Pluggable (SFP+) ports Note: Built-in 10-GB ports cannot be reduced to 1-GB speed.	No	Yes, Four 10 Gigabit Ethernet Small Form-Factor Plus Pluggable (SFP+) ports, plus optional 4 configurable 1GE/10GE ports	Yes: Eight 10 Gigabit Ethernet Small Form-Factor Plus Pluggable (SFP+) ports Note: Built-in 10-GB ports cannot be reduced to 1-GB speed	No	No	No	No	No
Network interface module	Yes	No	No	Yes	No	No	No	No	No

ВЯРНО С ОРИГИНАЛА

A1

Table 5. Cisco ASR 1000 Series processor module comparison and specifications

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
ESP support	Cisco ASR 1000 Series 2.5-Gbps ESP (default) Upgradable through a software-activated feature license to 5, 10, or 20 Gbps	Cisco ASR 1002-X ESP with 5-Gbps (default) Upgradable through software-activated feature license to 10, 20, or 36 Gbps	Integrated ESP up to 60 Gbps throughput	Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100) equivalent	Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10), noncrypto Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10-N), Cisco ASR 1000 Series 20-Gbps ESP (ASR1000-ESP20), and Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40)	Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10), noncrypto Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10-N), Cisco ASR 1000 Series 20-Gbps ESP (ASR1000-ESP20), Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40), and Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100)	Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40), Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100), Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X) and ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200-X)	Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40), Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100), Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X), and Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200) and Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200-X)	Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40), Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100), Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X),and Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200)
ESP bandwidth	2.5 to 20 Gbps	5 to 36 Gbps	60 Gbps	100 Gbps	10 to 40 Gbps	10 to 100 Gbps	40 to 100 Gbps	40 to 200 Gbps	40 to 200 Gbps
ESP memory	Share the same control memory on route	Share the same control memory on route ...ocessor	Share the same control memory on route processor	Share the same control memory on route processor	Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10)	Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10) and ASR 1000 Series 10-Gbps ESP (ASR1000-	Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40): 8-GB	Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40): 8-GB DRAM Cisco ASR 1000	Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40): 8-GB DRAM

ВЯРНО С ОРИГИНАЛА

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					and ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10): 2-GB DRAM default; 2-GB DRAM maximum Cisco ASR 1000 Series 20-Gbps ESP (ASR1000-ESP20): 4-GB DRAM default; 4-GB DRAM maximum	ESP10): 2-GB DRAM default; 2-GB DRAM maximum Cisco ASR 1000 Series 20-Gbps ESP (ASR1000-ESP20): 4-GB DRAM default; 4-GB DRAM maximum Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40): 8-GB DRAM Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100): 16-GB DRAM	DRAM Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100): 16-GB DRAM Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X): 32-GB DRAM Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200-X): 64-GB DRAM	Series 100-Gbps ESP (ASR1000-ESP100): 16-GB DRAM Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200): 32-GB DRAM Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X): 32-GB DRAM Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200-X): 64-GB DRAM	Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100): 16-GB DRAM Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200): 32-GB DRAM Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X): 32-GB DRAM
SIPs and Ethernet line cards	Integrated in chassis; not upgradable	Integrated in chassis; not upgradable	Integrated in chassis; not upgradable	Integrated in chassis; not upgradable	Supports Cisco ASR 1000 Series 10-Gbps SIP Carrier Card (ASR1000-SIP10), Cisco ASR 1000 Series 40-Gbps SIP	Supports Cisco ASR 1000 Series 10-Gbps SIP Carrier Card (ASR1000-SIP10), Cisco ASR 1000 Series 40-Gbps SIP Carrier Card (ASR1000-SIP40), and ASR 1000 Fixed Ethernet	Supports Cisco ASR 1000 Series 40-Gbps SIP Carrier Card (ASR1000-SIP40), Cisco ASR1000 Series MIP 100-Gbps Carrier Card (ASR1000-	Supports Cisco ASR 1000 Series 40-Gbps SIP Carrier Card (ASR1000-SIP40), Cisco ASR1000 Series MIP 100-Gbps Carrier Card (ASR1000-MIP100), and ASR 1000 Fixed Ethernet	Supports Cisco ASR 1000 Series 40-Gbps SIP Carrier Card (ASR1000-SIP40), Cisco ASR1000 Series MIP 100-Gbps Carrier Card (ASR1000-MIP100), and ASR

ВЯРНО С ОРИГИНАЛА

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					Carrier Card (ASR1000-SIP40), and ASR 1000 Fixed Ethernet Line Cards; two 10 GE + twenty 1 GE line cards (ASR1000-2T+20X1GE); and six 10 GE line cards (ASR1000-6TGE)	Line Card; two 10 GE + twenty 1 GE line cards (ASR1000-2T+20X1GE); and six 10 GE line cards (ASR1000-6TGE)	MIP100), and ASR 1000 Fixed Ethernet Line Card; two 10 GE + twenty 1 GE line cards (ASR1000-2T+20X1GE); and six 10 GE line cards (ASR1000-6TGE)	Line Card; two 10 GE + twenty 1 GE (ASR1000-2T+20X1GE) line cards; and six 10 GE line cards (ASR1000-6TGE)	1000 Fixed Ethernet Line Card; two 10 GE + twenty 1 GE (ASR1000-2T+20X1GE) line cards; and six 10 GE line cards (ASR1000-6TGE)
Embedded hardware-based encryption **(highest throughput numbers are for 1400B packets)**	Yes: Up to 8-Gbps crypto support throughput	Yes: Up to 4-Gbps crypto support throughput	Yes: Up to 16-Gbps crypto support throughput	Yes: Up to 25-Gbps crypto support throughput	Yes: On Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10) with up to 4 Gbps and on Cisco ASR 1000 Series 20-Gbps ESP (ASR1000-ESP20) with up to 8-Gbps crypto support throughput **Note:** No support on noncrypt	Yes: On Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10) with up to 4-Gbps crypto support throughput, Cisco ASR 1000 Series 20-Gbps ESP (ASR1000-ESP20) with up to 8-Gbps crypto support throughput, Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40) with up to 11-Gbps crypto support throughput,	Yes: On Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40) with up to 11-Gbps crypto support throughput, Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100) with up to 29-Gbps crypto support throughput, Cisco ASR 1000	Yes: On Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40) with up to 11-Gbps crypto support throughput, Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100) with up to 29-Gbps crypto support throughput, Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200) with up to 78-Gbps crypto	Yes: On Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40) with up to 11-Gbps crypto support throughput, Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100) with up to 29-Gbps crypto support throughput, and Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200) with up to

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
					o Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10-N)	and Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100) with up to 29-Gbps crypto support throughput **Note:** No support on noncrypto Cisco ASR 1000 Series 10-Gbps ESP (ASR1000-ESP10-N)	Series 100-Gbps ESP (ASR1000-ESP100-X) with up to 142-Gbps crypto support throughput and Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200-X) with up to 197-Gbps crypto support throughput	support throughput, Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X) with up to 142-Gbps crypto support throughput and Cisco ASR 2000 Series 100-Gbps ESP (ASR1000-ESP200-X) with up to 197-Gbps crypto support throughput	78-Gbps crypto support throughput, Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X) with up to 142-Gbps crypto support throughput
Minimum Cisco IOS XE Software release	Cisco IOS XE Software Release 3.12.0	Cisco IOS XE Software Release 3.7.0S	Cisco IOS XE Software Release 16.3.1S	Cisco IOS XE Software Release 16.2.1S	Cisco IOS XE Software Release 2.1	Same as for Cisco ASR 1002 except Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40) requires Cisco IOS XE Software Release 3.1.0S **Note:** Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100) requires Cisco IOS XE	Cisco IOS XE Software Release 3.16.0 **Note:** Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X) and Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200-	Cisco IOS XE Software Release 3.16.0 **Note:** Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X) and Cisco ASR 1000 Series 200-Gbps ESP (ASR1000-ESP200-X) requires Cisco IOS XE Software Release 17.2	Cisco ASR 1000 Series 40-Gbps ESP (ASR1000-ESP40) requires Cisco IOS XE Software Release 3.1.0S, ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100) requires Cisco IOS XE Software Release 3.7.0S, and ASR 1000 Series

ВЯРНО С ОРИГИНАЛА

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
						Software Release 3.7.0S.	X) requires Cisco IOS XE Software Release 17.2		200-Gbps ESP (ASR1000-ESP200) requires Cisco IOS XE Software Release 3.10.0S **Note:** Cisco ASR 1000 Series 100-Gbps ESP (ASR1000-ESP100-X) requires Cisco IOS XE Software Release 17.2
Rack-mounting	Yes: 19-inch	Yes: 19-inch	Yes: 19-inch	Yes: 19-inch	Yes: 19-inch	Yes: 19-inch	Yes: 19-inch	Yes: 19-inch	Yes: 19-inch
Wall-mounting	No	No	No	No	No	No	No	No	No
External USB flash memory	1-GB USB flash-memory support	1-GB USB flash-memory support	1-GB USB flash-memory support	1-GB USB flash-memory support	1-GB USB flash-memory support	1-GB USB flash-memory support	1-GB USB flash-memory support	1-GB USB flash-memory support	1-GB USB flash-memory support
Redundant power supply	Yes: Dual power supplies by default; option of either AC or DC power supply **Note:** A mix of one AC and one DC power supply is not supported.	Same as for Cisco ASR 1002	Yes: Dual power supplies by default; option of either AC or DC power supply **Note:** A mix of one AC and one DC power supply is not supported.	Yes: Dual power supplies by default; option of either AC or DC power supply **Note:** A mix of one AC and one DC power supply is not supported.	Same as for Cisco ASR 1002	Same as for Cisco ASR 1002	Yes: Dual power supplies by default, expandable up to a total of six, depending on configuration and redundancy preferences; option of either 1100W AC or 950W DC **Note:** A	Yes: Dual power supplies by default, expandable up to a total of six, depending on configuration and redundancy preferences; option of either 1100W AC or 950W DC **Note:** A mix of AC and DC power	Yes: Quad power supplies (redundant pairs) by default; option of either AC or DC power supplies **Note:** A mix of AC and DC power supplies is not supported

ВЯРНО С ОРИГИНАЛА

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
							mix of AC and DC power supplies is not supported.	supplies is not supported.	
Power input	Worldwide ranging AC input range (85 to 264 VAC) Worldwide ranging DC (-40 to -72V; 48V nominal)	Same as for Cisco ASR 1002	Worldwide ranging AC input range (85 to 264 VAC) Worldwide ranging DC (-40 to -72; -48V nominal)	Worldwide ranging AC input range (85 to 264 VAC) Worldwide ranging DC (-40 to -72; -48V nominal)	Same as for Cisco ASR 1002	Same as for Cisco ASR 1002	Worldwide ranging AC input range (85 to 264 VAC) Worldwide ranging DC (-40 to -72; -48V nominal)	Worldwide ranging AC input range (85 to 264 VAC) Worldwide ranging DC (-40 to -72; -48V nominal)	Worldwide ranging AC (180 to 264V; 240V; 60 or 50 Hz nominal) Worldwide ranging DC (-40.5 to -72; -48V nominal)
Power consumption	• Maximum (DC): 242W • Maximum (AC): 250W • Maximum (out): 250W	• Maximum (DC): 590W • Maximum (AC): 560W • Maximum (out): 470W	• Maximum (DC): 360W • Maximum (AC): 360W • Maximum (out): 360W	• Maximum (DC): 500W • Maximum (AC): 500W • Maximum (out): 500W	• Maximum (DC): 1020 W • Maximum (AC): 960W • Maximum (out): 765W	• Maximum (DC): 1700W • Maximum (AC): 1600W • Maximum (out): 1275W • Or • Maximum (DC): 2100W • Maximum (AC-high line): 2000W • Maximum (out): 1695W	• Maximum (DC): 4600W • Maximum (AC): 4500W • Maximum (out): 4030W	• Maximum (DC): 5200W • Maximum (AC): 5100W • Maximum (out): 4575W	• Maximum (DC): 4200W • Maximum (AC-high line): 4000W • Maximum (out): 3390W
Airflow	Front-to-back	Front-to-back	Front-to-back	Front-to-back	Front-to-back	Front-to-back	Front-to-back	Front-to-back	Front-to-back
Operating temperature (nominal)	32 to 104°F (0 to 40°C)	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X
Operating temperature (shor	32 to 122°F (0 to 50°C)	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
term)									
Operating humidity (nominal) (relative humidity)	10 to 85%	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X
Operating humidity (short-term)	5 to 90%	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1002
Storage temperature	-40 to 150°F (-40 to 70°C)	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X
Storage humidity (relative humidity)	5 to 95%	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X
Operating altitude	-500 to 10,000 feet (-152 to 3048 meters)	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X
Network Equipment Building Standards (NEBS)	GR-1089 and GR-63	GR-1089 and GR-63	GR-1089 and GR-63	GR-1089 and GR-63	GR-1089 and GR-63	GR-1089 and GR-63	GR-1089 and GR-63	GR-1089 and GR-63	GR-1089 and GR-63
EMC standards	• FCC 47 CFR Part 15 Class A • VCCI Class A • AS/NSZ Class A • ICES-003 Class A • EN55022 /CISPR 22 Information Technolo	Same as for Cisco ASR 1001-X	**Emissions** • FCC 47CFR15 Class A • AS/NZS CISPR 22 • CISPR 22 Class A • EN55022 Class A • ICES-003 Class A • VCCI Class A • CNS-13438 Class A • EN61000-	**Emissions** • FCC 47CFR15 Class A • AS/NZS CISPR 22 • CISPR 22 Class A • EN55022 Class A • ICES-003 Class A • VCCI Class A • CNS-13438 Class A • EN61000-	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X	Same as for Cisco ASR 1001-X

ВЯРНО С ОРИГИНАЛА

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
	s) • EN55024/CISPR 24 Information Technology Equipment • (Immunity) • EN300 386 Telecommunications Network Equipment • (EMC) • EN50082-1/EN61000-6-1 Generic Immunity Standard		3-2 • EN61000-3-3 • Immunity • IEC/EN61000-4-2 Electrostatic Discharge Immunity • IEC/EN61000-4-3 Radiated Immunity • IEC/EN61000-4-4 EFT-B Immunity • IEC/EN61000-4-5 Surge • IEC/EN61000-4-6 Immunity to Conducted Disturbances • IEC/EN61000-4-8 Power Frequency Magnetic Field Immunity • IEC/EN61000-4-11 Voltage Dips, Short Interruptions, and Voltage Variations **ETSI/EN** • EN55022/CISPR 22 Information Technology Equipment (Emissions) • EN55024/CISPR 24 Information Technology Equipment (Immunity) • EN300 386 Telecommunications	3-2 • EN61000-3-3 **Immunity** • IEC/EN61000-4-2 Electrostatic Discharge Immunity • IEC/EN61000-4-3 Radiated Immunity • IEC/EN61000-4-4 EFT-B Immunity • IEC/EN61000-4-5 Surge • IEC/EN61000-4-6 Immunity to Conducted Disturbances • IEC/EN61000-4-8 Power Frequency Magnetic Field Immunity • IEC/EN61000-4-11 Voltage Dips, Short Interruptions, and Voltage Variations **ETSI/EN** • EN55022/CISPR 22 Information Technology Equipment (Emissions) • EN55024/CISPR 24 Information Technology Equipment					

ВЯРНО С ОРИГИНАЛА

Cisco ASR 1000 Series	Cisco ASR 1001-X	Cisco ASR 1002-X	Cisco ASR 1001-HX	Cisco ASR 1002-HX	Cisco ASR 1004	Cisco ASR 1006	Cisco ASR 1006-X	Cisco ASR 1009-X	Cisco ASR 1013
			Network Equipment • EN50082-1/EN61000-6-1 Generic Immunity Standard	(Immunity) • EN300 386 Telecommunications Network Equipment • EN50082-1/EN61000-6-1 Generic Immunity Standard					
Safety Standard	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1	UL60950-1 CSA C22.2 No. 60950-1-03 EN 60950-1 IEC 60950-1 AS/NZS 60950.1

Ordering information

Cisco ONE Software for WAN is available for the ASR 1000 Series.

Cisco ONE Software offers a complete solution that delivers an optimal experience over any connection while helping you get the most from your WAN investment with secure, fault-tolerant connectivity.

Benefits:

- Connect branch offices and your campus securely at an optimal cost by improving application performance through application protocol acceleration and optimization techniques that offload the WAN.
- Integrate voice and video across branch offices and your campus to increase productivity.

For ordering information for Cisco ONE Software for the ASR 1000 Series, go to https://www.cisco.com/c/en/us/products/software/one-wan/wan-part-numbers.html.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

ВЯРНО С ОРИГИНАЛА

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Support for Cisco Software-Defined WAN

The ASR 1000 series is optimized for Cisco Software Defined WAN (SD-WAN). For enterprises, this means that business critical applications run faster, with more reliability and reduced Operational Expenditure (OpEx). Cisco SD-WAN achieves this by making all branches and Data Centers have the ability to monitor, control, move and report on streams of application data such as specific web (HTTP) traffic for example. The ASR 1000 series has deep packet inspection capability and can accurately identify and control thousands of different applications including custom in-house enterprise applications.

The entire SD-WAN implementation on the ASR 1000 is implemented by managing the end device either from the Cloud or On-Premise through ascending levels of throughput based licenses. All licenses that support Cisco SD-WAN, whether On-Premise or on Cloud are all enabled using Subscription Licenses. These subscription licenses enable all customers to seamlessly transition between On-Premise and Cloud management as needed. The license tiers are structured to support the growth in business needs through simple subscriptions that help simplify the journey to intent-based networking for the WAN.

Cisco SD-WAN subscriptions are aligned across three subscription licenses of **Cisco DNA Essentials, Cisco DNA Advantage and Cisco DNA Premier,** each expanding functionally. The **Cisco DNA Essentials on ISR 1000 and ISR 4000** covers all types of connectivity & router life cycle management, support for Network & application visibility coupled with basic premise and transport security. ASR 1000 series support two Cisco DNA tiers, Cisco DNA Advantage and Cisco DNA Premier. The **Cisco DNA Advantage** provides for Advanced WAN topologies, Application aware policies supported by enhanced network security. The **Cisco DNA Premier** provides for Cloud connectivity with unlimited segmentation, Advanced Application optimization & Network Analytics, secured by advanced threat protection.

For more information on Cisco SD-WAN please refer to https://www.cisco.com/c/en/us/products/software/one-wan-subscription/index.html.

To place an order, visit the Cisco Commerce Workspace.

To get started with the Cisco ASR 1000 Series, refer to the detailed product part numbers and descriptions in the following tables:

- Table 6: Chassis
- Table 7: Processor Modules
- Table 8: Interfaces and Modules

For software image, feature and upgrade license, and more details about the Cisco ASR 1000 Series bundles and how to order the Cisco ASR 1000 Series, refer to the Cisco ASR 1000 Ordering Guide.

Table 6. Ordering Information for Cisco ASR 1000 Series Chassis

Product number	Product description
Cisco ASR 1000 Series Chassis	
ASR1001-X	Cisco ASR 1001-X System, Crypto, 6 built-in GE, Dual P/S
ASR1001-X=	Cisco ASR 1001-X System, Crypto, 6 built-in GE, Dual P/S, Spare
ASR 1001-HX	Cisco ASR1001-HX System, 8x10GE+8x1GE, 2xP/S, optional crypto
ASR 1001-HX=	Cisco ASR1001-HX System, 8x10GE+8x1GE, 2xP/S, optional crypto, spare
ASR1002-HX	Cisco ASR 1002-HX System, 4x10GE+4x1GE built-in, Dual P/S, optional crypto
ASR1002-HX=	Cisco ASR 1002-HX System, 4x10GE+4x1GE built-in, Dual P/S, optional crypto, spare
ASR1002-X	Cisco ASR 1002-X System, Crypto, 6 Built-In GE, Dual P/S
ASR1002-X=	Cisco ASR 1002-X System, Crypto, 6 Built-In GE, Dual P/S, Spare
ASR1004	Cisco ASR 1004 Chassis, Dual P/S
ASR1004=	Cisco ASR 1004 Chassis, Dual P/S, Spare
ASR1006	Cisco ASR 1006 Chassis, Dual P/S
ASR1006=	Cisco ASR 1006 Chassis, Dual P/S, Spare
ASR1006-X	Cisco ASR 1006-X Chassis
ASR1006-X=	Cisco ASR 1006-X Chassis, Spare
ASR1009-X	Cisco ASR 1009-X Chassis
ASR1009-X=	Cisco ASR 1009-X Chassis, Spare
ASR1013	Cisco ASR 1013 Chassis, Redundant P/S
ASR1013=	Cisco ASR 1013 Chassis, Redundant P/S, Spare
Cisco ASR 1000 Series USB Memory Options	
MEMUSB-1024FT	1 GB USB Flash Token for Cisco ASR 1000 Series
MEMUSB-1024FT=	1 GB USB Flash Token for Cisco ASR 1000 Series, Spare

ВЯРНО С ОРИГИНАЛА

Table 7. Ordering information for processor modules

Product number	Product description
Cisco ASR 1000 Series Embedded Services Processor	
ASR1000-ESP20	Cisco ASR 1000 Embedded Services Processor, 20 Gb
ASR1000-ESP20=	Cisco ASR 1000 Embedded Services Processor, 20 Gb, Spare
ASR1000-ESP40	Cisco ASR 1000 Embedded Services Processor, 40 Gb
ASR1000-ESP40=	Cisco ASR 1000 Embedded Services Processor, 40 Gb Spare
ASR1000-ESP100	Cisco ASR 1000 Embedded Services Processor, 100 Gb
ASR1000-ESP100=	Cisco ASR 1000 Embedded Services Processor, 100 Gb Spare
ASR1000-ESP200	Cisco ASR 1000 Embedded Services Processor, 200 Gb
ASR1000-ESP200=	Cisco ASR 1000 Embedded Services Processor, 200 Gb Spare
ASR1000-ESP100-X	Cisco ASR 1000 Embedded Services Processor, 100 Gb
ASR1000-ESP100-X=	Cisco ASR 1000 Embedded Services Processor, 100 Gb Spare
ASR1000-ESP200-X	Cisco ASR 1000 Embedded Services Processor, 200 Gb
ASR1000-ESP200-X=	Cisco ASR 1000 Embedded Services Processor, 200 Gb Spare
Cisco ASR 1000 Series route processor	
ASR1000-RP2	Cisco ASR 1000 Route Processor 2
ASR1000-RP2=	Cisco ASR 1000 Route Processor 2, Spare
ASR1000-RP3	Cisco ASR 1000 Route Processor 3
ASR1000-RP3=	Cisco ASR 1000 Route Processor 3, Spare
ASR1000-RP3-32G-2P	Cisco ASR1000 RP3 w/ 32 GB, 2 Pack
ASR1000-RP3-64G-2P	Cisco ASR1000 RP3 w/ 64 GB, 2 Pack

ВЯРНО С ОРИГИНАЛА

Table 8. Ordering information for interfaces and modules

Product number	Product description
Cisco ASR 1000 Series SPA Interface Processor and Ethernet Line Cards	
ASR1000-SIP40	Cisco ASR 1000 SPA Interface Processor 40
ASR1000-SIP40=	Cisco ASR 1000 SPA Interface Processor 40, SPARE
ASR1000-6TGE	Cisco ASR 1000 Fixed Ethernet Line Card, 6X10GE
ASR1000-6TGE=	Cisco ASR 1000 Fixed Ethernet Line Card, 6X10GE, Spare
ASR1000-2T+20X1GE	Cisco ASR 1000 Fixed Ethernet Line Card, 2X10GE + 20X1GE
ASR1000-2T+20X1GE=	Cisco ASR 1000 Fixed Ethernet Line Card, 2X10GE + 20X1GE, Spare
ASR1000-MIP100	Cisco ASR 1000 Ethernet Line Card, 100 Gb Modular Interface Processor
ASR1000-MIP100=	Cisco ASR 1000 Ethernet Line Card, 100 Gb Modular Interface Processor, spare
EPA-1X100GE	Cisco ASR 1000 1x100GE Ethernet Port Adapter
EPA-1X100GE=	Cisco ASR 1000 1x100GE Ethernet Port Adapter, spare
EPA-2X40GE	Cisco ASR 1000 2x40GE Ethernet Port Adapter (Native QSFP)
EPA-2X40GE=	Cisco ASR 1000 2x40GE Ethernet Port Adapter (Native QSFP), spare
EPA-1X40GE	Cisco ASR 1000 1x40GE Ethernet Port Adapter (2 physical QSFP ports - optional license to enable 2nd port)
EPA-1X40GE=	Cisco ASR 1000 1x40GE Ethernet Port Adapter (2 physical QSFP ports - optional license to enable 2nd port), spare
L-FLA1-EPA-1X40GE	Cisco ASR 1000 1x40GE e-Delivery Port License for EPA-1X40GE
EPA-QSFP-1X100GE	Cisco ASR 1000 1x100GE QSFP Ethernet Port Adapter
EPA-QSFP-1X100GE=	Cisco ASR 1000 1x100GE QSFP Ethernet Port Adapter, spare
EPA-CPAK-2X40GE	Cisco ASR 1000 2x40GE Ethernet Port Adapter (breakout cable)
EPA-CPAK-2X40GE=	Cisco ASR 1000 2x40GE Ethernet Port Adapter (breakout cable), spare
EPA-10X10GE	Cisco ASR 1000 10x10GE Ethernet Port Adapter
EPA-10X10GE=	Cisco ASR 1000 10x10GE Ethernet Port Adapter, spare
EPA-18X1GE	Cisco ASR 1000 18x1GE Ethernet Port Adapter
EPA-18X1GE=	Cisco ASR 1000 18x1GE Ethernet Port Adapter, spare

ВЯРНО С ОРИГИНАЛА

Upgrade paths

Cisco ASR 1000 Series Routers are included in the standard Cisco Technology Migration Program. Refer to https://www.cisco.com/go/tmp and contact your local Cisco account representative for program details. Cisco Services.

Cisco Services make networks, applications, and the people who use them work better together.

Cisco and our certified partners can help make your enterprise WAN edge deployment a success with a broad portfolio of services based on proven methodologies. We can help you establish a secure, resilient WAN architecture and successfully integrate security and Cisco Unified Communications technologies with bandwidth to support video, collaboration, branch-office solutions, and growth in alignment with your business goals.

The Cisco Lifecycle approach to services defines the requisite activities at each phase of the solution lifecycle. Planning and design services expedite solution adoption. Award-winning technical support increases operational efficiency. Optimization services improve performance, resiliency, stability, and predictability and prepare your network and teams for change. For more information, please visit https://www.cisco.com/go/services.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about the Cisco ASR 1000 Series, visit https://www.cisco.com/go/asr1000 or contact your local Cisco account representative. For information about the Cisco ASR 1000 Series bundles, refer to the Cisco ASR 1000 Ordering Guide.

[redacted]

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

ВЯРНО С ОРИГИНАЛА

C78-731632-23 05/2[redacted]

А1

КП2

[redacted]

Превод от английски език

CISCO
Мост към възможното

Информационен лист
Cisco публичен

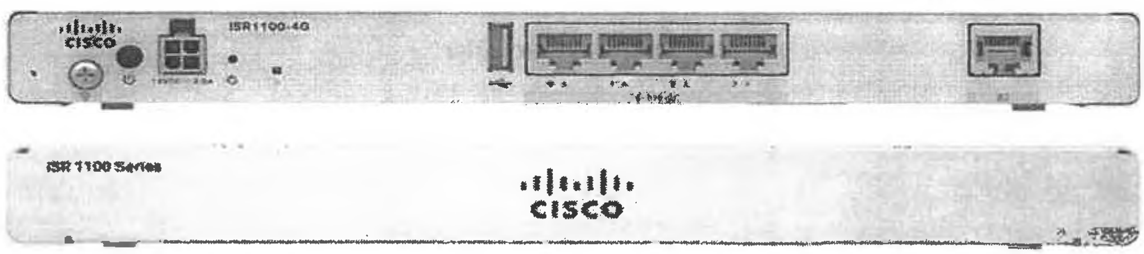
Рутери Cisco ISR1100-4G, 1100-4GLTE и1100-6G

Съдържание

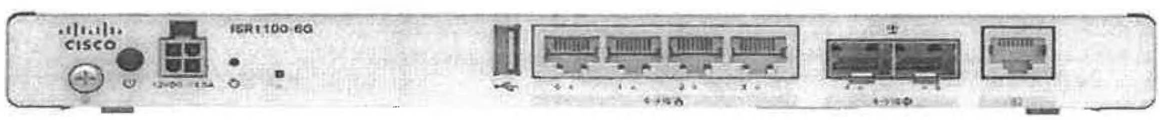
Част от серията Cisco® 1000 рутери за интегрирани услуги (ISR) - моделите ISR 1100-4G, ISR1100-4GLTE и ISR 1100-6G се захранват от операционната система Viptela® и комбинират WAN и цялостна сигурност в една кабелна високоефективна платформа.
ISR 1100-4G, 1100-4GLTE и 1100-6G комбинират една бизнес платформа с най-добрата в този клас SD-WAN.

Софтуерно дефинираната WAN на Cisco (SD-WAN), е първата облачна архитектура, която осигурява несравнима видимост във вашата WAN, оптимално свързване за крайните потребители и най-сигурна платформа за защита на вашата мрежа. Cisco SD-WAN осигурява транспортна независимост, богата мрежа и услуги за сигурност, както и гъвкавост на крайните точки.

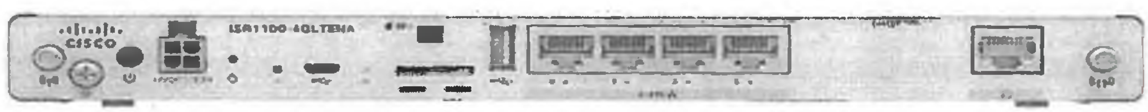
Рутерите ISR 1100-4G, 1100-6G и 1100-4GLTE се доставят като платформи, които се разполагат в периметъра на обекта, като отдалечен офис, браншови офис, кампус или център за данни. Те участват в създаването на сигурна насложена виртуална мрежа върху комбинация от всякакви WAN транспорти.



Фигура 1.
ISR 1100-4G, изглед отпред и отзад



Фигура 2.
ISR 1100-6G, изглед отпред; изгледа отзад е като на ISR 1100-4G по-горе



Фигура 3.
ISR1100-4GLTE изглед отпред; изгледа отзад е като на ISR 1100-4G по-горе

Основни характеристики и предимства

Таблица 1. Бизнес предимства

Бизнес нужда	Характеристики/ описание
Лек, компактен размер с ниска консумация на енергия	• Може да се използва в много различни среди, където пространството, разсейването на топлината и ниската консумация на енергия са критични фактори
Висока производителност за изпълнение на едновременни услуги	• Високата производителност позволява на клиентите да се възползват от скоростите на широколентовата мрежа, докато работи едновременно със защитени данни, глас, видео и безжични услуги.
Висока достъпност и непрекъснатост на бизнеса	• Резервирани WAN връзки за защита от срив и балансиране на натоварването • Динамични протоколи за срив на системата, като Протокол за виртуална резервираност на рутера (VRRP; RFC 2338)
Постоянни високи нива на производителност на приложението	• Рутерът може да изпълнява няколко услуги едновременно с минимално влошаване на производителността. • Cisco SD-WAN предоставя най-доброто потребителско изживяване във всяка връзка.
Намаляване на риска чрез многостепенна сигурност	• Поверителност на данните чрез високоскоростна IP сигурност (IPsec) и криптиране по Усъвършенстван стандарт за криптиране (AES) • Надеждни системи и закотвяне на хардуера
Дистанционна конфигурация и управление за поддържане на ограничен местен ИТ персонал	• Осигуряване на автоматизация със Системата за управление на мрежи Cisco vManage (NMS) • Поддържа отделен конзолен порт
По-ниски разходи за WAN	• Cisco SD-WAN, задвижвана от операционна система Viptela с поддръжка на Overlay Management Protocol (OMP) за оптимизирана WAN връзка, както и лесно за използване решение за управление с Cisco vManage.
Заплащане с растежа на бизнеса: Модел за надграждане на производителността IPsec	• IPsec капацитетът на на рутера може да бъде увеличен с отдалечено изпълнение, надстройка на лиценза при поискване (без надстройка на хардуер) за по-добро управление на бюджета за капиталови разходи.
ИТ консолидация, спестяване на пространство и подобрени Общи разходи за собственост (TCO)	• Единичната конвергирана браншова платформа интегрира възможности за управление на маршрутизирането, сигурността и производителността.

Архитектура и възможности на платформата

Таблица 2. Важни архитектурни елементи

Архитектурни характеристики	Ползи/ Описание
Многоядрена архитектура	• Специализирана равнина на контрола за надеждност на услугата; многоядрена равнина за данни за по-висока производителност в ISR1100-6G
Интегрирани Gigabit Ethernet портове	• Осигурява до четири вградени 10/100/1000 Ethernet порта за WAN или LAN. • Платформата ISR1100-6G разполага с два допълнителни Ethernet порта, които могат да поддържат вграждаема (Pluggable) свързаност, базирана на малък форм-фактор (SFP) в допълнение към RJ-45 връзки, което позволява свързване на медни или оптични проводници.
Достъп чрез конзола	• Конзолният порт RJ45 поддържа свързаност на управлението
Поддръжка на флаш памет	• Рутерите от серия 1100 се доставят с фиксирана двойна серийна флаш памет от 16 MB • Групова флаш памет: 8 GB eMMC pSLC (използваемо хранилище: 5.8 G) • USB портове тип A 3.0 (4.5 W) осигуряват възможности за удобно съхранение
DRA	• Серията ISR1100 се доставя с 4 GB фиксирана DDR4 ECC DRAM

Архитектурни характеристики	Ползи/ Описание
Вградена сигурност на устройството	• Функция на Cisco за предотвратяване на измами • UEFI сигурно зареждане

Таблица 3. Решения за управление на мрежата

Оперативна фаза	Приложение	Описание
Инсталиране, конфигуриране, наблюдение и отстраняване на проблеми в цялата мрежа	Cisco vManage	• Cisco SD-WAN автоматизира гъвкавостта на приложенията при множество връзки, като например Интернет и MPLS • Богатите мрежови и защитни услуги се доставят с няколко прости кликвания. Внедрете оптимизация на WAN, защита на облака, защитна стена, IPS и филтриране на URL адреси в структурата на SD-WAN от едно място • Разширете и управлявайте структурата на SD-WAN във физически или виртуални платформи за браншови офис, кампус, център за данни и облак

Таблица 4. Вградени възможности за управление

Характеристика	Описание
Споразумения за ниво на обслужване на Cisco IP (IP SLAs)	• Ориентирано към приложенията маршрутизиране на базата на SLA и определяне на параметрите на ефективността
Прост протокол за управление на мрежата (SNMP), отдалечен мониторинг (RMON), системна регистрация, CFlowd, експорт на информация за IP потока (IPFix)	• SNMP • Мрежова конференция по SSH, CLI, REST (vManage)

Таблица 5. Характеристики на софтуера и протоколи

Характеристика	Описание
Протоколи	Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), eBGP, iBGP, BGP Router Reflector, статичен, свързан, OMP, 802.1Q, native VLAN, мостови домейни, IRB, режим на хостван мост, нулево доверие,бял списък, защитени от фалшификации модули, DTLS/TLS, IPSec, DDOS защита, защита на равнината за управление, класификация, приоритизация, опашка с ниска латентност, бележки, оформяне, планиране, контрол, огледално дублиране,IGMP v1/v2, PIM, Auto- RP, мащабирана репликация на трафика, реклама на услугата и политика за показване, IPv4, SNMP, NTP, DNS клиент, Dynamic Host Configuration Protocol (DHCP), DHCP клиент, DHCP сървър, транспиация на DHCP, архивиране на конфигурациите, системна регистрация, SSH, SCP, Cflowd v10 IPFIX експорт, IPv6 за транспортната страна, VRRP, MPLS, симетрична NAT, статична NAT, NAT списъци, NAT64, NAT/PAT, NAT траверсиране, разделена DNS, Списъци за контрол на достъпа (ACL)
Капсулиране	Генерично рутинг капсулиране (GRE), IPSec, Ethernet, 802.1q VLAN, CHAP/PAP за PPP през Ethernet (PPPoE)
Управление на трафика	Качество на услугата (QoS), COS маркиране, ориентирано към приложенията маршрутизиране, Претеглено произволно ранно откриване (WRED), наблюдение за загуби/ латентност и нестабилност, политики за маршрутизиране, ориентирано към приложенията маршрутизиране, политика за контрол, политика за данни, ACL политика, политика за VPN членство, мулти-VRF поддръжка, Ефективно маршрутизиране (PfR) Мрежова конференция по SSH, CLI, REST (vManage), Linux shell, ZBFs (Зоново-базирани защитни стени)

КП2

Характеристика	Описание
Криптографски алгоритми	Криптиране: AES-256 (в режими CBC и GCM), Internet Key Exchange (IKE), Cisco PKI Удостоверяване: Удостоверяване, упълномощаване и отчитане (AAA), RSA (2048 bit), Интегриран QAT, ESP-256-CBC, Хедър за удостоверяване, HMAC-SHA1, ECDSA (256/384 bit); Интегритет: HMAC-MD5, SHA-1, SHA-2

Спецификация на продукта

Таблица 6. Серия ISR 1100 и LTE SKUs

Модел	WAN			LAN	Интегрирана USB 3.0 AUX/конзола
	GE (меден проводник)	SFP	LTE (CAT4)	GE (меден проводник)	
ISR1100-4G	4	-	-	4	Да
ISR1100-6G	4	2	-	4	Да
ISR1100-4GLTENA	4	-	Северна Америка	4	Да
ISR1100-4GLTEGB	4	-	LATAM/APAC/EMEAR	4	Да

Спецификации на системата

Таблица 7. Спецификации на системата на серията ISR 1100

Характеристика	Спецификация
Памет (по подразбиране и максимална)	DRAM: 4 GB Флаш: 8 GB (5.8 GB използваеми)
Конзола	• Cisco RJ45 конзолен порт
Удостоверяване и сигурност	• TACACS+ • RADIUS • Локален, базиран на ролята контрол на достъпа
Външно захранване	Спецификации на захранването на продукта: • Външен адаптер: 30W 341-100891-01 • Входно AC напрежение Универсално 100 до 240 VAC • Честота: 50 до 60 Hz • Максимална изходна мощност 30W • Изходно напрежение: +12VDC за захранване на системата
USB 3.0	• Поддържани USB устройства ◦ USB флаш памет • **Бележка:** Поддържаните USB 3.0 устройства да се свързват външно. Вижте USB Device Support Da Sheet.

„ФИДЕС ИНТЕРКОНСУЛТ“ ООД

A1 България ЕАД

Характеристика	Спецификация
LED светлинни сигнали	• Състояние на системата. не свети = няма захранване, зелена постоянно светеща = нормална работа. кехлибарна постоянно светеща = система блокира/ грешка, кехлибарна мигаща = фаза на зареждане • OMP статус: Зелена постоянно светеща = Връзката е нормална. не свети = Връзката е изключена • по 1 зелена за всяка Ethernet; не свети = няма връзка, постоянно свети = осъществена връзка, мигаща = тече трафик • SIM: зелена; не свети = няма SIM, свети постоянно = има SIM, мигаща: тече трафик • по 1 зелена за всеки SFP
Физически размери (Ш x Д x В)	• 10.2 x 7 x 1.1 инча (259 x 178 x 28 mm)
Тегло	• 2.64 паунда (1.08 kg)
Стандартни сертификати за сигурност	• UL 60950-1, второ издание • CAN/CSA C22.2 No. 60950-1, второ издание • EN 60950-1, второ издание • CB to IEC 60950-1, второ издание с всички групови различия и национални варианти • AS/NZS 60950.1:2011 • IEC-62368 (CB and UL/CSA) • NOM-019-SCFI-1998 • GB4943
EMC емисии	• EN55022/CISPR22, CFR 47 Part 15, ICES003, VCCI-V-3, AS/NZS CISPR22, CNS13438, EN300-386, EN61000-3-2, EN61000-3-3, KN22, TCVN 7189, и EN61000-6-1
EMC защита	• EN55024/CISPR24, (EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000- 4-6, EN61000-4-11), EN61000-6-1, KN24, TCVN 7317, и EN300-386
Работен диапазон на околната среда	• Работна температура: От 0 до 40°C (32 до 104° F) на морско равнище (температурата намалява с по 1,5° C на всеки 1000 фута надморска височина, приложимо до максимум 10 000 фута или 3000 m) • Работна надморска височина: Максимум 10 000 фута (3000 m) с 1° C намаляване на всеки 1000 фута • Работна влажност: 0 до 95% относителна влажност без кондензация

Таблица 8. Поддържани LTE честотни ленти

Регион или театър	ISR1100-4GLTENA	ISR1100-4GLTEGB
Честотни ленти	LTE: B2, B4, B5, B12, B13, B14, B17, B66 FDD LTE 1900 MHz (лента 2), 1700 MHz (лента 4), 850 MHz (лента 5), 700 MHz (лента 12, 13, 14, 17), 1700MHz (лента 66) UMTS: B2, B4, B5	LTE: B1, B3, B7, B8, B20, B28 FDD LTE 2100 MHz (лента 1), 1800 MHz (лента 3), 2600 MHz (лента 7), 900 MHz (лента 8), 800 MHz (лента 20), 700 MHz (лента 28) UMTS: B1, B8 GSM/GPRS/EDGE: E-GSM 900, DCS 1800
Теоретична скорост на изтегляне/качване	150 Mbps/50 Mbps	150 Mbps/50 Mbps
САЩ	•	
Европа		•
Канада	•	

A1 България ЕАД
Страница [redacted]

Регион или театър	ISR1100-4GLTENA	ISR1100-4GLTEGB
Близкия изток със специфични LTE диапазони/честоти		•
Югоизточна Азия		•
Латинска Америка		Зависи от конкретните оператори, поддържащи диапазоните LTE, изброени по-горе.

Таблица 9. Cisco LTE спецификации

Елемент	Спецификация
Информация за модема	• Форм фактор на модема: Серия WP7600
Важни LTE характеристики	• Ширина на честотния диапазон 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz и 20 MHz • WCDMA резервираност • Ел. верига като последно средство • SIM-базиран избор на фърмуер на носителя (Verizon, AT&T, Generic)
Поддръжка на SIM	• Един слот за Micro SIM (3FF) карта
Поддържани безжични технологии	Cisco LTE Advanced 3.0 LTE (вижте Таблица 9: Поддържани LTE честотни ленти) Обратна съвместимост: • UMTS и HSPA+
Включена антена	• Две многодиапазонни диполни антени (LTE-ANTM-SMA-D) • За указания за инсталиране на N-антена и кабела, вижте Connected Grid Antennas Installation Guide

Лицензиране и пакетиране на Cisco IOS софтуер

Изображение на софтуера за Cisco SD-WAN

С платформата се доставя една операционна система Cisco SD-WAN, включваща всички функции. Разширените функции могат да бъдат разрешени чрез просто активиране на софтуерен лиценз на изображението. Лицензирането опростява доставката на софтуер и намалява оперативните разходи за внедряване на нови функции.

Таблица 10. Номера на продуктови части и изображения на софтуер

Номер на част от продукта	Описание
Изображение на софтуера на рутера	
Viptela-OS	Viptela-OS версии 19.2.0 и по-нови
Мрежови лицензи	
NETWORK-PNP-LIC	Мрежов лиценз Plug-n-Play за автоматично инсталиране на устройството
Аксесоари	
CAB-CONAUX	Допълнителен конзолен кабел

„ФИДЕС ИНТЕРКОНСУЛТ" ООД

A1 България ЕАД

Номер на част от продукта	Описание
CAB-CONSOLE-RJ45	RJ45 конзолен кабел
CAB-ETH-S-RJ45	Ethernet кабел, RJ45
LTE-ADPT-SM-TF	Антена Cisco LTE SMA
LTE-AE-MAG-SMA	Магнитна основа за удължаване на антената
LTE-ANTM-SMA-D	Диполна антена LTE SMA

Таблица 11. Списък на поддържаните от ISR 1100 вграждаеми устройства с малък форм фактор

Вграждаем с малък форм фактор	ISR 1100-6G	Описание
VIP-SFP-1GE-BASET	Да	Вграждаем трансивър - 1GE BaseT 10/100/1000
VIP-SFP-1GE-LX	Да	Вграждаем трансивър с малък форм фактор - 1GE LX
VIP-SFP-1GE-SX	Да	Вграждаем трансивър с малък форм фактор - 1GE LX

За ръководството за конфигуриране на хардуер и софтуер за маршрутизатори Cisco ISR 1100-4G / 6G / LTE, отидете на:

- https://www.cisco.com/c/en/us/td/docs/routers/sdwan/hardware/isr1100-4g-6g/cisco-isr-1100- 4g-6g-hig.html.
- https://www.cisco.com/c/en/us/support/routers/sd-wan/products-installation-and-configuration- guides-list.html.

Услуги на Cisco и партньорите

Услугите на Cisco и нашите сертифицирани партньори могат да ви помогнат да намалите разходите и сложността на инсталирането в браншовия офис. Техническата поддръжка от Cisco Smart Net Total Care® за серията Cisco ISR 1000 се предлага на базата на еднократен или годишен договор. Опциите за поддръжка варират от асистенция чрез Бюро за помощ до проактивна консултация на място.

За повече информация посетете https://www.cisco.com/go/services.

Информация за поръчка

За да направите поръчка, посетете Cisco Ordering Home Page. За да изтеглите софтуера, посетете Cisco Software Center.

А1 България ЕАД
София

Устойчивост на околната среда на Cisco

Информация за политиките и инициативите на Cisco за устойчивост на околната среда за нашите продукти, решения, операции и разширени операции или верига на доставки е предоставена в раздела "Устойчивост на околната среда" в доклада за Корпоративна социална отговорност (CSR) на Cisco.

Референтните връзки към информация по ключови теми за устойчивост на околната среда (споменати в раздела „Устойчивост на околната среда" в доклада CSR) са дадени в следната таблица:

Тема относно устойчивостта	Препратка
Информация относно законите и разпоредбите за съдържанието на материалите в продуктите	Материали
Информация относно закони и разпоредби за електронните отпадъците, включително продукти, батерии и опаковки	Съответствие с WEEE

Cisco предоставя достъп до данните за опаковките само за информация. Тя може да не отразява най-актуалните правни разработки и Cisco не твърди и не гарантира, че е пълна, точна или актуална. Тази информация подлежи на промяна без предупреждение.

Cisco Капитал

Гъвкави решения за плащане, които ще помогнат да постигнете вашите цели

Cisco Капитал улеснява получаването на правилната технология за постигане на вашите цели, дава възможност за трансформация на бизнеса и ви помага да останете конкурентоспособни. Можем да ви помогнем да намалите общите разходи за собственост, да запазите капитала и да ускорите растежа. В повече от 100 държави нашите гъвкави разплащателни решения могат да ви помогнат да придобиете хардуер, софтуер, услуги и допълващо оборудване на трети страни с лесни и предвидими плащания. Научете повече.

За повече информация

За повече информация относно рутерите серия Cisco ISR 1000 посетете https://www.cisco.com/go/ISR1000 или се свържете с местния представител на Cisco.

Главен офис в Америка
Cisco Systems, Inc.
San Jose, CA

Главен офис в Азия-Тихи океан
Cisco Systems (USA) Pte. Ltd.
Singapore

Главен офис в Европа
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco има над 200 офиса по света. Номерата на телефоните и факсовете са изписани в сайта на Cisco https://www.cisco.com/go/offices.

Подписаният Огнян Петков Кирилов удостоверявам верността на извършения от мен превод от английски на български език на приложения документ – "Рутери Cisco ISR1100-4G, 1100-4GLTE и1100-6G". Преводът се състои от 10 (десет) страници.

Преводач: Огнян Петков Кирилов [redacted]

Отпечатано в [redacted]

C78-742893-02 [redacted] 05/20

A1 България ЕАД

[redacted]

The bridge to possible

Data sheet
Cisco public

Cisco ISR1100-4G, 1100-4GLTE and 1100-6G Routers

ВЯРНО С ОРИГИНАЛА

Contents

Part of the Cisco® 1000 Series Integrated Services Routers (ISR), the ISR 1100-4G, ISR1100-4GLTE and ISR 1100-6G models are powered by the Viptela® operating system and combine WAN and comprehensive security in a wired high-performance platform. The ISR 1100-4G, 1100-4GLTE and 1100-6G combine an enterprise grade platform with best-in-class SD-WAN.

Cisco Software-Defined WAN (SD-WAN) is a cloud-first architecture that provides unparalleled visibility across your WAN, optimal connectivity for end users, and the most comprehensive security platform to protect your network. Cisco SD-WAN provides transport independence, rich network, and security services as well as endpoint flexibility.

The ISR 1100-4G, 1100-6G and 1100-4GLTE routers are delivered as platforms that sit at the perimeter of a site, such as a remote office, branch office, campus, or data center. They participate in establishing a secure virtual overlay network over a mix of any WAN transports.

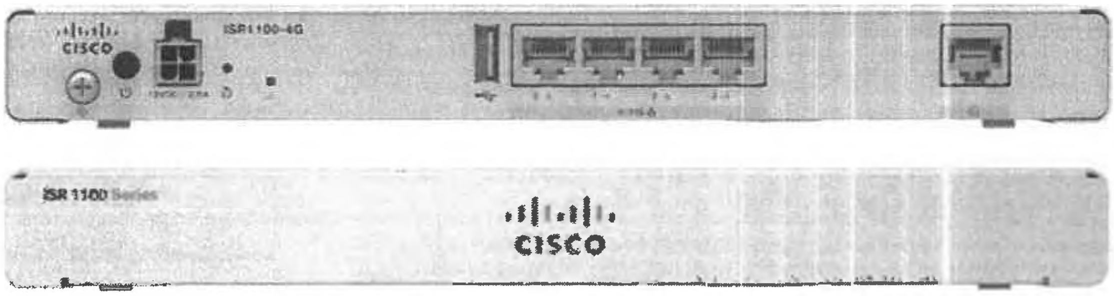


Figure 1.
ISR 1100-4G, front and back view

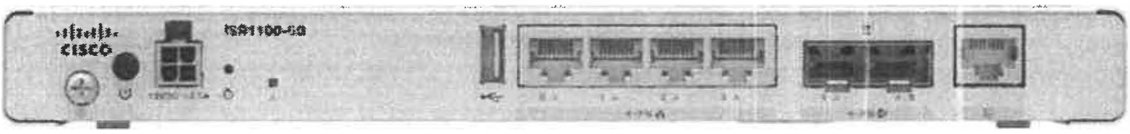


Figure 2.
ISR 1100-6G, front view; back view same as ISR 1100-4G above

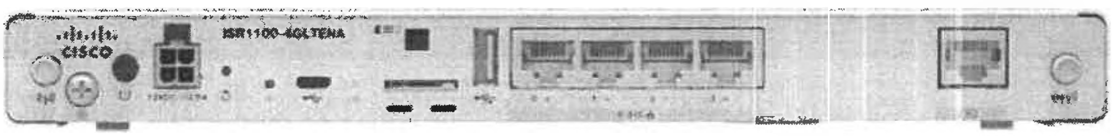


Figure 3.
ISR1100-4GLTE front view, back view same as ISR1100-4G above

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Primary features and benefits

Table 1. Business benefits

Business need	Features/description
Lightweight, compact size with low power consumption	• Can be deployed in many different environments where space, heat dissipation, and low power consumption are critical factors
High performance to run concurrent services	• High performance allows customers to take advantage of broadband network speeds while running secure, concurrent data, voice, video, and wireless services
High availability and business continuity	• Redundant WAN connections for failover protection and load balancing • Dynamic failover protocols such as Virtual Router Redundancy Protocol (VRRP; RFC 2338)
Consistent, high application performance levels	• The router can run multiple services simultaneously with minimal performance degradation. • Cisco SD-WAN delivers the best user experience over any connection.
Risk mitigation with multilevel security	• Data privacy through high-speed IP Security (IPsec) and Advanced Encryption Standard (AES) encryption • Trustworthy systems and hardware anchor
Remote configuration and management to keep local IT staff lean	• Zero-touch provisioning with Cisco vManage Network Management System (NMS) • Supports separate console port
Lower WAN expenditures	• Cisco SD-WAN powered by Viptela operating system with Overlay Management Protocol (OMP) support for optimized WAN connection as well as easy-to-use management solution with Cisco vManage
Pay as you grow: IPsec performance upgrade model	• Router IPsec capacity can be increased with a remote-performance, on-demand license upgrade (no hardware upgrade) for better CapEx budget management
IT consolidation, space savings, and improved TCO	• Single converged branch platform integrates routing, security, and performance management capabilities

Platform architecture and capabilities

Table 2. Architectural highlights

Architectural feature	Benefits/description
Multicore architecture	• Dedicated control plane for service reliability; multicore data plane for higher performance in ISR1100-6G
Integrated Gigabit Ethernet ports	• Provides up to four built-in 10/100/1000 Ethernet ports for WAN or LAN • ISR1100-6G platform has an additional two Ethernet ports that can support Small Form-Factor Pluggable (SFP)-based connectivity in addition to RJ-45 connections, enabling fiber or copper connectivity
Console access	• RJ45 console port supports management connectivity
Flash memory support	• The 1100 Series routers ship with a fixed dual 16 MB serial flash memory • Bulk flash: 8 GB eMMC pSLC (usable storage: 5.8 G) • USB type A 3.0 ports (4.5 W) provide capabilities for convenient storage
DRAM	• The ISR1100 Series comes with 4 GB fixed DDR4 ECC DRAM

ВЯРНО С ОРИГИНАЛА

A1

Architectural feature	Benefits/description
Embedded device security	• Cisco anticounterfeit functionality • UEFI secure boot

Table 3. Network management solutions

Operational phase	Application	Description
Networkwide deployment, configuration, monitoring, and troubleshooting	Cisco vManage	• Cisco SD-WAN automates application flexibility over multiple connections, such as the Internet and MPLS • Rich networking and security services are delivered with a few simple clicks. Deploy WAN optimization, cloud security, firewalling, IPS, and URL filtering across the SD-WAN fabric from a single location • Extend and manage SD-WAN fabric across physical or virtual platforms for branch, campus, data center, and cloud

Table 4. Embedded management capabilities

Feature	Description
Cisco IP Service-Level Agreements (IP SLAs)	• App-aware routing based on SLAs and performance parameter polling
Simple Network Management Protocol (SNMP), Remote Monitoring (RMON), syslog, CFlowd, IP Flow Information Export (IPFix)	• SNMP • Netconf over SSH, CLI, REST (vManage)

Table 5. Software features and protocols

Feature	Description
Protocols	Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), eBGP, iBGP, BGP Router Reflector, static, connected, OMP, 802.1Q, native VLAN, bridge domains, IRB, host-mode bridging, zero-trust, whitelisting, tamper-proof module, DTLS/TLS, IPSec, DDOS protection, control plane protection, classification, prioritization, low latency queuing, remarking, shaping, scheduling, policing, mirroring, IGMP v1/v2, PIM, Auto-RP, scale-out traffic replication, service advertisement and insertion policy, IPv4, SNMP, NTP, DNS client, Dynamic Host Configuration Protocol (DHCP), DHCP client, DHCP server, DHCP relay, config archival, syslog, SSH, SCP, Cflowd v10 IPFIX export, IPv6 for transport-side, VRRP, MPLS, symmetric NAT, static NAT, NAT pools, NAT64, NAT/PAT, NAT traversal, split DNS, Access Control Lists (ACL)
Encapsulations	Generic Routing Encapsulation (GRE), IPSec, Ethernet, 802.1q VLAN, CHAP/PAP for PPP over Ethernet (PPPoE)
Traffic management	Quality of Service (QoS), COS marking, app-aware routing, Weighted Random Early Detection (WRED), loss/latency and jitter monitoring, route policies, app-aware routing, control policy, data policy, ACL policy, VPN membership policy, multi-VRF support, Performance Routing (PfR)
	Netconf over SSH, CLI, REST (vManage), Linux shell, ZBFs (Zone-Based Firewalls)

ВЯРНО С ОРИГИНАЛА

Feature	Description
Cryptographic algorithms	Encryption: AES-256 (in CBC and GCM modes), Internet Key Exchange (IKE), Cisco PKI Authentication: Authentication, Authorization, and Accounting (AAA), RSA (2048 bit), Integrated QAT, ESP-256-CBC, Authentication Header, HMAC-SHA1, ECDSA (256/384 bit); Integrity: HMAC-MD5, SHA-1, SHA-2

Product specifications

Table 6. ISR 1100 Series and LTE SKUs

Model	WAN			LAN	Integrated USB 3.0 AUX/console
	GE (Copper)	SFP	LTE (CAT4)	GE (Copper)	
ISR1100-4G	4	-	-	4	Yes
ISR1100-6G	4	2	-	4	Yes
ISR1100-4GLTENA	4	-	North America	4	Yes
ISR1100-4GLTEGB	4	-	LATAM/APAC/EMEAR	4	Yes

System specifications

Table 7. ISR 1100 Series system specifications

Feature	Specification	
Memory (default and maximum)	DRAM: 4 GB	Flash: 8 GB (5.8 GB usable)
Console	• Cisco RJ45 Console port	
Authentication and security	• TACACS+ • RADIUS • Local, role-based access control	
External power supply	Product power specifications: • External Adapter: 30W 341-100891-01 • AC input voltage: Universal 100 to 240 VAC • Frequency: 50 to 60 Hz • Maximum output power: 30W • Output voltage: +12VDC for system power	
USB 3.0	• USB devices supported: ◦ USB flash memory • **Note:** Supported USB 3.0 devices to be connected externally. View the USB Device Suppor[redacted] Data Sheet.	

ВЯРНО С ОРИГИНАЛА

Feature	Specification
LEDs	• System status: off = no power, green steady on = normal operation, amber steady on = system going down/fault, amber blink = boot up phase • OMP Status: Green steady on = Connection is up, Off = Connection is down • 1x green per Ethernet; off = no link, steady on = link connected, blink = traffic flowing • SIM: green: off = no SIM, steady on = SIM present, blink: traffic flowing • 1x green per SFP
Physical dimensions (W x D x H)	• 10.2 x 7 x 1.1 in (259 x 178 x 28 mm)
Weight	• 2.64 lbs (1.08 kg)
Standard safety certifications	• UL 60950-1, second edition • CAN/CSA C22.2 No. 60950-1. second edition • EN 60950-1, second edition • CB to IEC 60950-1. second edition with all group differences and national deviations • AS/NZS 60950.1:2011 • IEC-62368 (CB and UL/CSA) • NOM-019-SCFI-1998 • GB4943
EMC emissions	• EN55022/CISPR22, CFR 47 Part 15, ICES003, VCCI-V-3, AS/NZS CISPR22, CNS13438, EN300-386, EN61000-3-2. EN61000-3-3, KN22, TCVN 7189, and EN61000-6-1
EMC immunity	• EN55024/CISPR24, (EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-11), EN61000-6-1, KN24. TCVN 7317, and EN300-386
Environmental operating range	• Operating temperature: 0 to 40°C (32 to 104°F) at sea level (temperature derating of 1.5°C per 1000 feet of altitude applicable up to max of 10,000 feet or 3000 m) • Operating altitude: Maximum 10,000 ft (3000 m) with 1°C derating per 1000 ft • Operating humidity: 0 to 95% relative humidity noncondensing

Table 8. LTE Bands Supported

Region or theater	ISR1100-4GLTENA	ISR1100-4GLTEGB
Bands	LTE: B2, B4, B5. B12, B13, B14, B17, B66 FDD LTE 1900 MHz (band 2), 1700 MHz (band 4), 850 MHz (band 5), 700 MHz (band 12, 13, 14, 17), 1700MHz (band 66) UMTS: B2. B4, B5	LTE: B1, B3, B7, B8. B20, B28 FDD LTE 2100 MHz (band 1), 1800 MHz (band 3), 2600 MHz (band 7), 900 MHz (band 8), 800 MHz (band 20), 700 MHz (band 28) UMTS: B1, B8 GSM/GPRS/EDGE: E-GSM 900, DCS 1800
Theoretical download/upload speeds	150 Mbps/50 Mbps	150 Mbps/50 Mbps
United States	•	
Euro		•
Cana	•	

ВЯРНО С ОРИГИНАЛА

A1

Region or theater	ISR1100-4GLTENA	ISR1100-4GLTEGB
Middle East with specific LTE bands/frequencies		•
Southeast Asia		•
Latin America		Dependent upon specific operators supporting the LTE bands listed above.

Table 9. Cisco LTE Specifications

Item	Specification
Modem information	• Modem form factor: WP7600 Series
Important LTE features	• 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz and 20 MHz RF bandwidth • WCDMA fallback • Last resort circuit • SIM based carrier firmware selection (Verizon, AT&T, Generic)
SIM support	• Single Micro (3FF) SIM card socket
Wireless technologies supported	**Cisco LTE Advanced 3.0 LTE (Refer to Table 9: LTE Bands Supported)** **Backward compatibility:** • UMTS and HSPA+
Included antenna	• Two multiband swivel-mount dipole antennas (LTE-ANTM-SMA-D) • For -N antenna and cable installation guidance, view the Connected Grid Antennas Installation Guide

Cisco IOS software licensing and packaging

Cisco SD-WAN software image

A single Cisco SD-WAN operating system encompassing all functions is delivered with the platform. Advanced features can be enabled simply by activating a software license on the image. Licensing simplifies software delivery and decreases the operational costs of deploying new features.

Table 10. Product part numbers and software images

Product part number	Description
Router software images	
Viptela-OS	Viptela-OS versions 19.2.0 and later
Network Licenses	
NETWORK-PNP-LIC	Network Plug-n-Play License for zero-touch device deployment
Accessories	
	Auxiliary console cable

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Product part number	Description
CAB-CONSOLE-RJ45	RJ45 Console cable
CAB-ETH-S-RJ45	Ethernet cable, RJ45
LTE-ADPT-SM-TF	Cisco LTE SMA Antenna
LTE-AE-MAG-SMA	Magnetic Antenna Extension Base
LTE-ANTM-SMA-D	LTE SMA dipole antenna

Table 11. List of Small Form-Factor Pluggables supported with ISR 1100 Series

Small Form-Factor Pluggable	ISR 1100-6G	Description
VIP-SFP-1GE-BASET	Yes	Pluggable transceiver - 1GE BaseT 10/100/1000
VIP-SFP-1GE-LX	Yes	Small form-factor pluggable transceiver - 1GE LX
VIP-SFP-1GE-SX	Yes	Small form-factor pluggable transceiver - 1GE SX

For the Cisco ISR 1100-4G/6G/LTE Routers Hardware and Software Configuration Guide, go to:

- https://www.cisco.com/c/en/us/td/docs/routers/sdwan/hardware/isr1100-4g-6g/cisco-isr-1100-4g-6g-hig.html.
- https://www.cisco.com/c/en/us/support/routers/sd-wan/products-installation-and-configuration-guides-list.html.

Cisco and partner services

Services from Cisco and our certified partners can help you reduce the cost and complexity of branch-office deployments. Cisco Smart Net Total Care™ technical support for the Cisco ISR 1000 Series is available on a one-time or annual contract basis. Support options range from help-desk assistance to proactive, onsite consultation.

For more information, visit https://www.cisco.com/go/services.

Ordering information

To place an order, visit the Cisco Ordering Home Page. To download software, visit the Cisco Software Center.

ВЯРНО С ОРИГИНАЛА

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

For more information about ISR 1000 Series routers, visit https://www.cisco.com/go/ISR1000 or contact your local Cisco account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices.**

Printed in USA

C78-742893-02 05/20

Превод от английски език

Информационен лист

Лого на LiveAction

LiveNX

Платформа за мониторинг на мрежата и ефективността на приложенията

LiveNX събира и анализира данни директно от мрежовите устройства, за да анализира и представя информация за проектиране, проверка на политиките и операциите в цялото предприятие, за да осигури максимална ефективност и оптимално изживяване на клиента.

Общ преглед

Визуализации на потока от край до край в цялата мрежа

Патентованата технология за визуализация на LiveNX опростява мрежовите операции и отстраняване на проблеми. LiveNX корелира множество набори от данни, за да предостави изгледи, графики и карти, които да илюстрират текущото състояние на приложения и производителност на мрежата.

Видимост на приложението и отстраняване на проблеми

Получавате дълбоко разбиране на трафика на приложенията с пълна видимост на протокола и вида на приложението, включително видео, глас, незабавни съобщения, трансфер на файлове и др. Разберете как се използва вашата мрежа, как се изпълняват приложенията и кои санкционирани или несанкционирани приложения се използват.

Интуитивен графичен интерфейс за QoS контрол

Създавайте, редактирайте и прилагайте QoS политики за рутери Cisco и Слой 3 суичъри в работещи мрежи последователно и уверено. QoS съветникът и вградените шаблони са достъпни за прилагане на политики, базирани на най-добрите практики на Cisco или използване на редактора QoS GUI за изграждане на персонализирани политики. LiveNX генерира отчет за одит на QoS, за да показва подробно QoS политиките , включително настройки за конфигурация, проблеми с производителността, спадове и грешка в правилата.

Софтуерно дефинирано управление на WAN

Използвайте визуализациите на приложенията и маршрутите, за ефективно валидиране на възвръщаемост на инвестициите (ROI) във WAN за традиционните MPLS, хибридни или софтуерно дефинирани WAN (SD-WAN). Когато един мрежов елемент прави промяна на пътеката, за да защити приложенията поради условие извън политиката (OOP), LiveNX прави графичните промени на пътеката от край до край. Визуализира мрежовите и наслагващите се пътеки от браншовия офис от доставчика (ите) на услугите до центъра за данни, където се намират приложенията, за получаване на смислена и приложима информация.

LiveNX събира данни в реално време, както от мрежата с много доставчици, така и от специфичните за Cisco REST API (DNA Center, vManage BFD (двупосочно предно откриване) и AppId (Идентификация на приложението за осигуряване на точен визуален анализ)).

Кое е новото

Докладване / Пултове за управление

- Усъвършенствани отчети на WebUI
- Уиджети за достъпност на пултовете
- Подобрено планиране на отчетите и опции за споделяне
- Добавено управление на историята на скорошните отчетите
- Поддръжка в работно време за многоинтерфейсни SNMP отчети
- Въведен пулт за преглед на „Ситуационната осведоменост"
- Подобрения в отчитането на работата на приложенията и глас/видео и подобрения в пулта за управление
- Подобрена поддръжка на IPv6
- DMVPN QoS мониторинг на тунелите
- Катализатор 9k: QoS мониторинг чрез пакетна скорост (CBQoS MIB)
- Добавени са следните отчети:
- Мултикаст одитен доклад
- Обобщени отчети за честотната лента и използване на интерфейса (SNMP)
- Ежедневен обобщен доклад за честотната лента на интерфейса
- Използване на интерфейса над прага за извънреден труд
- Допълнителни шаблони за отчети

Топология

- Подобрена уеб гео-топология за голямомащабни операции

LiveWire

- Поддръжка на SNMP
- Допълнителен кръстосан старт към опциите на Omnipeek

WebUI История

- История на планиране на капацитета на WAN
- История на използване на WAN интерфейса
- Търсене по историята на DN (повиквания)

София 1504, ул. "Св. Климент Охридски" №4
л.: 02/ 946 13 92; тел./факс: 02/ 943 86 65
e-mail: office@fides.bg
www.fides.bg

Управление на устройството/системата

- Групиране на гео-локацията на WebUI
- Персонализирано управление на приложения (w/NBAR)
- Подобрено филтриране на пулта за управление
- Подобрено архивиране и възстановяване на системата за устройства, които не са snmp управлявани
- Поддръжка на актуализиран шаблон на Cisco WLC Netflow (по-висока видимост)
- Гео-топология: поле за текущото състояние на предупредителните сигнали
- Конфигуруемо време за автоматично опресняване на устройството
- Подобрена адаптация на Cisco SD-WAN
- Единично влизане (SSO) чрез SAML (ADFS)

Алармени сигнали

- Уеб: Детайлизиране от алармен сигнал до съответния доклад
- QoS Клас универсален праг за отпадане
- Алармени сигнали с много прагове за:
- Интерфейс, устройство, предупреждения за достъпност на сайта
- Алармени сигнали за CPU/паметта на устройството
- Алармени сигнали за използването на WAN
- Обслужи сега: Инциденти (спешност/ подкатегория полета)
- Подобрения в SD-WAN: vManage алармен сигнал и видимост на събитията
- Режим на поддръжка

LiveAction мрежов анализ (LiveNA) (преглед)

- Устройства, базирани на GPU
- Откриване на аномалии в поведението на приложението
- Разширени анотации и анализи

Облачен мониторинг за AWS/Azure (преглед)

- Видимост от край до край - както в облака, така и в офиса
- Видимост през VPC и VNet трафик
- Видимост на локалната регистрация на потока

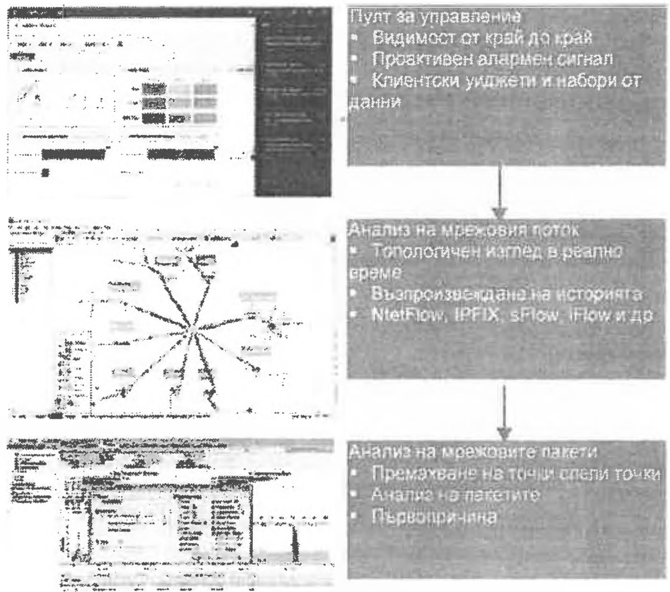
Моля, свържете се с *support@liveaction.com*, ако желаете да видите демонстрация на продуктите - LiveNA и Cloud Monitoring.

Основни характеристики

Бърза реакция на инциденти с анализ на потоците към пакетите Оптимизация на работния поток

Разрешаването на сложни инциденти може да бъде предизвикателство, когато са включени различни системи, доставчици, устройства и софтуер. LiveNX оптимизира бърз работен процес за реакция на инциденти с алармено известие или прогноза, когато събитието е идентифицирано за отстраняване. В рамките на инженерната конзола на LiveNX, NetOps може лесно да изолира проблема с визуалния анализ, представен като топология, изгледи на сайт или устройство.

LiveNX представя времевия отпечатък от алармения сигнал и изолация на проблема от потока на данните, ако е необходим допълнителен анализ, екипът на NetOps може бързо да стартира Omnipeek за задълбочен анализ на пакета за първопричината.



Бързо реагиране на инциденти за по-бързото им разрешаване

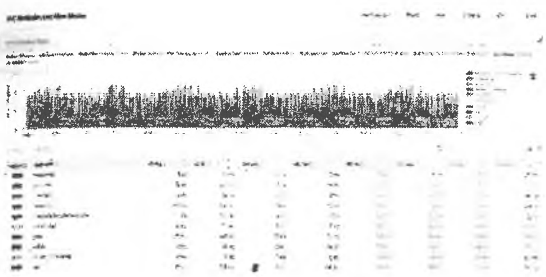
Интеграция на LiveWire за наблюдение на WAN едж сегменти

LiveWire - WAN едж непрекъснат мониторинг

Уредът за наблюдение на мрежата LiveWire е оптимизиран за WAN едж приложения, за да осигури улавяне на пакети и интегрирано решение за IPFIX експорт с LiveNX. LiveWire улавя и преобразува пакетни данни в реално време, които се подават директно в машината за визуализация на LiveNX.

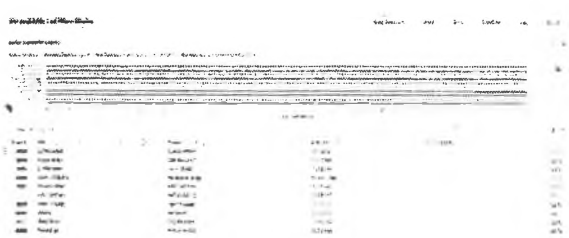
LiveWire и LiveNX заедно предлагат нови визуални представи и анализи в традиционно „тъмните" среди, като например класификация на приложенията и управление на производителността за внедряване на SD-WAN или традиционна наследена среда на много доставчици. LiveWire е изключително мощен за използване при много случаи, включително безжичен мониторинг на браншовете, отстраняване на неизправности при транзакции на пост-терминал и VoIP.

Отчети за видимост и контрол на приложението (AVC)



LiveNX представя разширени данни за ефективността на мрежата с данни от Cisco Отчети за видимост и контрол на приложението (AVC). С тези мрежови данни LiveNX докладва за висока ефективност на приложенията и AVC приложения с латентност, нестабилност, загуба на пакети и разширени показатели за ефективност за: сайтове, устройства, потребители и средата на доставчиците на услуги.

Подобрения на алармените сигнали - видимост на сайта

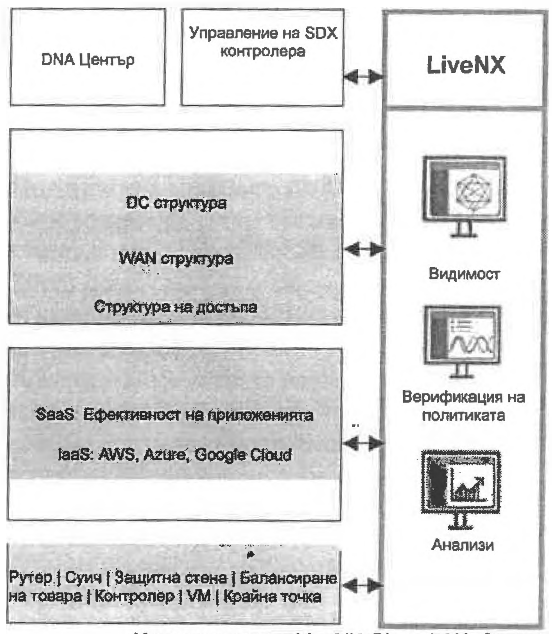


LiveNX Оперативно табло - Текущи алармени сигнали по обекти

LiveNX — Доклад за наличност на сайта

Контролното табло за операции LiveNX сега поддържа отчети за наличност на сайтове и персонализирани уиджети, за да илюстрира обобщен преглед на алармените сигнали. Екипите на NetOps вече могат да визуализират алармените сигнали на таблото за управление на едно място чрез сайта, устройството или интерфейса за по-лесен достъп с обобщени изгледи. Наблюдението за наличието на сайт е една полезна тенденция. Това е мястото, където колебанията трябва да са много малки, а Ключовите показатели за ефективност (KPI) да се контролират стриктно. Като водещ индикатор за възможни нарушения на SLA, опасни зони или лоши сценарии на внедряване, отчетите за наличност на сайта са най-добре интегрирани в Прегледа на нивото на услугата и се свързва с Докладите за ефективността на приложението QoS клас на мрежата.

Cisco интеграция



Интегриране на LiveNX Cisco DNA Center

LiveNX предлага най-широк набор от интеграции за Cisco среди. В LiveNX 8 интегрирането на Cisco DNA Center API вече е достъпно за Обща наличност, в допълнение към Cisco Identity Service Engine (ISE), vManage (SD-WAN), SD-Access и PxGrid конекторите. Тези интеграции предоставят богати набори от данни за напреднали визуални анализи на LiveNX. Топологичните прегледите на потока в реално време и криминалистично възпроизвеждане и анализ са ключови елементи на NetOps

Ключови възможности

Оптимизиран работен процес за потоци и пакети за отстраняване на проблеми в мрежата

Чрез анализ на нивото на потока и пакетите NetOps вече може бързо да изолира проблемните области и да има готов отговор за всеки тежък инцидент.
С топологичните изгледи на потока и интегриран експертен анализ на пакетите LiveNX оптимизира изолацията на проблема до първопричината в цикъла на управление на инцидентите. С интегрирания работен процес на ServiceNow ITOM LiveNX е ключова платформа за NetOps за по-бързо разрешаване на инциденти и докладване на състоянието и въздействието върху бизнеса.

Визуални анализи
Визуализацията ви позволява да разберете по-добре мрежовия трафик, така че да можете да идентифицирате проблемните места.
- Анализ на приложението и пътя на потока
- Поддръжка на много доставчици - NetFlow v5/v9, IPFIX, sFlow и J-Flow
- Нестабилност, закъснение, показатели за загуба на пакети за глас и видео
- Показатели за време на реакция на приложението, време за обратно пътуване, закъснение на сървъра и закъснение на клиента
- NetFlow регистрация на събития по сигурността (NSEL)

• Безжична информация, включително самоличност на потребителя
• Бърза регистрация от защитната стена
• Крайна система (тип устройство, ОС) и информация за крайния потребител
• Интеграция с брокери на мрежови пакети
• Поток DVR за възпроизвеждане на исторически данни
• Вградено разрешаване на имена от Система за имена на домейни (DNS)
• Експорт на топология към Visio

Софтуерно дефиниран WAN мониторинг

GUI-базирано управление за SD-WAN мониторинг за контрол на пътеката и оптимизация на работата на приложението.
• Визуализация на контрола на пътеката
• SD-WAN табло и тенденция
• PfRv3 Поддръжка на много центрове за данни
• Показва каква нестандартна причина задейства промяна на пътеката
• Отчети за трафика по клас/приложение

Поддръжка на Cisco SD-WAN (Viptela)

LiveNX консолидира унифицирано отчитане, инвентаризация и известие за алармени сигнали. За Cisco SD-WAN LiveNX поддържа:
• Поддръжка на платформите Cisco vEdge, cEdge и ENCS
• Поддръжка на Cisco IWAN
• Преглед на топологията по сайтове на Cisco SD-WAN
  • Видимост на наслагване - VPN, тунел
  • Транспорт на доставчик на услуги
  • Състояние на изпълнението
  • Филтриране по приложения, DSCP, VPN или доставчик на услуги
• Анализ по сайтове на Cisco SD-WAN
  • Проверка на политиката
  • Приложение - VPN - DSCP - Доставчика на услуги
Състояние на услугата
• Устройство за инвентаризация Viptela, включително vEdge рутери и устройства за управление като vManage, vBond и vSmart
• Добавя подходящи интерфейси за наблюдение от всеки vEdge рутер.
• Удостоверения за мониторинг на устройства, като например SNMP настройки
• Събера мрежова семантична информация за всяко устройство и интерфейс:
  • Асоциирани сайтове за всяко устройство
  • Геолокация на сайта
  • WAN интерфейси на всяко устройство
  • Доставчик на услуги, свързан с всеки WAN интерфейс.
  Бележка: Viptela refers to the service provider information as 'colors.' Капацитет на WAN връзки (входящи и изходящи)

• Мапинг на IP на сайтовете
• Определя дали дадено устройство е в центъра за данни
• Viptela VPN ID мапинг по VPN име
• vManage API: BFD (Двупосочно разпознаване напред), AppId и аларми.

Поддръжка на Cisco IWAN
• PfR конфигурация на множество главни контролери
• Автоматично научаване на семантични настройки за PfRv3 мониторинг за опростяване на настройката
• Поддръжка на много PfRv3 центрове за данни

QoS Мониторинг
Проследява качеството на QoS за всеки клас.
Мониторингът и алармирането за проблеми с приоритетни опашки осигурява проактивно уведомяване за потенциални проблеми с качеството на гласовата информация.
• Визуализация на приложението NBAR2
• Персонализирани дефиниции на NBAR
• Графики преди и след QoS
• Подробен графичен дисплей на интерфейса и CBQoS статистиката
• 95/99 перцентил, тримесечни, годишни и съпоставени доклади

Алармени сигнали
LiveNX асоциира събития от устройства (рутери, комутатори, защитни стени и др.) с алармите, които се генерират при изпълнение на конкретни критерии, като праг на задействане, и се показват в оперативното табло.
С концепцията за мапинг Аларма - Събитие LiveNX е в състояние да премахне често срещаното оплакване, че броят на създадените аларми е твърде голям, като по този начин показва само алармите, които изискват незабавно внимание.
Сигналите са категоризирани в три нива на тежест:

Критичен:
С най-високата тежест, напр. за аларми, които биха причинили най-големия проблем в мрежата

Предупреждение:
Висока тежест, напр. за сигнали, които показват факти, които са проблемни или ще станат проблемни

Информация:
Ниска тежест, напр. проблем, за който си струва да се знае, но може да не е толкова пагубен за мрежата
Предупрежденията могат да бъдат конфигурирани така, че да се интегрират в работните процеси в индустриални системи за управление на инциденти като ServiceNow и PagerDuty.

QoS конфигурация
Създава, редактира и прилага QoS политики за рутери Cisco и Слой 3 суичъри в работещи мрежи . Използвайте QoS съветникът и вградените шаблони за прилагане на политики, базирани на най-добрите практики на Cisco или използвайте редактора QoS GUI за изграждане на политики.

А1 България ЕАД

• Поддръжка на пълна модулна QoS конфигурация, включително WRED, CBWFQ и приоритетна опашка
• Създаване на йерархична политика за разширени конфигурации
• Персонализирани NBAR2-базирани съвпадения, включително атрибути на високо ниво, HTTP URL, MIME, HOST и RTP протоколи
• Вграден ACL редактор
• Вградени правила за QoS настройки, които осветяват нарушенията
• Пътека за одит на конфигурация
• Общ системен одит на QoS
• Политика за LAN услуга

LAN

Визуализира Протокола за обхващащо дърво. Осигурява визуализации на Слой 2 в реално време за мрежи, включително интерфейс на магистралите, канали на портовете, VLAN асоциации и проценти на честотна лента. Изготвя отчети за Слой 2 на QoS.

Маршрутизиране

Визуализации на маршрутизирането в реално време за мрежи Cisco, които могат да идентифицират проблеми с достъпността, маршрутни цикли и асиметрични пътища, засягащи качеството на трафика. В допълнение, базиран на политиката наблюдател/ редактор на маршрутизацията, осигурява висока степен на контрол върху политиката на трафика, за да маршрутизира трафика лесно и предсказуемо по указани от потребителя пътища.

IP SLA

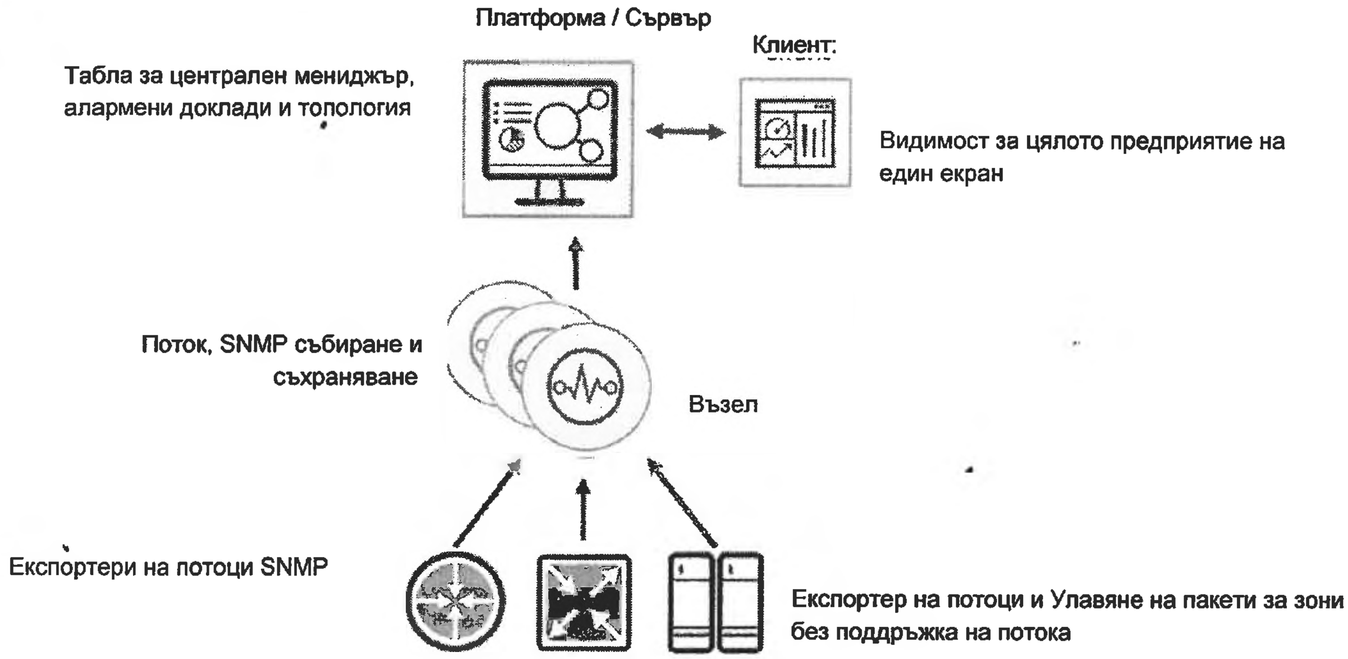
Cisco IOS IP SLA е лесно достъпен за генериране и следене на синтетичен мрежов трафик, за да се определи производителността на мрежата, да се изпробват промените в политиката или активно да се наблюдават ключовите мрежови пътища. Синтетичните типове трафик включват данни (HTTP, FTP, DNS, DHCP) и глас, които могат да се използват за измерване на латентността, загубите, нестабилността и Средна оценка на мнение (MOS) за VoIP. Високо интерактивният графичен интерфейс предоставя функционалността и гъвкавостта на IP SLA функциите, без да е необходимо да научите и използвате командните редове на Cisco устройството.

Типове тест:
DHCP, DNS, ICMP Echo, FTP, HTTP, Jitter, UDP Echo, Видео операции

Латентност:
MOS измервания на производителността, загуба, нестабилност

Широкомащабни:
Предоставяне на IP SLA, базирани на съветника, с пълна конфигурация на мрежата и хъба/разклоненията

Интеграция и компоненти на архитектурата



LiveNX

LiveNX е платформа за мониторинг на работата на мрежата и приложенията с патентована визуализация от край до край за глобален изглед на мрежата и възможност за разширяване до отделни устройства. Използвайки LiveNX, предприятията получават в реално време непрекъснат поглед върху мрежовия трафик на базата на активност на приложения и потребителско ниво. LiveNX предлага възможността да се събират и анализират обеми от мрежови данни в мащаб от всяко устройство, приложение и потребител, за да се намали средното време за ремонт и извършва проучвателен и обяснителен анализ.

Omnipeek

- Дълбок анализ на пакетите
- Голяма библиотека от декодери
- Експертна система - предложени каузи

LiveUX

LiveUX наблюдава опита на крайния потребител с уеб приложенията. Чрез комбиниране на показателите за преживяване на крайния потребител с информацията за мониторинг на мрежовата ефективност можете бързо да сортирате проблемите с производителността.

- **Интегрирано табло за управление LiveNX и LiveUX за незабавна видимост на състоянието на сайта, мрежовите** устройства, използването на приложенията и ефективността на приложението (вкл. Унифицираните комуникации).
- Бързо идентифициране на сайтовете, които имат влошаване на производителността и засегнати приложения
- **От сайта разгледайте подробно условията на мрежата, включително използването на честотната лента, грешки във връзката, QoS показатели и приложения, които се конкурират за честотната лента**

LiveNX Монитор на мониторите

LiveNX Monitor of Monitor предоставя един екран за настройки на сървъра, състояние на системата, сайтове и конфигурация, обобщавайки множество географски или организационно сегментирани LiveNX домейни. Чрез слой за обобщаване всеки LiveNX домейн сървър вкарва подходящи данни за обобщени изгледи и управление на таблото чрез северен REST API.

А1 България ЕАД

Системни изисквания

Опции за внедряване

Компонент	Виртуален уред (OVA)	Виртуален уред (Hyper-V)	Уеб услуги на Amazon (AMI)	Microsoft Azure	LiveNX Server Appliance
LiveUX Мониторинг на приложения	X	X	X	X	X
LiveNX Сървър	X	X	X	X	X
LiveNX възел	X	X	X	X	X

Внедряване на LiveNX

Опции за внедряване

Компонентите на LiveNX могат да бъдат внедрени чрез следните методи: Виртуален, физичен и облачен. Спецификациите за виртуално внедряване, както и списъците за поддръжка на устройства Cisco и Multi-Vendor Device са посочени по-долу.

Ако се интересувате от внедряване на LiveNX във физическа, облачна (Azure, AWS и Google Cloud), Hyper-V или KVM среда, моля, свържете се с LiveAction продажби (sales@liveaction.com) за спецификациите, подходящи за тези среди и вашите нужди.

Спецификации за виртуално внедряване

Сървърът LiveNX се използва предимно като VMware OVA уред и е напълно оперативен веднага. Сървърната операционна система работи на Linux (TinyCore или Ubuntu) платформа.

Спецификации на сървърната платформа

• VMware ESXi v5.0 или по-нова версия - VMware хардуер версия 8 (vmx-8)

• Мрежов хардуер - Най-малко два физически NICS на ESXi

• Поддръжка до 10 Gbps

• Виртуалните NIC на OVA използват E1000

Доказателство за концепция (POC)	Малко внедряване	Средно внедряване	Голямо внедряване	Физическо внедряване
<= 25 устройства или <= 25 k потока/sec.	<= 100 устройства или <= 50 k потока/sec.	100 до 500 устройства или <= 100 k потока/sec.	500 до 1000 устройства или <= 150 k потока/sec.	1000 или повече устройства или <= 350 k потока/sec.
Мнимални изисквания - 8vCPU Xeon или i7 -16 GB RAM -LiveNX Сървър макс. хип размер 8 GB -500 GB диск за данни	Мнимални изисквания -16 vCPU Xeon или i7 -32 GB RAM -LiveNX Сървър макс. хип размер 16 GB -2 TB Дискове за данни	Мнимални изисквания -16 vCPU Xeon или i7 -64 GB RAM -LiveNX Сървър макс. хип размер 31 GB -4 TB Дискове за данни	Мнимални изисквания -32 vCPU Xeon или i7 -64 GB RAM -LiveNX Сървър макс. хип размер 31 GB -8 TB Дискове за данни	Мнимални изисквания -48 vCPU Intel Xeon Gold - 5118, активиран Hyperthreading -96 GB RAM -LiveNX Сървър макс. хип размер 64 GB -32 TB Дискове за данни

Всеки LiveNX сървър / възел поддържа до 76 TB дисково пространство. Препоръчва се да добавите всеки диск на стъпки от 10 TB.
Препоръка за сървър IOPS LiveNX 8.0 - 1000 IOPS четене и 4500 IOPS запис.

Спецификации на клиентската платформа

- Windows или macOS
- 4 ядра
- 8GB RAM
- Уеб браузър: IE11 и по-нови версии, Firefox, Chrome и Safari

Поддържани мрежови устройства

LiveNX Flow

LiveNX Flow осигурява усъвършенствани визуализации на потока от край до край за мрежи с много доставчици. Следните устройства са преминали през тестване с анализ на потока с LiveNX.

Рутери от серията Adtran NetVanta	F5 BIG-IP Платформи за контрол на доставки на приложения
Рутери Alcatel-Lucent	Gigamon GigaSMART
Рутери от серията Brocade	Превключватели от серията Hewlett-Packard Enterprise Procurve
Рутери от серията Cisco (Рутери от серията ISR, CRS-1, рутери ASR 1000 и ASR 9000, ENCS5000)	Мрежово решение за видимост на Ixia
Превключватели Cisco Catalyst	Рутери от серията Juniper MX
Превключватели Cisco Nexus (Nexus серия 3000, 7000 & 9000)	nTop nProbe
Защитни стени на Cisco серия ASA 5500	Защитни стени на Palo Alto Networks
Модул за видимост на мрежата Cisco AnyConnect на Windows и macOS X платформи	Оптимизирани WAN контролери Riverbed SteelHead
Cisco DNA Center, Cisco APIC-EM Cisco Meraki MX	Оптимизирани WAN контролери Silver Peak
Cisco NetFlow Generation Appliance	Cisco vEdge/cEdge Рутери Cisco Viptela VManage API
Екстремни мрежови превключватели	Краен агент

LiveNX IP SLA

- Серия Cisco рутери поддържат се 800, 1000, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V

LiveNX LAN

Превключватели серия Cisco Catalyst поддържат се 2960, 2960-X, 3560, 3650, 3750, 3850, 4500, 6500, 9000.

LiveNX маршрутизиране

Серия Cisco рутери: поддържат се 800, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V, ENCS .

LiveNX QoS Монитор

LiveNX QoS Монитор осигурява мониторинг на качеството на услугата и отстраняване на неизправности за Cisco рутери и превключватели.

- Серия Cisco рутери: 800, 1000, 1700, 1800, 1900, 2600,2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V
- Cisco ASR 1000 и 9000

  Препоръчват се IOS версии 12.3 или по-нова или 15.0 или по-нова за използване със софтуера (IOS XE 2.6.0 или по-нова версия за серия.ASR 1000). По-ранните версии на IOS също могат да работят, но официално не се поддържат. Версиите с IOS с общо издание се препоръчват, въпреки че версиите с ранно и ограничено издаване също ще работят с LiveNX.
- Превключватели серия Cisco Catalyst 3650, 3850, 4500-X и 9000 с ограничена поддръжка на LiveNX QoS монитор в 3-рутируеми интерфейси и VLAN в зависимост от възможностите на Cisco хардуера.
- Компютърна система за корпоративна мрежа корпорация серия Cisco 5000
- Превключватели серия Cisco Nexus: 7000

LiveNX QoS Конфигурация

LiveNX QoS Конфигурация осигурява конфигуриране и отстраняване на неизправности в качеството на услугата за рутери и превключватели на Cisco.

- Серия Cisco рутери: 800, 1000, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V

  Препоръчват се IOS версии 12.3 или по-нова или 15.0 или по-нова за използване със софтуера (IOS XE 2.6.0 или по-нова версия за серия ASR 1000). По-ранните версии на IOS също могат да работят, но официално не се поддържат. Версиите с IOS с общо издание се препоръчват, въпреки че версиите с ранно и ограничено издаване също ще работят с LiveNX.
- Превключватели серия Cisco Catalyst 9000
- Превключватели серия Cisco Catalyst 3850 &4500-X Limited LiveNX QoS Monitor се поддържа на Слой 3-маршрутизиращи интерфейси и VLAN в зависимост от възможностите на Cisco хардуера.
- Превключватели серия Cisco Nexus: Серията 7000 се поддържа частично

LiveAction
3500 West Bayshore Rd.
Palo Alto, CA 94303

Телефон + eFAX: +1 888-881-1116
Имейл: *sales@liveaction.com*
Уебсайт: *www.liveaction.com*

#040920

Подписаният Огнян Петко [redacted] удостоверявам верността на извършения от мен превод от английски на български език на приложения документ – “Платформа за монитори [redacted] ефективността на приложенията". Преводът се състои от 8 страници.

Преводач: Огнян Петков [redacted]

[redacted]

A1 [redacted] ЕАД

Data Sheet

LiveNX

LiveAction

Network and Application Performance Monitoring Platform

LiveNX collects and analyzes data directly from network devices to analyze and present insights to design, policy verification, and operations across the enterprise to deliver peak performance for an optimal customer experience.

Overview

End-to-end Flow Visualizations Across the Network

LiveNX's patented visualization technology simplifies network operations and troubleshooting. LiveNX correlates multiple data sets to provide views, graphs and maps to illustrate the current state of applications and network performance.

Application Visibility and Troubleshooting

Gain a deep understanding of application traffic with full visibility of protocol and application type including video, voice, instant messaging, file transfer, etc. Troubleshoot applications deployed in the data center, public cloud or SaaS. Understand how your network is being used, how applications are performing, and which sanctioned or unsanctioned applications are being used.

Intuitive Graphical Interface for QoS Control

Create, edit and apply QoS polices for Cisco routers and Layer 3 switches on live networks consistently and confidently. QoS wizard and built-in templates are available to apply policies based on Cisco best practices or use the QoS GUI editor to build custom policies. LiveNX generates a QoS audit report to show QoS policies in detail, including configuration settings, performance issues, drops, and policy errors

Software-Defined WAN Management

Utilize application and path visualizations to effectively validate WAN Return-on-Investment (ROI) for traditional MPLS, hybrid, or Software- Defined WAN (SD-WAN). When a network element makes a path change to protect the applications due to an Out-of-Policy (OOP) condition, LiveNX renders the end-to-end path changes graphically. Visualize the network and overlay paths from the branch-office, through the service provider(s) to the data center where the applications reside, for meaningful and actionable information.

LiveNX gathers real-time data from both multi-vendor network elements as well as Cisco-specific REST APIs (DNA Center, vManage BFD (Bidirectional Forward Detection) and AppId (Application Identification to provide accurate visual analytics)).

What's New

Reporting/Dashboards

- WebUI enhanced report drilldowns
- Availability dashboards widgets
- Enhanced report scheduling and sharing options
- Added recent report history management
- Business hours support for multi-interface SNMP reports
- Introduced "Situational Awareness" overview dashboard
- Application and voice/video performance reporting and dashboarding enhancements
- Enhanced IPv6 support
- DMVPN Per-Tunnel QoS monitoring
- Catalyst 9k: QoS monitoring via packet rate (CBQoS MIB)
- Added the following reports:
  - Multicast Audit Report
  - Interface Bandwidth and Utilization Summary Reports (SNMP)
  - Daily Interface Bandwidth Summary
  - Interface utilization above threshold overtime
  - Additional report templates

Topology

- Enhanced web Geo Topology for large-scale operations

LiveWire

- SNMP support
- Additional cross-launch to Omnipeek options

WebUI Stories

- WAN Capacity Planning Story
- WAN Interface Utilization Story
- Search by DN (call) Story

ВЯРНО С ОРИГИНАЛА

Device/System Management

- WebUI Geo-location grouping
- Custom application management (w/NBAR)
- Enhanced dashboard filtering
- Improved system backup and restore for non-snmp managed devices
- Updated Cisco WLC Netflow template support (Higher Visibility)
- Geo-Topology: current alerts status box
- Configurable device auto-refresh time
- Improved Cisco SD-WAN onboarding
- Single Sign-On (SSO) vis SAML (ADFS)

Alerting

- Web: Drilldown from Alert to relevant report
- QoS Class Drop catch-all threshold
- Multi-threshold alerting for:
  - Interface, Device, Site Reachability Alerts
  - Device CPU/Memory Alerts
  - WAN Utilization Alert
- Service Now: Incidents (urgency/sub-category fields)
- SD-WAN Enhancements: vManage alert and event visibility
- Maintenance Mode

LiveAction Network Analytics (LiveNA) (Preview)

- On-premise GPU based appliance(s)
- Anomaly detection of app behavior
- Advanced baselining and analytics

Cloud Monitoring for AWS/Azure (Preview)

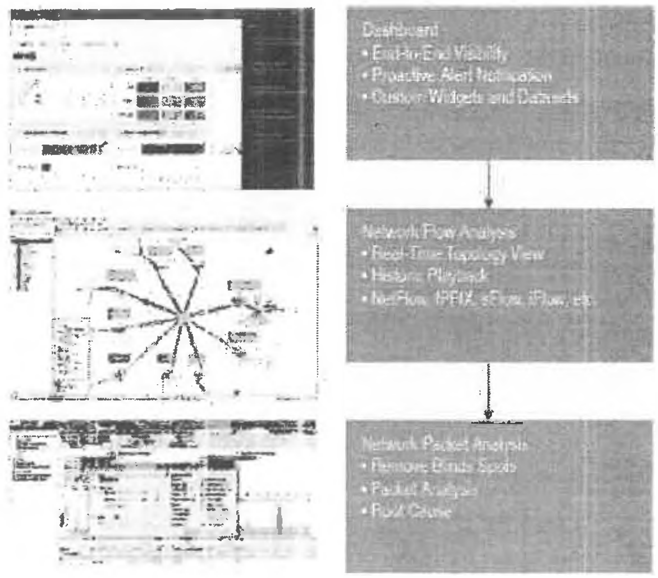
- End to End Visibility – both cloud and on-premise
- Visibility across VPC and VNet traffic
- Native flow log visibility

Please contact *support@liveaction.com* if you are interested in seeing a demo of the Preview products—LiveNA and Cloud Monitoring.

Key Features

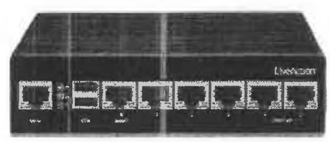
Rapid Incident Response with Flow to Packet Analysis Workflow Optimization

Resolving complex incidents can be challenging when different systems, vendors, devices and software are involved. LiveNX optimizes a rapid incident response workflow with Alert notification or predictive insight where the event is identified for remediation. Within LiveNX's Engineering Console, NetOps can easily isolate the issue with the visual analytics presented as topology, site or device views. LiveNX presents the time stamp from the Alert and problem isolation from the Flow data, should additional analysis be necessary the NetOps team can quickly cross launch Omnipeek for deep packet analysis for root cause.



Rapid Incident Response for Faster Incident Resolution

LiveWire Integration for Monitoring WAN Edge Segments



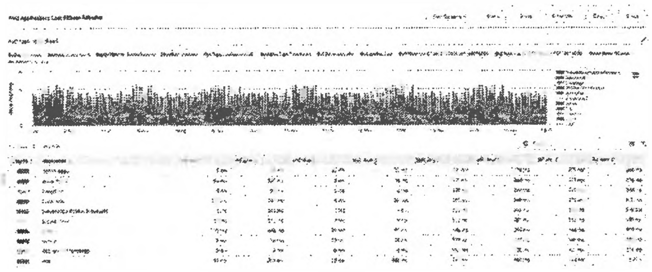
LiveWire — WAN Edge Continual Monitoring

The LiveWire Network Monitoring Appliance is optimized for WAN edge applications to provide packet capture and integrated IPFIX Export solution with LiveNX. LiveWire captures and converts real-time packet data which feeds directly into the visualization engine of LiveNX.

Together, LiveWire and LiveNX bring new visual insights and analytics to traditionally "dark" environments such as application classification and performance management for SD-WAN deployments or traditioal legacy multi-vendor edge switch environments. LiveWire is extremely powerful for numerous use cases including branch wireless monitoring, point-of-sale transaction troubleshooting and VoIP troubleshooting.

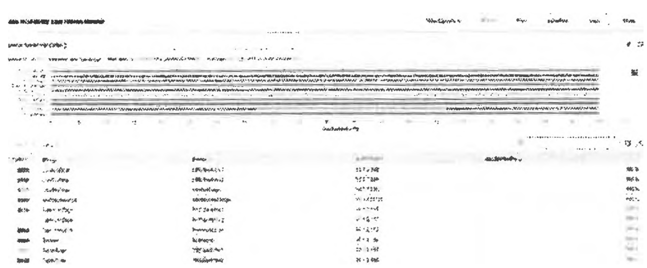
ВЯРНО С ОРИГИНАЛА

Application Visibility and Control (AVC) Reports



LiveNX presents advanced network performance data with Cisco Application Control and Visibility (AVC) data. With this network data, LiveNX reports on Top Applications Performance and AVC Applications with latency, jitter, packet loss and advanced performance indicators for: sites, devices, users and service provider environments.

Alerting Enhancements – Site Availability



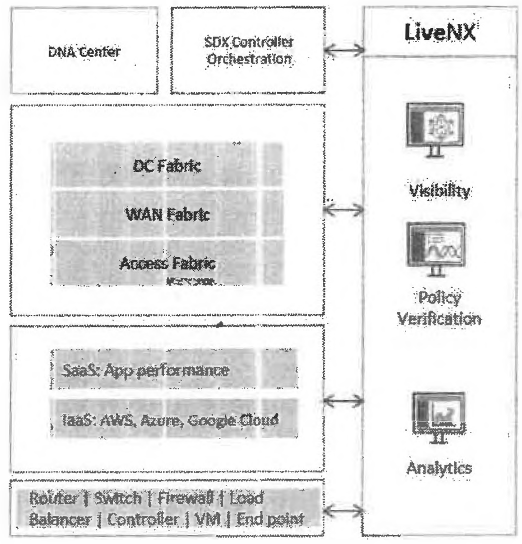
LiveNX Operations Dashboard — Current Alerts by Site

LiveNX — Site Availability Report

The LiveNX Operations Dashboard now supports site availability reports and custom widgets to illustrate an aggregated alerting view. NetOps teams can now visualize the Dashboard Alerts in one location by Site, Device, or Interface for easier access with summarized views.

Site availability is a helpful trend to observe. This is one where fluctuations should be very small, and KPIs controlled tightly. As a leading indicator of possible SLA violations, hazardous areas or poor deployment scenarios, Site Availability Reports are best integrated in a Service Level View and tie it together with Application performance and Network QoS Class reporting.

Cisco Integrations



LiveNX Cisco DNA Center Integration

LiveNX offers the broadest suite of integration for Cisco environments. In LiveNX 8, Cisco DNA Center API integration is now available for General Availability, in addition to Cisco Identity Service Engine (ISE), vManage (SD-WAN), SD-Access and PxGrid connectors. These integrations provide rich datasets for LiveNX advanced visual analytics. Real-time Topology Flow Views and forensic playback and analysis are key NetOps elements.

Key Capabilities

Flow and Packet Optimized Workflow for Network Troubleshooting

With both flow and packet level analysis NetOps can now isolate problem areas quickly and have a rapid response ready for any high severity incidents.

With Flow Topology Views and integrated Expert Packet Analysis, LiveNX optimizes the problem isolation to root cause incident management cycle. With integrated ServiceNow ITOM workflows, LiveNX is a key platform for NetOps to resolve incidents faster, and report on status and impact to the business.

Visual Analytics

Visualization allows you to better understand network traffic so that you can identify trouble spots.

- Application and flow path analysis
- Multi-vendor support – NetFlow v5/v9, IPFIX, sFlow and J-Flow
- Jitter, delay, packet loss metrics for voice and video
- Application response times, round-trip time, server delay and client delay metrics
- NetFlow Secure Event Logging (NSEL)

ВЯРНО С ОРИГИНАЛА

- Wireless information including user identity
- Firewall high-speed logging
- End-system (device type, OS) and end-user information
- Integration with Network Packet Brokers
- Flow DVR for playback of historical data
- Built-in Domain Name System (DNS) name resolution
- Topology export to Visio

Software-Defined WAN Monitoring

GUI-based management for SD-WAN monitoring for path control and application performance optimization.

- Path control visualization
- SD-WAN dashboard and trending
- PfRv3 multiple data center support
- Shows what Out-of-Policy reason triggers path change(s)
- Reports on traffic class/application associated

Cisco SD-WAN Support (Viptela)

LiveNX consolidates a unified reporting, inventory, and alert notification. For Cisco SD-WAN, LiveNX supports:

- Cisco vEdge, cEdge and ENCS platform support
- Cisco IWAN support
- Cisco SD-WAN Site to Site Topology View
  - Overlay visibility – VPN, tunnel
  - Service Provider transport
  - Performance Status
  - Filtering by application, DSCP, VPN or Service Provider
- Cisco SD-WAN Site to Site Analysis
  - Policy verification
  - Application – VPN – DSCP – Service Provider service status
- Viptela device inventory, including vEdge routers and management devices like vManage, vBond and vSmart
- Add relevant interfaces for monitoring from each vEdge router.
- Device monitoring credentials, like SNMP settings
- Gather network semantic information per device and interface:
  - Site association per device
  - Site geo location
  - WAN interfaces per device
  - Service Provider associated with each WAN interface. Note: Viptela refers to the service provider information as 'colors.' Capacity of WAN links (inbound and [redacted]
  - Site IP mappings
  - Determine if a device is in the data center
  - Viptela VPN ID mapping to a VPN name
  - vManage API: BFD (Bidirectional Forward Detection), AppId and Alarms.

Cisco IWAN Support

- PfR configuration of multiple Master Controllers
- Automatically learn semantic settings for PfRv3 monitoring to simplify setup
- PfRv3 multiple data center support

QoS Monitoring

Track QoS performance on a per-class basis. Monitoring and alerting of priority queue drops provides proactive notification of potential voice quality issues.

- NBAR2 application visualization
- Custom NBAR definitions
- Pre- and post-QoS graphs
- Detailed graphical display of interface and CBQoS statistics
- 95th/99th percentile, quarterly, yearly and collated reports

Alerting

LiveNX associates Events from devices (routers, switches, firewalls, etc.) to Alerts, which are generated upon meeting specific criteria, such as a threshold, and are displayed in the Operations Dashboard.

With the Event-to-Alert mapping concept, LiveNX is able to eliminate the common complaint that the number of alerts being created is too high, thereby displaying only the alerts that require immediate attention.

Alerts are categorized into three severity levels:

Critical:

The highest severity, e.g. for alerts that would cause the biggest problem to the network

Warning:

A high severity, e.g. for alerts that may indicate issues that are problematic or will become problematic

Info:

A low severity, e.g. an issue that is worth knowing about but may not be that detrimental to the network

Alerts can be configured to integrate into workflows within industry incident management systems such as ServiceNow and PagerDuty.

QoS Configuration

Create, edit, and apply QoS policies for Cisco routers and Layer 3 switches on live networks. Use the QoS wizard and built-in templates to apply policies across multiple devices based on Cisco best practices or use the QoS GUI editor to build policies.

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

[redacted]

- Full Modular QoS configuration support including WRED, CBWFQ, and Priority Queue
- Hierarchical policy creation for advanced configurations
- Custom NBAR2-based matches including high-level attributes, HTTP URL, MIME, HOST and RTP protocols
- Built-in ACL editor
- Built-in rules for QoS settings that highlight violations
- Configuration audit trail
- System-wide QoS audit
- LAN Service Policy

LAN

Visualize Spanning Tree Protocol. Provide real-time Layer 2 visualizations for networks, including trunk interface, port channels, VLAN associations and bandwidth percentages. Run Layer 2 QoS reports.

Routing

Real-time routing visualizations for Cisco networks that can identify reachability problems, routing loops, and asymmetric paths affecting traffic quality. In addition, the policy-based routing viewer/editor provides a high degree of control over traffic policy to route traffic easily and predictably over user-specified paths.

IP SLA

Cisco IOS IP SLA is easily accessible to generate and monitor synthetic network traffic to baseline network performance, test policy changes, or proactively monitor key network paths. Synthetic traffic types include data (HTTP, FTP, DNS, DHCP) and voice that can be used to measure latency, loss, jitter, and Mean Opinion Score (MOS) for VoIP. The highly interactive graphical interface delivers the functionality and flexibility of IP SLA features without the need to learn and use Cisco device command lines.

Test Types:

DHCP, DNS, ICMP Echo, FTP, HTTP, Jitter, UDP Echo, Video Operations

Latency:

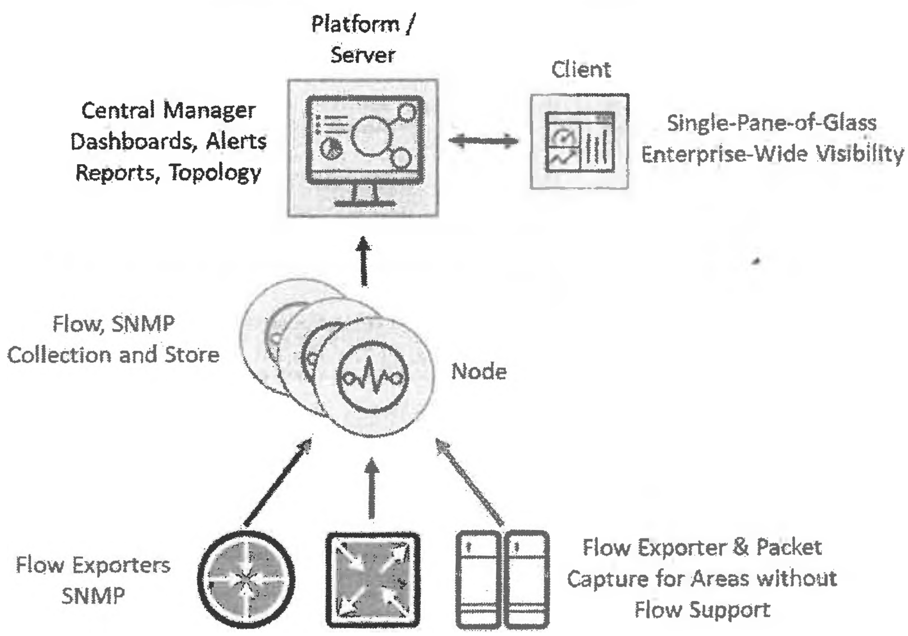
MOS performance measurements, loss, jitter

Large-Scale:

Wizard-based IP SLA provisioning in full-mesh and hub/spoke configuration

ВЯРНО С ОРИГИНАЛА

Integrations and Component Architecture



LiveNX

LiveNX is a network and application performance monitoring platform with patented end-to-end visualization for a global view of the network and the ability to drill-down to individual devices. Using LiveNX, enterprises gain real- time and continuous insight into network traffic based on application and user level activity. LiveNX offers the ability to gather and analyze volumes of network data at scale from every device, application and user to reduce mean time to repair, and it performs exploratory and explanatory analysis.

Omnipeek

- Deep packet analysis
- Vast library of decoders
- Expert system – suggested causes

LiveUX

LiveUX monitors end-user experience of web applications. By combining the end-user experience metrics with the network performance monitoring information, you can quickly triage performance issues.

- Integrated LiveNX and LiveUX dashboard for instant visibility of site health, network devices, application usage, and application performance (incl. Unified Communications).
- Quickly identify the sites that are experiencing [redacted] nd the applications impacted
- From the site, drill down to examine network conditions including bandwidth utilization, link errors, QoS metrics and applications that are competing for the bandwidth

LiveNX Monitor of Monitors

LiveNX Monitor of Monitors provides a single-pane-of-glass for server settings, system health, sites and configuration, aggregating multiple geographical or organizationally segmented LiveNX domains. Through an aggregation layer, each LiveNX server domain instance injects relevant data for summary dashboard views and management by way of a north-bound REST API.

LiveNX

LiveAction

System Requirements

Deployment Options

Component	Virtual Appliance (OVA)	Virtual Appliance (Hyper-V)	Amazon Web Services (AMI)	Microsoft Azure	LiveNX Server Appliance
LiveUX Application Monitoring	X	X	X	X	X
LiveNX Server	X	X	X	X	X
LiveNX Node	X	X	X	X	X

LiveNX Deployment

Deployment Options

LiveNX components can be deployed via the following methods: Virtual, Physical, and Cloud. The Virtual Deployment Specifications, as well as the Cisco and Multi-Vendor Device Support lists are provided below.

If you are interested in deploying LiveNX in a Physical, Cloud (Azure, AWS, & Google Cloud), Hyper-V, or KVM environment, please contact LiveAction sales (sales@liveaction.com) for the specifications appropriate for those environments and your needs.

Virtual Deployment Specifications

The LiveNX Server is primarily deployed as a VMware .OVA appliance and is fully operational right out of the box. The server operating system runs on a Linux (TinyCore or Ubuntu) platform.

Server Platform Specifications

- VMware ESXi v5.0 or higher - VMware Hardware Version 8 (vmx-8)
- Network Hardware - At least two Physical NICS on ESXi
  - Support up to 10 Gbps
  - Virtual NICs on OVA are utilizing E1000

Proof of Concept (POC)	Small Deployment	Medium Deployment	Large Deployment	Physical Deployment
<= 25 devices or <= 25 k flows/sec.	<= 100 devices or <= 50 k flows/sec.	100 to 500 devices or <= 100 k flows/sec.	500 to 1000 devices or <= 150 k flows/sec.	1000 or more devices, or <= 350 k flows/sec.
Min. Requirements: 8 vCPU Xeon or i7 16 GB RAM LiveNX Server Max Heap Size 8 GB 500 GB Data Disk	Min. Requirements: 16 vCPU Xeon or i7 32 GB RAM LiveNX Server Max Heap Size 16 GB 2 TB Data Disks	Min. Requirements: 16 vCPU Xeon or i7 64 GB RAM LiveNX Server Max Heap Size 31 GB 4 TB Data Disks	Min. Requirements: 32 vCPU Xeon or i7 64 GB RAM LiveNX Server Max Heap Size 31 GB 8 TB Data Disks	Min. Requirements: 48 vCPU Intel Xeon Gold 5118, Hyperthreading enabled 96 GB RAM LiveNX Server Max Heap Size 64 GB 32 TB Data Disks

Each LiveNX server/node supports up to 76 TB disk space. It is recommended to add each disk in 10 TB increments.
Server IOPS Recommendation LiveNX 8.0 - 1000 IOPS Read and 4500 IOPS Write.

ВЯРНО С ОРИГИНАЛА

А1

КП 2

Client Platform Specifications

- Windows or macOS
- 4 Cores
- 8 GB RAM
- Web browser: IE11 and higher, Firefox, Chrome, and Safari

Network Device Support

LiveNX Flow

LiveNX Flow provides advanced end-to-end system-level flow visualizations for multi-vendor networks. The following devices have gone through flow-analysis testing with LiveNX.

Adtran NetVanta Series Routers	F5 BIG-IP Application Delivery Controller Platforms
Alcatel-Lucent Routers	Gigamon GigaSMART
Brocade Series Routers	Hewlett-Packard Enterprise Procurve Series Switches
Cisco Series Routers (ISR Series, CRS-1, ASR 1000 & ASR 9000 Series Routers, ENCS5000)	Ixia's Network Visibility Solution
Cisco Catalyst Switches	Juniper MX Series Routers
Cisco Nexus Switches (Nexus 3000, 7000 & 9000 Series)	nTop nProbe
Cisco ASA 5500 Series Firewalls	Palo Alto Networks Firewalls
Cisco AnyConnect Network Visibility Module on Windows and macOS X Platforms	Riverbed SteelHead WAN Optimization Controllers
Cisco DNA Center, Cisco APIC-EM Cisco Meraki MX	Silver Peak WAN Optimization Controllers
Cisco NetFlow Generation Appliance	Cisco vEdge/cEdge Routers Cisco Viptela VManage API
Extreme Network Switches	Endpoint Agent

LiveNX IP SLA

- Cisco Series Routers: 800, 1000, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V are supported

LiveNX LAN

Cisco Catalyst Series Switches: 2960, 2960-X, 3560, 3650, 3750, 3850, 4500, 6500, 9000 are supported.

LiveNX Routing

Cisco Series Routers: 800, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V, ENCS are supported.

LiveNX QoS Monitor

LiveNX QoS Monitor provides quality of service monitoring and troubleshooting for Cisco router and switches.

- Cisco Series Routers: 800, 1000, 1700, 1800, 1900, 2600,2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V
- Cisco ASR 1000 and9000

  Recommend IOS versions 12.3 or higher or 15.0 or higher for use with the software (IOS XE 2.6.0 or higher for ASR 1000 series). Earlier IOS versions may also work but are not officially supported. General-release IOS versions are recommended, although early- and limited- release versions will also work with LiveNX.
- Cisco Catalyst Series Switches: 3650, 3850, 4500-X and 9000 Limited LiveNX QoS Monitor support on Layer 3-routable interfaces and VLANs depending upon Cisco hardware capabilities.
- Cisco 5000 Series Enterprise Network Compute System
- Cisco Nexus Series Switches: 7000

LiveNX QoS Configure

LiveNX QoS Configure provides for configuring and troubleshooting Quality of Service for Cisco routers and switches.

- Cisco Series Routers: 800, 1000, 1700, 1800, 1900, 2600, 2600XM, 2800, 2900, 3600, 3700, 3800, 3900, 4300, 4400, 7200, 7600, ASR1000, CSR 1000V

  Recommend IOS versions 12.3 or higher or 15.0 or higher for use with the software (IOS XE 2.6.0 or higher for ASR 1000 series). Earlier IOS versions may also work but are not officially supported. General-release IOS versions are recommended, although early- and limited-release versions will also work with LiveNX.
- Cisco Catalyst Series Switches: 9000
- Cisco Catalyst Series Switches: 3850 &4500-X

  Limited LiveNX QoS Monitor support on Layer 3-routable interfaces and VLANs depending upon Cisco hardware capabilities.
- Cisco Nexus Series Switches: 7000 Series are partially supported

ВЯРНО С ОРИГИНАЛА

A1

Превод от английски език

CISCO
The bridge to possible
СИСКО
Мостът към възможното

Информационен лист
Публичен за CISCO

Cisco SD-WAN

Съдържание

[redacted]

[redacted] [redacted] [redacted]

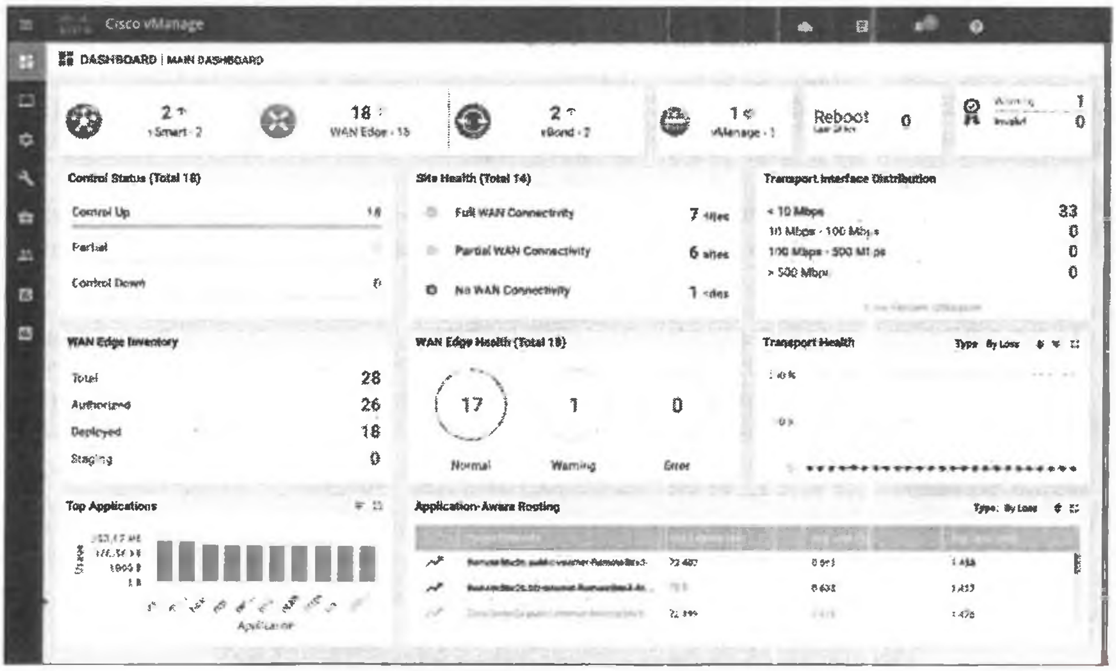
София 1504, ул. "Св. Климент Охридски" №4
тел.: 02/ 946 13 92; тел./факс: 02/ 943 86 65
e-mail: office@fides.bg
www.fides.bg

[redacted] [redacted] [redacted]

Решението на Cisco® SD-WAN (Software Defined Wide Area Network – Софтуерно дефинирана глобална мрежа) предлага цялостна платформа за SD-WAN с вградено централизирано управление и сигурност, създавайки защитена overlay WAN архитектура в кампуса, клона и центъра за данни и мултиоблачни приложения. Софтуерното решение работи на редица SD-WAN рутери в хардуерни, виртуални и облачни фактори на формата.

Преглед на решението

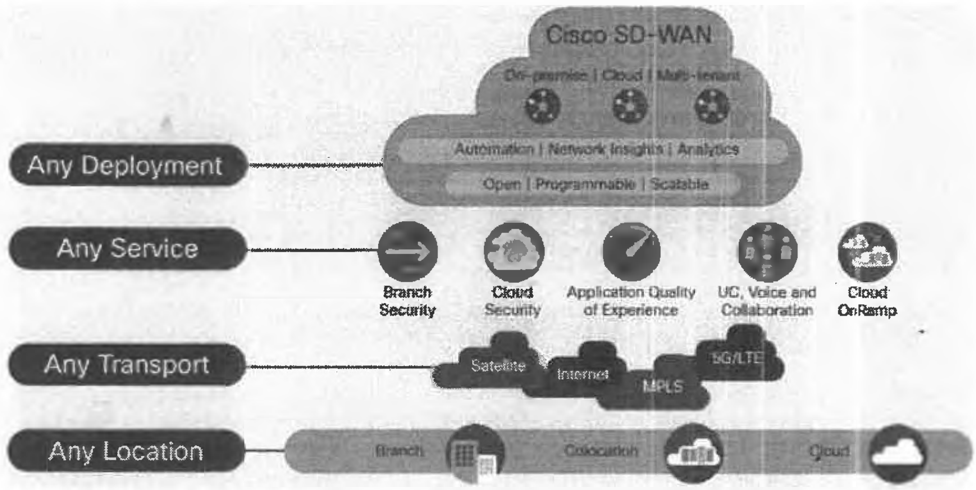
Таблото за управление на Cisco SD-WAN (Фигура 1) свързва всички центрове за данни на компанията, местата на ядрото и кампуса, клонове на WAN, съоръжения за колокация, облачна инфраструктура и отдалечени работници. Cisco SD-WAN използва протокола Overlay Management Protocol (OMP), за да контролира цялата мрежа. Той опростява ИТ операциите с автоматизирано предоставяне, унифицирани политики и опростено управление, за да подпомогне предоставянето на бързи актуализации и решения, и осигурява разширена функционалност, надеждност и сигурност на мрежата.



Фигура 1.

Таблото за управление на Cisco SD-WAN

Dashboard | Main dashboard	Табло за управление | Главно табло				
Control Status (Total 18)	Статус на контрола (общо 18)	Site Health (Total 14)	Здраве на сайта (общо 14)	Reboot	Рестартиране
WAN Edge Inventory	Списък на WAN Edge	WAN Edge Health	Здраве на WAN Edge (общо 18)	Transport Interface Distribution	Разпределение на транспортния интерфейс
Top Applications	Топ приложения	Application-Aware Routing	Насочена към приложението маршрутизация	Transport Health Type: By Loss	Транспортно здраве Тип: По загуби



Фигура 2.

Сигурната архитектура в облачен мащаб на Cisco SD-WAN

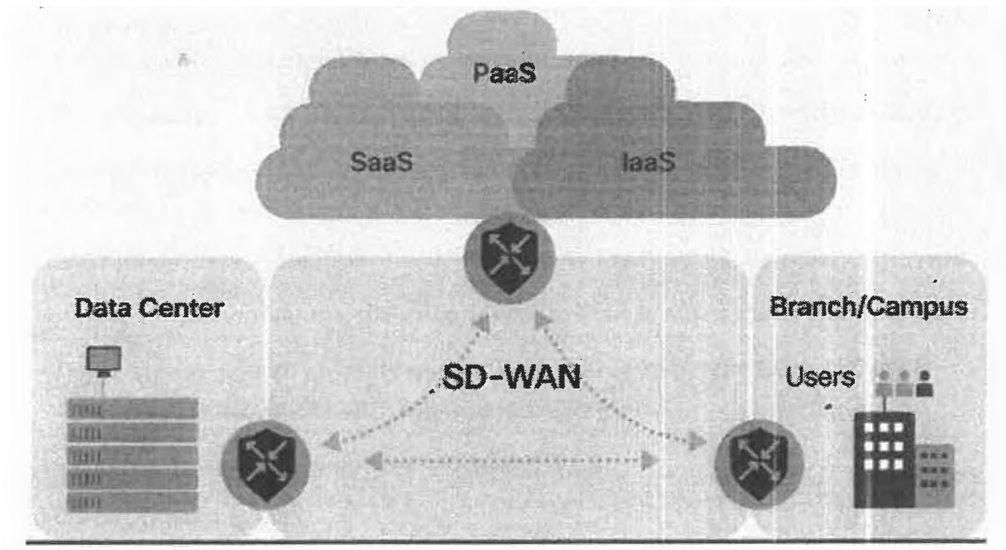
Any Deployment	Всяко разгръщане	On-premise | Cloud | Multi-tenant	Локална мрежа | Облак | За много наематели
Any Service	Всяка услуга	Automation | Network | Analytics	Автоматизация | Мрежа| Аналитичност
Any Transport	Всеки транспорт	Branch Security |Cloud Security | Application Quality of Experience | UC, Voice and Collaboration | Cloud OnRamp	Сигурност на клон |Сигурност на облак| Качество на опита за приложението | UC, гласова връзка и съвместна работа | Облак OnRamp
Any Location	Всяка локация	Branch | Colocation| Cloud	Клон| Колокация| Облак

Cisco SD-WAN осигурява гъвкава архитектура за разширяване на SD-WAN до всяка среда (Фигура 2). Решението автоматично открива, удостоверява и предоставя както нови, така и съществуващи устройства на Cisco SD-WAN.

След свързване със Cisco SD-WAN, всяко мрежово устройство може да намери най-добрия път към приложенията, които се намират в центъра за данни или мултиоблак. Cisco SD-WAN може да използва всеки транспортен метод (сателит, широколентов, MPLS, 5G/LTE) от всяко място (ядро, край, облак) за всяка услуга на мрежата (сигурност, качество на опита [QoE] за приложение, гласова връзка). Чрез OMP Cisco SD-WAN поддържа както общи, така и усъвършенствани протоколи за маршрутизация, които са необходими за управление на мрежи през WAN и облак, като Border Gateway Protocol (BGP), Enhanced Internal Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP) и IPv6. Cisco SD-WAN осигурява тази гъвкавост както при изцяло, така и при частично криптирани мрежи, като позволява максимално персонализиране въз основа на бизнес нуждите.

Характеристики и предимства

Характеристика	Предимство
Пълен SD-WAN набор от функции с унифицирани комуникации	Решението осигурява сложен контрол на мрежата с набор от функции за маршрутизация, унифицирани комуникации, мултиоблак, сигурност и централизиран контрол и управление на политиката.
Избор и контрол в мултиоблак	Позволява обхват на оптимизация за мултиоблачни приложения, използващи Cloud OnRamp архитектура. Той оптимизира основните SaaS (софтуер като услуги) приложения и интеграцията на работния процес към основните публични облаци и колокационни доставчици.
Сигурност, която е вградена, а не прикрепена	Позволява централизирани политики за сигурност и осигурява сегментиране в цялата мрежа и пълен набор защити или на място, или в облака Cisco Umbrella® (Фигура 3). Незабавно разполага правилната защита на правилното място, всичко от едно табло за управление.
Видимост и аналитичност	Централизира управлението, за да улесни разгръщането на SD-WAN и сигурността, като същевременно поддържа политика в хиляди сайтове.
Максимален избор и контрол	Предлага гъвкавост с cloud-first архитектура за свързване на всеки потребител към всяко приложение, през всеки облак.



Фигура 3.
Вградена сигурност на Cisco SD-WAN (локална мрежа on-premise или облак Cisco Umbrella)

Data Center Център за данни

Branch/Campus Клон/Кампус
Users Потребители

Отличителен признак

Най-добрите в класа технологични иновации

- **Напълно интегрирана сигурност навсякъде**
    - Вградена сигурност или облачна сигурност със Cisco Umbrella Secure Internet Gateway (SIG)
    - Разузнаване на маршрутизацията и заплахите на сертифицирана сигурна инфраструктура
    - Интегрирана авто-регистрация и авто-конфигурация на Cisco Umbrella от SD-WAN
    - Talos® сигурност, позволяваща бързо, водещо в индустрията откриване на заплахи
- Истинска SD-WAN архитектура
    - Отделни и специализирани компоненти за равнината на управление, равнината на данни и управлението и оркестрацията на WAN
    - Гъвкавост за прилагане на overlay, underlay, физически и виртуални мрежи
    - Поддръжка на гласови и унифицирани комуникации (UC)
    - Поддръжка на IPv6 (BGP, OSPF)

- Надеждна IP поддръжка за множествено предаване (мултикаст)
  - Позволява контрол на мрежовия трафик, повишава ефективността, като премахва излишъка на трафика и намалява натоварването на сървъра и процесора
  - Ефективно се справя с комуникации от един към много или от много към много
  - Осигурява възможност за множествено предаване в платформи (PIM-SSM, IGMPv2 и IGMPv3)
- Защита на инвестициите
  - Използва традиционните транспортни протоколи за най-добрия опит с приложенията
  - Позволява ви просто да надградите съществуващите рутери Cisco с SD-WAN функционалност, ако вашите клиенти предпочитат
- Гъвкави мултиоблачни опции за разгръщане
  - Cloud OnRamp за IaaS
  - Cloud OnRamp за SaaS (с поддръжка на Cisco IOS® XE)
  - Cloud OnRamp за колокация

Матрица на софтуерните функции

Категория	Описание
Удостоверяване, упълномощаване и отчитане (AAA)	TACACS +, RADIUS, локален, базиран на ролите контрол на достъпа
Маршрутизация	OSPF, външен BGP (eBGP), вътрешен BGP (iBGP), EIGRP, статичен, свързан, OMP
Мостово свързване	802.1Q, естествена VLAN, мостови домейни, интегрирана маршрутизация и мостово свързване (IRB), мостово свързване в хост режим
Сигурност	Вградена сигурност: система за предотвратяване на проникване, уеб сигурност, Enterprise защитна стена, Cisco Advanced Malware Protection (AMP), антивирус от следващо поколение (NGAV), филтриране на URL адреси и проверка на SSL Облачна сигурност (Cisco Umbrella): Уеб сигурност с SSL proxy, прилагане на DNS-слой, филтриране на URL адреси, Cloud Access Security Broker (CASB) и Enterprise защитни стени. Прочетете повече: https://learn-umbrella.cisco.com/i/1153736-cisco-umbrella-secure-internet-gateway-sig-essentials/0? Защита на ниво устройство и мрежа: Нулево доверие, сегментация, бели списъци, защитен от фалшифициране модул, сигурност на транспортния слой на дейтаграми (DTLS)/TLS, IPsec, ESP-256-CBC, заглавка за удостоверяване, HMAC-SHA1, защита от разпределен отказ на услугата (DDoS), защита на контролната равнина, преминаване на Network Address Translation (NAT)
Унифицирани комуникации	SIP, поддръжка на гласова и факсимилна връзка в обществена комутируема телефонна мрежа (PSTN), Survivable Remote Site Telephony (SRST), обаждания на 911, конферентна връзка, Cisco Unified Communications Manager и Webex Calling
Оптимизация на приложения/WAN	Предварителна корекция на грешки (FEC) и дублиране на пакети за User Datagram Protocol (UDP), TCP оптимизация, Cloud OnRamp оптимизация за SaaS приложения

Категория	Описание
Мултиоблак и колокация	Интеграции на обществен облак в AWS, Azure и Google Cloud Cloud OnRamp оптимизация за SaaS приложения Cloud OnRamp за колокация
Препращане и качество на услугата (QoS)	Класификация, приоритизация, опашка с ниско забавяне, ремаркиране, оформяне, планиране, прилагане на политики, огледало, транслация на мрежов адрес (NAT) / адресна транслация на порт (PAT)
Множествено предаване (мултикаст)	Протокол за управление на интернет групата (IGMP) v1/v2/v3, независимо от протокола множествено предаване (PIM), Auto-RP, мащабирана репликация на трафик
Политика	Маршрутни политики, насочена към приложението маршрутизация, политика за контрол, политика за данни, политика за ACL (списък за контрол на достъпа), политика за членство във VPN
Услуги за местоположение	Политики за маршрута, насочено към приложението маршрутизация, политика за контрол, политика за данни, политика за ACL, политика за членство във VPN
Клетъчни	Вграден 4G/LTE модем на някои устройства
Мобилност	Wi-Fi 802.11a/b/g/n/ac, WPA2-Enterprise, WPA2-Personal, MAC филтриране, 8 SSIDs на радио, 802.11i подобряване на сигурността и 802.11e QoS, откриване и защита от безжично проникване
Системни и мрежови услуги	IPv4, прост протокол за управление на мрежата (SNMP), протокол за мрежово време (NTP), DNS клиент, протокол за динамично конфигуриране на хост (DHCP) клиент, DHCP сървър, DHCP реле, архивиране на конфигурация, syslog, Secure Shell (SSH), защитно копиране (SCP)), NAT/PAT, Cflowd v10 IPFIX експорт
Конфигурация и мониторинг	NETCONF през SSH, интерфейс на командния ред (CLI), REST (vManage), Linux shell
Управление извън лентата	Порт за управление (vEdge 1000, vEdge 2000, vEdge 5000), порт за серийна конзола (vEdge 1000, vEdge 2000, vEdge 5000), USB конзолен порт

Лицензиране

Cisco DNA софтуер за SD-WAN и маршрутизация

Абонаментното лицензиране на софтуера Cisco DNA Software предлага три функционални нива: Cisco DNA Essentials, Cisco DNA Advantage и Cisco DNA Premier. Това са вложени SKU и представляват добри, по-добри и най-добри оферти. Всички те се предлагат като 3-годишен или 5-годишен абонамент и имат опции за нива на честотната лента.

Предимства:

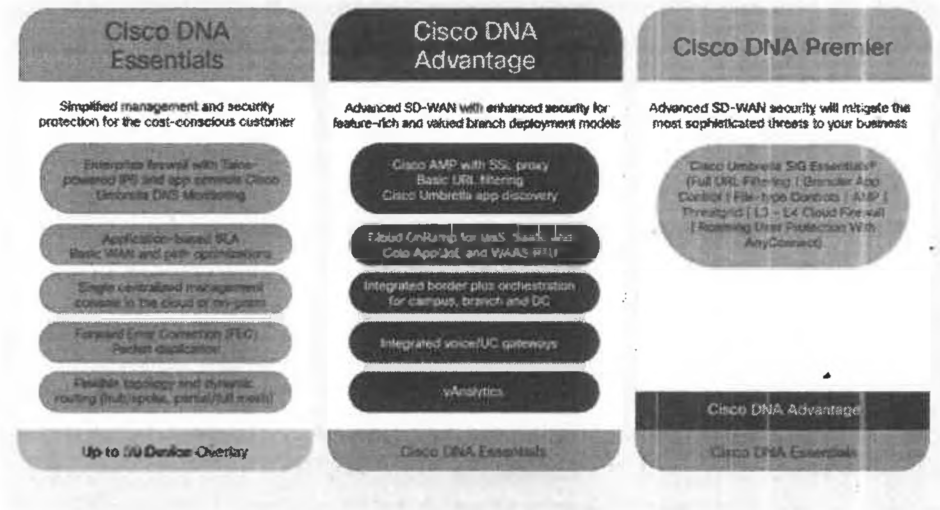
- Най-последните иновации чрез прости абонаментни нива
- Предлага се в целия портфейл
- Гъвкавост за избор на локално (on-premise) или облачно управление
- Лесна преносимост на лицензи в локалната мрежа и облака
- Лесно надграждане през различните нива
- Включена услуга за софтуерна поддръжка (SWSS)

[redacted]

A1 България ЕАД

[redacted]

За повече информация за абонаментите на Cisco DNA отидете на:
https://www.cisco.com/c/m/en_us/products/software/sd-wan-routing-matrix.html?oid=otren019258



Фигура 4.

Абонаментно лицензиране на софтуер Cisco DNA за SD-WAN и маршрутизация

Cisco DNA Essentials	Cisco DNA Essentials	Cisco DNA Advantage	Cisco DNA Advantage	Cisco DNA Premier	Cisco DNA Premier
Simplified management and security protection for the cost-conscious customer	Опростено управление и защита на сигурността за икономически осъзнатия клиент	Advanced SD-WAN with enhanced security for feature-rich and valued branch deployment models	Усъвършенствана SD-WAN с повишена сигурност за много-функционални и ценни модели за разгръщане на клонове	Advanced SD-WAN will mitigate the most sophisticated threats to your business	Advanced SD-WAN ще смекчи най-сложните заплахи за вашия бизнес
Enterprise firewall with Talos-powered IPS and app controls Cisco Umbrella DNS Monitoring Application-based SLA Basic WAN and path optimizations	Корпоративна защитна стена със захранван от Talos IPS и приложение контролира Cisco Umbrella DNS Monitoring Базирано на приложение SLA Базови оптимизации на WAN и пътя	Cisco AMP with SSL proxy Basic URL filtering Cisco Umbrella app discovery Cloud OnRamp for IaaS, SaaS, and Colo AppQoE and WAAS RTU	Cisco AMP със SSL proxy Базово филтриране на URL адреси Cisco Umbrella откриване на приложения Облак OnRamp за IaaS, SaaS, и Colo AppQoE и WAAS RTU	Cisco Umbrella SIG Essentials® (Full URL Filtering | Granular App Control | File-type Controls | AMP | Threatgrid | L3 - L4 Cloud Firewall | Roaming User Protection With AnyConnect)	Cisco Umbrella SIG Essentials® (Филтриране на пълен URL адрес | Гранулиран контрол на приложението | Контрол на типа на файла | AMP | Threatgrid | L3 - L4 облачна защитна стена | Защита на потребителите в роуминг с AnyConnect)
Single centralized management console in the cloud or on-prem Forward Error Correction (FEC) Packet duplication	Единична централизирана конзола за управление в облака или локалната мрежа Предварителна корекция на грешки (FEC) Дублиране на пакети	Integrated border plus orchestration for campus, branch and DC Integrated voice/UC gateways	Интегрирана граница плюс оркестрация за кампус, клон и DC Интегрирани гласови/UC шлюзове		
Flexible topology and dynamic routing (hub/spoke, partial/full mesh)	Гъвкава топология и динамична маршрутизация (хъб/спица, частична/пълна мрежа)	vAnalytics	vAnalytics	Cisco DNA Advantage	Cisco DNA Advantage
Up to 50 Device Overlay	До 50 устройства за наслагване	Cisco DNA Essentials	Cisco DNA Essentials	Cisco DNA Essentials	Cisco DNA Essentials

За повече информация прегледайте софтуера Cisco DNA **за** SD-WAN **и** Routing Ordering Guide (**Ръководство за поръчка Маршрутизация**).

Забележка: Предлагат се и други програми за закупуване, включително Enterprise Agreements (EA) и Managed Service Licensing Agreement (MSLA) (Споразумение за лицензиране на управлявани услуги). Едно споразумение за Cisco Enterprise предоставя по-прост начин за управление на лицензи и намалява разходите, а едно споразумение обхваща закупуването на софтуер и лицензи за абонамент, както и поддръжката на приложен софтуер. MSLA помага на партньорите да изравнят бизнес разходите с модела, базиран на абонамент, за своите клиенти.

Екологична устойчивост на Cisco

Информация за политиките и инициативите за екологична устойчивост на Cisco **за нашите продукти, решения, операции и разширени операции или верига на доставки е предоставена в раздела „Екологична устойчивост" на** Corporate Social Responsibility (CSR) Report (**Доклад за корпоративна социална отговорност**) **на** Cisco. **Референтните връзки към информация по ключови теми за устойчивост на околната среда (споменати в раздела „Устойчивост на околната среда" на доклада за** CSR) **са дадени в следната таблица:**

Тема за устойчивост	Позоваване
Информация относно законите и разпоредбите за съдържанието на материалните продукти	Материали
Информация относно законите и разпоредбите за електронни отпадъци, включително продукти, батерии и опаковки	WEEE съответствие

Cisco **предоставя данните за опаковките на разположение само за информация. Тя** ~~може да не~~ **отразява най-актуалните правни разработки и** Cisco **не представя, осигурява или гарантира, че е пълна, точна или актуална. Тази** [redacted]**ки на промяна без предупреждение.**

Cisco Капитал

Гъвкави решения за плащане, които ще ви помогнат да постигнете целите си
Cisco Capital улеснява получаването на правилната технология за постигане на вашите цели, дава възможност за трансформация на бизнеса и ви помага да останете конкурентноспособни. Можем да ви помогнем да намалите общите разходи за собственост, да запазите капитала и да ускорите растежа. В повече от 100 държави нашите гъвкави разплащателни решения могат да ви помогнат да придобиете хардуер, софтуер, услуги и допълващо оборудване на трети страни с лесни, предвидими плащания. Научете повече.

За повече информация

Вижте как Cisco SD-WAN може да ви помогне да се движите по-бързо, да намалите разходите и да намалите риска: https://cisco.com/go/sdwan.

История на документа

Нова или преразгледана тема	Описана в	Дата
Първоначално създаване на информационен лист с издаване на SD-WAN версия 17.2	Нова	08.05.2020

Централен офис Америка
Cisco Systems, Inc.
San Jose, Калифорния

Централен офис Азия и Тихия океан
Cisco Systems (USA) Pte. Ltd.
Сингапур

Централен офис Европа
Cisco Systems International BV Amsterdam,
Нидерландия

Cisco има повече от 200 офиса в цял свят. Адресите, номерата на телефони и номерата на факсове са дадени на уебсайта на Cisco на https://www.cisco.com/go/offices.

Отпечатано в САЩ C78-743816-00 06/20

Подписаният Колю Ненов Колев удостоверявам верността на извършения от мен превод от английски на български език на приложения документ – Cisco SD-WAN версия 17.2, издаден от Cisco на 08.05.2020 година. Преводът се състои от 8 (осем) страници.

Преводач: [redacted] *енов Колев)*

CISCO
The bridge to possible

Data sheet
Cisco public

Cisco SD-WAN

ВЯРНО С ОРИГИНАЛА

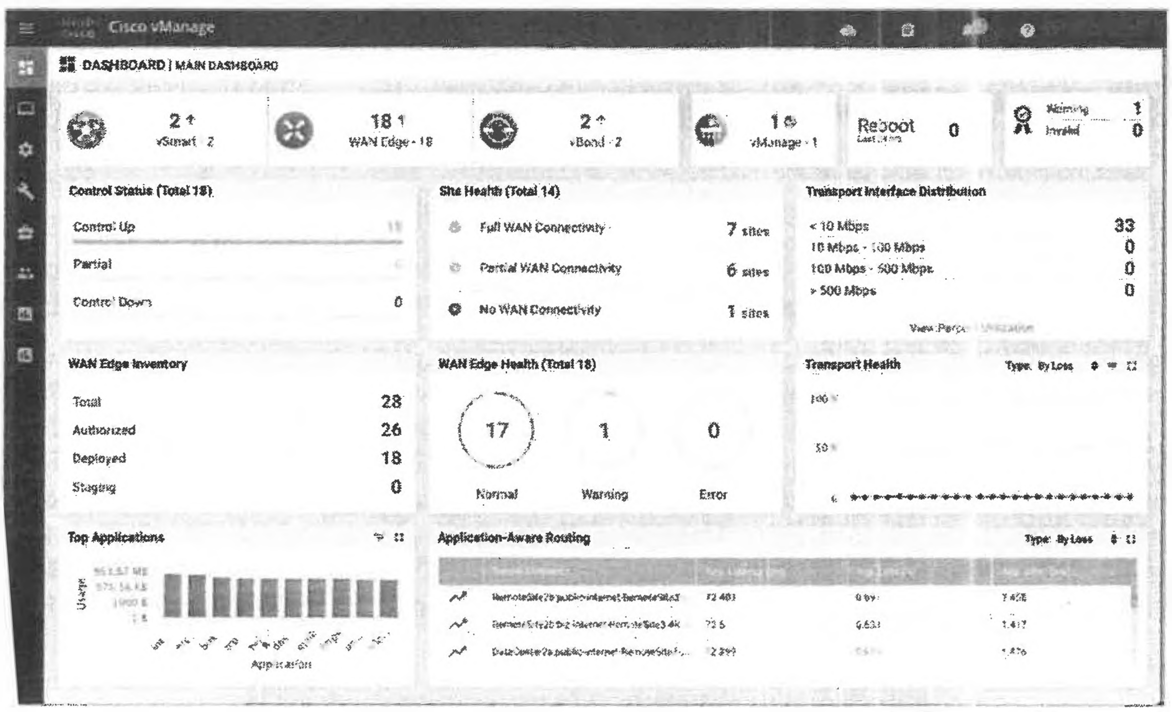
А1 България ЕАД

Contents

The Cisco® SD-WAN solution offers a complete SD-WAN fabric with centralized management and security built in, creating a secure overlay WAN architecture across campus, branch, and data center and multicloud applications. The software solution runs on a range of SD-WAN routers across hardware, virtual, and cloud form factors.

Solution overview

The Cisco SD-WAN dashboard (Figure 1) connects all company data centers, core and campus locations, WAN branches, colocation facilities, cloud infrastructure, and remote workers. Cisco SD-WAN uses the Overlay Management Protocol (OMP) to control the entire network. It simplifies IT operations with automated provisioning, unified policies, and streamlined management to help ensure rapid updates and resolutions, and provides advanced network functionality, reliability, and security.



gure 1.
ıe Cisco SD-WAN dashboard

ВЯРНО С ОРИГИНАЛА

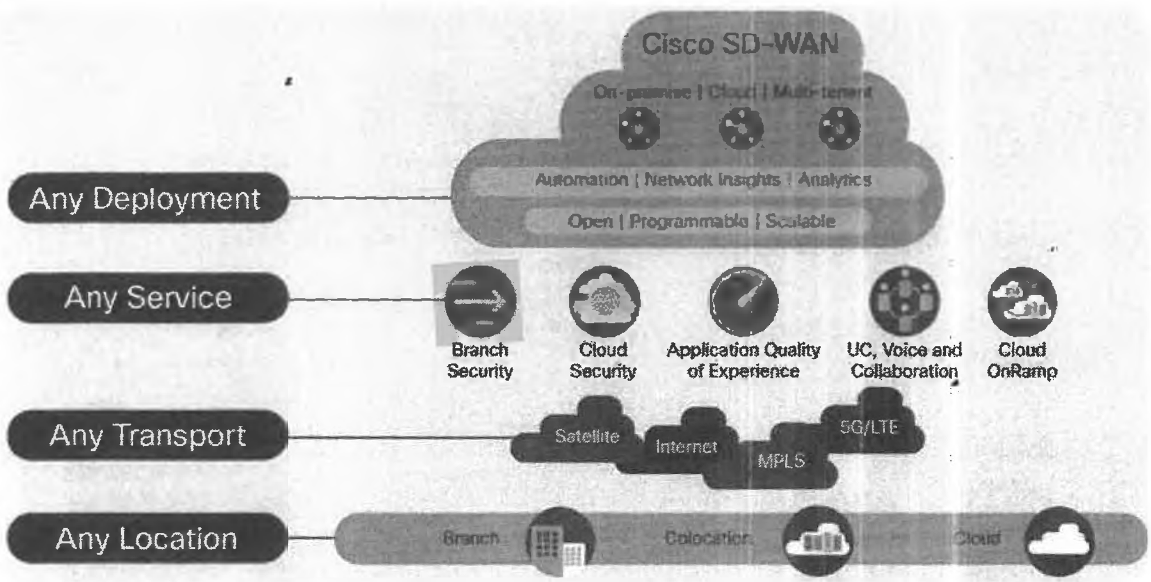


Figure 2.
The Cisco SD-WAN secure, cloud-scale architecture

Cisco SD-WAN provides a flexible architecture to extend SD-WAN to any environment (Figure 2). The solution automatically discovers, authenticates, and provisions both new and existing Cisco SD-WAN devices.

After connecting to Cisco SD-WAN, each network device can find the best path to the applications that reside in the data center or multicloud. Cisco SD-WAN can use any transport method (satellite, broadband, MPLS, 5G/LTE) from any location (core, edge, cloud) for any network service (security, application Quality of Experience [QoE], voice). Through OMP, Cisco SD-WAN supports both common and advanced routing protocols that are necessary for managing networks across the WAN and cloud, such as Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Virtual Router Redundancy Protocol (VRRP), and IPv6. Cisco SD-WAN provides this flexibility in both full and partial mesh encrypted deliveries, allowing maximum customization based on business needs.

Features and benefits

Feature	Benefit
Full SD-WAN feature stack with unified communications	The solution provides sophisticated control of the network with a set of features for routing, unified communications, multicloud, security, and centralized policy control and management.
Multicloud choice and control	Enables a range of optimization for multicloud applications using Cloud OnRamp architecture. It optimizes major software as a service (SaaS) applications and workflow integrations to major public clouds and collocation providers.
Security that is built in, not bolted on	Enables centralized security policies and provides segmentation across the entire network and a full security stack either on-premise or in the Cisco Umbrella® cloud (Figure 3). Instantly deploy the right security in the right place, all from a single dashboard.
Visibility and analytics	Centralizes management to make it easy to deploy SD-WAN and security while maintaining policy across thousands of sites.
M [illegible] control	Offers flexibility with a cloud-first architecture to connect any user to any application, across any cloud.

ВЯРНО С ОРИГИНАЛА

A1

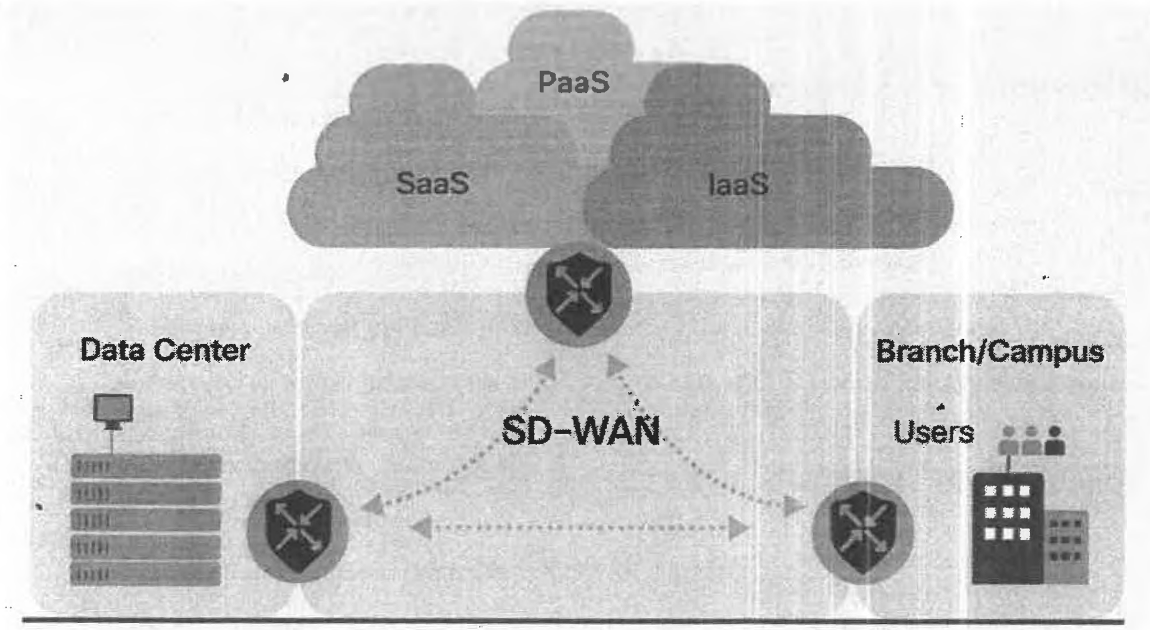


Figure 3.
Cisco SD-WAN built-in security (on-premise or Cisco Umbrella cloud)

Prominent feature

Best-in-class technology innovation

- Fully integrated security everywhere
  - Built-in security or cloud security with Cisco Umbrella Secure Internet Gateway (SIG)
  - Routing intelligence and threat intelligence on a certified trustworthy infrastructure
  - Integrated auto-registration and auto-configuration of Cisco Umbrella from SD-WAN
  - Talos security, enabling fast, industry-leading threat detection
- True SD-WAN architecture
  - Separate and dedicated components for the control plane, data plane, and management and orchestration of the WAN
  - Flexibility to implement overlay, underlay, physical, and virtual networks
  - Voice and Unified Communications (UC) support
  - IPv6 support (BGP, OSPF)

ВЯРНО С ОРИГИНАЛА

A1

- Robust IP multicast support
  - Enables network traffic control, enhances efficiency by eliminating traffic redundancy, and reduces server and CPU loads
  - Efficiently handles one-to-many or many-to-many communications
  - Provides multicast capability across platforms (PIM-SSM, IGMPv2, and IGMPv3)
- Investment protection
  - Leverages traditional transport protocols for the best application experience
  - Allows you to simply upgrade existing Cisco routers with SD-WAN functionality if your customers prefer
- Flexible multicloud deployment options
  - Cloud OnRamp for IaaS
  - Cloud OnRamp for SaaS (with Cisco IOS® XE support)
  - Cloud OnRamp for Colocation

Software feature matrix

Category	Description
Authentication, Authorization, and Accounting (AAA)	TACACS+, RADIUS, local, role-based access control
Routing	OSPF, external BGP (eBGP), internal BGP (iBGP), EIGRP, static, connected, OMP
Bridging	802.1Q, native VLAN, bridge domains, integrated routing and bridging (IRB), host-mode bridging
Security	Built-in security: Intrusion prevention system, web security, Enterprise firewall, Cisco Advanced Malware Protection (AMP), Next Generation Antivirus (NGAV), URL filtering, and SSL inspection Cloud security (Cisco Umbrella): Web security with SSL proxy, DNS-layer enforcement, URL filtering, Cloud Access Security Broker (CASB), and Enterprise firewalls. Read more: https://learn-umbrella.cisco.com/i/1153736-cisco-umbrella-secure-internet-gateway-sig-essentials/0? Device- and network-level security: Zero trust, segmentation, whitelisting, tamper-proof module, Datagram Transport Layer Security (DTLS)/TLS, IPsec, ESP-256-CBC, authentication header, HMAC-SHA1, Distributed Denial-of-Service (DDoS) protection, control plane protection, Network Address Translation (NAT) traversal
Unified Communications	SIP, public switched telephone network (PSTN) voice and fax support, Survivable Remote Site Telephony (SRST), 911 calling, conferencing, Cisco Unified Communications Manager and Webex Calling
Application/WAN optimization	Forward Error Correction (FEC) and packet duplication for User Datagram Protocol (UDP), TCP optimization, Cloud OnRamp optimization for SaaS applications

ВЯРНО С ОРИГИНАЛА

Category	Description
Multicloud and colocation	Public cloud integrations into AWS, Azure, and Google Cloud Cloud OnRamp optimization for SaaS applications Cloud OnRamp for Colocation
Forwarding and Quality of Service (QoS)	Classification, prioritization, low latency queuing, remarking, shaping, scheduling, policing, mirroring, NAT/Port Address Translation (PAT)
Multicast	Internet Group Management Protocol (IGMP) v1/v2/v3, Protocol Independent Multicast (PIM), Auto-RP, scale-out traffic replication
Policy	Route policies, app-aware routing, control policy, data policy, access control list (ACL) policy, VPN membership policy
Location services	Route policies, app-aware routing, control policy, data policy, ACL policy, VPN membership policy
Cellular	Integrated 4G/LTE modem on some devices
Mobility	Wi-Fi 802.11a/b/g/n/ac, WPA2-Enterprise, WPA2-Personal, MAC filtering, 8 SSIDs per radio, 802.11i security enhancement and 802.11e QoS, wireless intrusion detection and protection
System and network services	IPv4, Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), DNS client, Dynamic Host Configuration Protocol (DHCP) client, DHCP server, DHCP relay, configuration archival, syslog, Secure Shell (SSH), Secure Copy (SCP), NAT/PAT, Cflowd v10 IPFIX export
Configuration and monitoring	NETCONF over SSH, command-line interface (CLI), REST (vManage), Linux shell
Out-of-band management	Management port (vEdge 1000, vEdge 2000, vEdge 5000), serial console port (vEdge 1000, vEdge 2000, vEdge 5000), USB console port

Licensing

Cisco DNA Software for SD-WAN and Routing

Cisco DNA Software subscription licensing offers three feature tiers: Cisco DNA Essentials, Cisco DNA Advantage, and Cisco DNA Premier. These are nested SKUs and represent good, better, and best offers. All are [redacted] available as a 3-year or 5-year subscription and have bandwidth tier options.

Benefits:

- The latest innovations through simple subscription tiers
- Available across the portfolio
- Flexibility to choose on-premise or cloud management
- Easy license portability across on-premise and cloud
- Easy upgrade across tiers
- Software Support Service (SWSS) included

[redacted]

ВЯРНО С ОРИГИНАЛА

A1

[redacted]

For more information on Cisco DNA subscriptions, go to:
https://www.cisco.com/c/m/en_us/products/software/sd-wan-routing-matrix.html?oid=otren019258

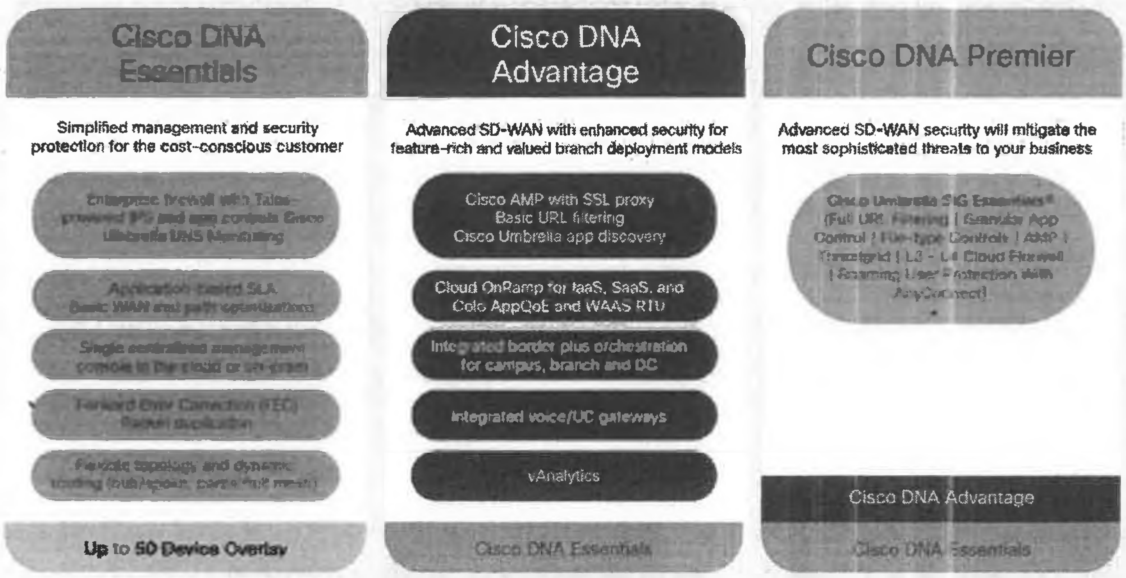


Figure 4.
Cisco DNA Software subscription licensing for SD-WAN and Routing

For more information, review the Cisco DNA Software for SD-WAN and Routing Ordering Guide.

Note: Other buying programs are available, including Enterprise Agreements (EA) and Managed Service Licensing Agreement (MSLA). A Cisco Enterprise Agreement provides a simpler way to manage licenses and reduces costs, and a single agreement covers the purchase of software and subscription licenses as well as application software support. The MSLA helps partners align business costs with a subscription-based model for their customers.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table:

Sustainability topic	Reference
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

ВЯРНО С ОРИГИНАЛА

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

For more information

See how Cisco SD-WAN can help you move faster, lower costs, and reduce risk: https://cisco.com/go/sdwan.

ВЯРНО С ОРИГИНАЛА

A1

Document history

New or Revised Topic	Described In	Date
Initial data sheet creation with SD-WAN version 17.2 release	New	05/08/2020

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices.**

Printed in USA [redacted]

ВЯРНО С ОРИГИНАЛА

Превод от английски език

Enterprise защитна стена с информираност за приложенията

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Enterprise защитна стена с информираност за приложенията

Корпоративната защитна стена на Cisco с Обръщане внимание на приложенията използва гъвкав и лесно разбираем модел на зоната за проверка на трафика в сравнение с по-стария модел, базиран на интерфейс.

Политиката на защитната стена е вид локализирана политика за сигурност, която позволява щателна проверка на потоците от данни на TCP, UDP и ICMP . Потоците на трафик, които възникват в дадена зона, могат да преминат към друга зона въз основа на политиката между двете зони. Зоната е групиране на една или повече VPN. Групирането на VPN в зони ви позволява да установите граници на сигурност във вашата наслагваща се мрежа, така че да можете да контролирате целия трафик на данни, който минава между зони.

Конфигурацията на зоната се състои от следните компоненти:

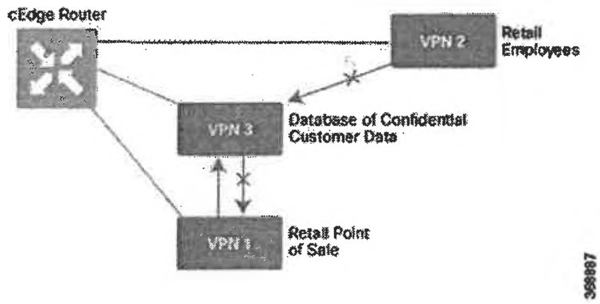
- Източна зона — групиране на VPN мрежи, откъдето произхождат потоците от данни. VPN може да бъде част от само една зона.
- Дестинационна зона — групиране на VPN, където потоците от данни прекратяват. VPN може да бъде част от само една зона.
- Политика за защитна стена — Политика за сигурност, подобна на локализирана политика за сигурност, която определя условията, при които потокът от данни на трафика от изходната зона трябва да съвпада, за да позволи на потока да продължи към зоната на местоназначение. Политиките на защитната стена могат да съответстват на IP префикси, IP портове, протоколи TCP, UDP и ICMP и приложения. Съвпадащите потоци за префикси, портове и протоколи могат да бъдат приети или изпуснати и заглавките на пакетите могат да бъдат регистрирани. Несъответстващите потоци отпадат по подразбиране. Съответстващите приложения са отказани.
- Двойна зона — контейнер, който свързва изходната зона с дестинационна зона и прилага политика на защитна стена към трафика, който протича между двете зони.

Съответстващите потоци, които са приети, могат да бъдат обработени по два различни начина:

- Инспектиране — заглавката на пакета може да бъде проверена, за да се определи неговият източник и адрес.
- Преминаване — Позволете на пакета да премине към целевата зона, без изобщо да проверява заглавката на пакета.

Следващата фигура показва прост сценарий, при който три VPN са конфигурирани на XE SD-WAN рутер. Един от VPN, VPN 3, има споделени ресурси, до които искате да ограничите достъпа. Тези ресурси могат да бъдат принтери или поверителни данни за клиентите. За останалите две VPN в този сценарий, само потребители в един от тях, VPN 1, имат право да имат достъп до ресурсите в VPN 3, докато на потребители в VPN 2 е отказан достъп до тези ресурси. В този сценарий искаме трафикът на данни да тече от VPN 1 към VPN 3, но не искаме трафикът да тече в другата посока, от VPN 3 до VPN 1.

[redacted]



Политиките на защитната стена извършват интензивна проверка на TCP, UDP и ICMP потоци между зоните. Те изследват IP адреса на източника и местоназначението в заглавките на пакетите, както и протокола на пакета. След това въз основа на конфигурираната политика, базирана на зоната, те позволяват на трафика да преминава между зоните или те изпускат трафика.

Изпълнението на политиките на защитната стена варира леко до това на локализираната политика за сигурност. Когато конфигурирате и приложите локализирана политика за защита, базирана само на VPN, вие конфигурирате и прилагате политики за защитна стена към една или повече VPN, които са групирани в зона. Активирате локализирана политика за сигурност, като я прилагате към отделни интерфейси на маршрутизаторите XE SD—WAN. Когато активирате политиките на защитната стена, те се прилагат към специфичните VPN в зоните, без да се вземат предвид конкретни интерфейси.

Защитна стена на приложението

Защитната стена на приложението проверява и блокира трафика въз основа на приложенията или семейството на приложенията. Тази функция за защитна стена, която знае приложението, осигурява следните предимства:

- Видимост на приложението и гранулиран контрол
- Класификация на 1400+ приложения 7 слой
- Блокира трафика по приложение или семейство на приложения

Можете да създавате списъци с отделни приложения или семейства от приложения. Последователност, която съдържа определено приложение или списък на семейството на приложения, може да бъде проверена. Това действие за инспекция е действие на ниво 4. Съответстващите приложения се блокират/отказват.

vEdge рутер осигурява FTP поддръжка на шлюз за приложения (ALG) с превод на мрежови адреси – Директен достъп до Интернет (NAT— DIA), услуга NAT и защитна стена на Enterprise. Поддръжката на NAT се добавя за FTP ALG на клиента, а не на FTP сървъра.

- Конфигуриране на политиките на защитната стена, на страница 2
- Примери за конфигуриране на защитна стена въз основа на зона, на страница 4

Конфигурирайте политиките на защитната стена

В vManage NMS конфигурирате политиките на защитната стена от екрана **Конфигурация> Защита,** като използвате съветника за конфигуриране на политика. В CLI конфигурирате тези защитни стени на XE SD—WAN рутера.

Конфигурационни компоненти

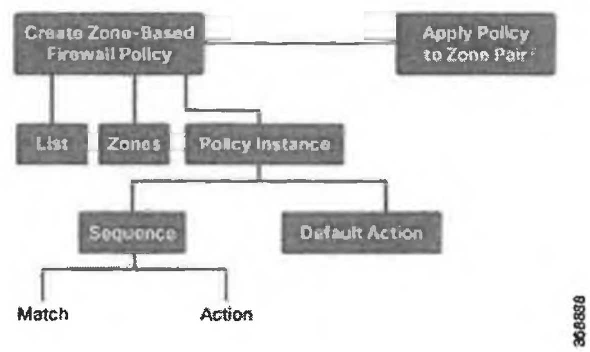
За политиките на защитната стена конфигурирате зони и политика, които да се прилагат към тези зони.

Всяка зона се състои от един от повече VPN мрежи в наслагването. Вие дефинирате изходна зона, която идентифицира VPN—тата, от които произхожда трафикът на данни, и дестинационна зона, която идентифицира VPN—тата, към които се изпраща трафика.

Политиката на защитната стена се състои от поредица от номерирани (подредени) последователности от двойки съвпадение—действие, които се оценяват по ред, от най—ниския номер на поредния номер до най—високия номер на поредицата. Когато пакет данни съвпада с условията на съвпадение, се предприемат свързаните действия или действия и оценката на политиката върху този пакет спира. Имайте предвид този процес, докато проектирате правилата си, за да гарантирате, че желаните действия са предприети по елементите, предмет на политиката.

Ако пакет не съвпада с никакви параметри в която и да е от последователностите на правилата, вие определяте действие по подразбиране, което трябва да се извърши върху пакета.

Следващата фигура илюстрира конфигурационните компоненти за политиките на защитната стена:



За да създадете политика за защитна стена на приложението, включвате следните компоненти в конфигурацията за маршрутизатор на XE SD—WAN:

Компоненти	Описание	vManage конфигурация	CLI команда за конфигуриране
списъци	Групиране на свързани елементи, които споменавате в частта за съответствие на конфигурацията на политиката на защитната стена.	Конфигурация ▶ Защита ▶ Персонализирани опции ▶ Списъци ▶ Приложение Конфигурация ▶ Защита ▶ Персонализирани опции ▶ Списъци ▶ Зони	**списъци с политики**
Политика за защитна стена	Контейнер за политика за защитна стена.	Конфигурация ▶ Защита ▶ Добавяне на политика за защита ▶ *<Сценарий>* ▶ Добавяне на политика за защитна стена	**политика зона на базата на политиката**
Номерирани последовател ности от двойки съвпадение—	Последователностите определят реда, в който се прилагат компонентите на политиката.	Конфигурация ▶ Защита ▶ Добавяне на политика за защита ▶ *<Сценарий>* ▶ Добавяне на политика за защитна стена ▶ Правило за последователност	**политика зона базирана политика политика**
Параметри на съвпадение на приложение то	Условия, които пакетите трябва да съвпадат, за да се считат за политика за сигурност.	Конфигурация ▶ Защита ▶ Добавяне на политика за сигурност ▶ *<Сценарий>* ▶ Добавяне на политика за защитна стена ▶ Правило на последователността ▶ Съвпадение ▶ Списък на	**политика зона базирана на политика последователност съвпадение списък на**

Компоненти	Описание	vManage конфигурация	CLI команда за конфигуриране
Действия	За последователност, която съдържа приложение или списък на семейството на приложенията, пакетите могат да бъдат проверявани. Съответстващите приложения	Конфигурация ► Сигурност ► Добавяне на политика за сигурност ► *<Сценарий>* ► Добавяне на политика за защитна стена ► Правило на последователността ► Действия ► Неспект	**политика инспектиране на последователностт а на действия на базата на зоната**
Действие по подразбиране	Действие, което трябва да се предприеме, ако пакет не съвпада с нито един от параметрите на съвпадение в някоя от последователностите. По	Конфигурация ► Защита ► Добавяне на политика за сигурност ► *<Сценарий>* ► Добавяне на политика за защитна стена ► Правило за последователност ► Действия	**политика падение по подразбиране, основано на зона**
Прилагайте политиката на защитната стена към	За да влезе в сила политиката на защитната стена, вие я включвате в дефиницията на зонална	Конфигурация ► Защита ► Добавяне на политика за сигурност ► *<Сценарий>* ► Прилагане на политика	**политическа зона—двойка**

Обща процедура за конфигуриране на vManage

За да конфигурирате политиките на защитната стена, използвайте съветника за конфигуриране на vManage политика. Съветникът е създател на UI политика, който ви позволява да конфигурирате компоненти на политиката:

- Създаване на списъци — Създавайте списъци, които групират заедно свързани елементи и които се обаждате в условията на съвпадение на правилата на защитната стена.
- Политика за защитна стена — дефинирайте съвпадението и условията на действие на политиката на защитната стена.
- Приложи конфигурация — Определете двойки зони.

Трябва да конфигурирате всички тези компоненти, за да създадете политика за защитна стена. Ако променяте съществуваща защитна стена, можете да пропуснете компонент, като кликнете върху бутона **Напред** в долната част на екрана. За да се върнете към компонент, кликнете върху бутона **Назад** в долната част на екрана.

Примери за конфигуриране на защитна стена на базата на зона

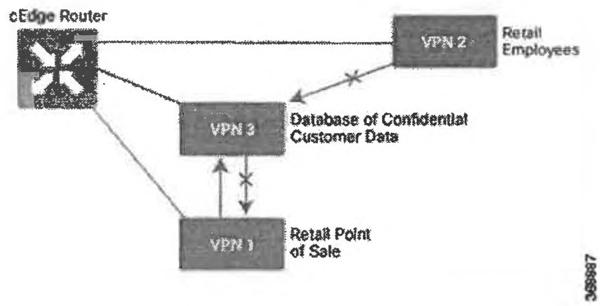
Тази тема дава пример за конфигуриране на обикновена защитна стена, базирана на зона, с помощта на CLI или vManage .

Изолиране на две VPN

В този пример за конфигуриране на защитна стена, базиран на зона, имаме сценарий, при който рутер е свързан към три мрежи от страна на услугата:

- Мрежа за гости, която предоставя услуги на PoS
- Мрежа на служителите
- Мрежа, която предоставя споделени услуги, включително споделени принтери и клиентската база данни

Искаме потребителите в мрежите на служители и гости да имат достъп до споделените услуги, но не искаме трафикът да се обменя между мрежата на служители и гости. По същия начин ние не искаме никакви трафик, който възниква от мрежата за споделени услуги, за да влезе в мрежата на служителите или в мрежата за гости. Следната фигура илюстрира този сценарий:



На тази фигура:

- VPN 1 е мрежата за гости, използвана за услуги на PoS .
- VPN 2 е мрежата, използвана от служителите на предприятието.
- VPN 3 съдържа споделените услуги, включително принтери и бази данни на клиенти.

Конфигурацията се състои от три секции:

- Определете зоните.
- Определете политиката на защитната стена, базирана на зоната.
- Приложете политиката на защитната стена, базирана на зоната, към двойка източник и дестинация зона.

Конфигурация на CLI

Първо дефинираме зоните за този сценарий:

```
vEdge (config) # политика
vEdge (config-policy) # зона пос-зона vpn 1
vEdge (config-policy) # зона служител зона
vpn 2 vEdge (конфигурация-политика) # зона услуги услуги-зона vpn 3
```

В този прост пример всяка зона съответства на един VPN. Ако по—късно трябва да добавите втори VPN за дискретна група служители (да кажем, че това е VPN 20) и искате този VPN да бъде подчинен на същата политика на защитната стена, можете просто да добавите тази VPN към зоната на служителите:

```
vEdge (config-policy) # зона служител зона vpn 20

vEdge (config-policy) # показване на политика за
пълна конфигурация зона служител зона
  vpn 2
  vpn 20
 !
!
```

След това конфигурираме политиката на защитната стена, базирана на зоната. Политиката съответства на целия трафик, който е предназначен за VPN 3, която е зоната на услугите и която има IP префикс 10.2.2.0/24. Тъй като искаме политиката да позволи на трафика да тече от VPN 1 и VPN 2 към VPN 3, но не искаме трафикът да тече в обратна посока, ние задаваме действието да **премине**

```
vEdge (доверeник-политика) # зона на базата на политиката VPN Изолиране-политика "(конфиг-зона на базата на политиката) # 10 последователност (конфиг-последователност) # съвпадение на дестинация-
IP 10.2.2.0/24
vEdge (конфигурационна последователност) # пропуск за действие
```

Искаме да изпуснем всеки трафик, който не съответства на зоната, базирана на политиката за защита на файловете :

vEdge (config-zone-based-policy) # **спад по подразбиране**

В последната стъпка от процеса на конфигуриране ние прилагаме политиката на защитната стена въз основа на зоната към зоните. Ето зоната сдвояване между гост и PoS зона и зона за услуги:

vEdge (конфигурация-политика) # **зона-двойка пос -услуги-сдвояване**

vEdge (двойка конфигурация-зона) # **изходна зона пос-зона (**

vEdge (двойка конфигурация-зона) # **услуги-дестинация зона-зона**

vEdge (конфигурация-зона -pair) # **зонова политика vpn -изолация-политика**

А ето и сдвояването между зоната на служителите и зоната на услугите:

vEdge (конфигурация-политика) # **зона-двойка служител-услуги-сдвояване**

vEdge (двойка конфигурация-зона) # **изходна зона служител-зона**

vEdge (двойка конфигурация-зона) # **услуги-дестинация зона-зона**

vEdge (конфигурация-зона -пара) # **сдвоена двойка служител-услуги-сдвояване**

Ето изглед на цялата политика:

vEdge (config-policy) # **показване на пълна конфигурация**

```
 политика
 зона служител
  зона vpn 2
! зона pos-
  zone vpn 1
 ! зона услуги -
  зона vpn 3
!
зона—двойка служител—услуги—сдвояване
  източник—зона        зона на обслужване
  на местоназначение — зона на услугите
  на работниците
  зона-политика        vpn -изолация-политика
 !
зони с двойка услуги—сдвояване
  източник—зона        пос—зона
  дестинация—зона услуги услуги—зона
  зона-политика        vpn -изолация-политика
 !
зона базирана политика vpn —изолация—
  политика
последователност 10
   съвпада
   destination-ip 10.2.2.0/24
  !
   действие преминават
  !
!
 спад по подразбиране
!
!
```

vManage конфигурация

За да конфигурирате тази политика, базирана на зона за защитна стена в vManage NMS:

1. Изберете **Конфигурация > Защита.**

2. Кликнете върху **Добавяне на политика.** Отваря се съветникът за конфигуриране на защитна стена, базиран на зоната.

Конфигурирайте групи и зони с префикс на данни на екрана Създаване на групи по интереси:

1. В левия прозорец изберете **Префикс на данни.**
2. В десния прозорец кликнете върху **Нов списък с префикс на данни.**
3. Въведете име за списъка.
4. Въведете префикса или префиксите за данни, които да включите в списъка.
5. Кликнете върху **Добави.**

Конфигурирайте зони на екрана Създаване на групи по интереси:

1. В левия прозорец изберете **Зони.**
2. В десния прозорец щракнете върху **Нов списък на зоните.**
3. Въведете име за списъка.
4. Въведете номера на зоната или зоните, които да включите в списъка. Отделете числата със запетая.
5. Кликнете върху **Добави.**
6. Кликнете върху **Напред,** за да преминете към Защитна стена на базата на зона в съветника за конфигуриране на защитна стена, базирана на зона.

Конфигуриране на базирани на зоната правила за защитна стена:

1. Кликнете върху **Добавяне на конфигурация** и изберете **Създаване на нова.**
2. Въведете име и описание на правилото.
3. В левия прозорец кликнете върху **Добавяне на последователност.**
4. В десния прозорец кликнете върху **Добавяне на правило за последователност.**
5. Изберете желаното съвпадение и условия за действие.
6. Кликнете върху **Същото съвпадение и действия.**
7. В левия прозорец щракнете върху **Действие по подразбиране.**
8. Изберете желаното действие по подразбиране.
9. Кликнете върху **Запазване на основани на зоната правила.**

Кликнете върху **Напред,** за да преминете към Прилагане на конфигурацията в съветника за конфигуриране на защитна стена, базиран на зоната.

1. Въведете име и описание за двойката зона на защитната стена, базирана на зона.
2. Кликнете върху **Добавяне на зона на двойката.**
3. В падащото меню Източна зона изберете зоната, от която произхожда трафикът на данни.
4. В падащото меню Дестинационна зона изберете зоната, към която се изпраща трафикът на данни.
5. Кликнете върху **Добави.**
6. Кликнете върху **Запазване на политиката.** След това се показва екранът **Конфигурация > Защита** и таблицата на защитните стени на базата на зоната включва новосъздадената политика.

Аз, долуподписаният, Явор Стоянов Профиров, удостоверявам верността на направения от мен превод от английски на български език на приложения документ. Преводът се състои от 8 (осем) страници.

Преводач: Явор Стоянов Профиров

Enterprise Firewall with Application Awareness

Cisco's Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.

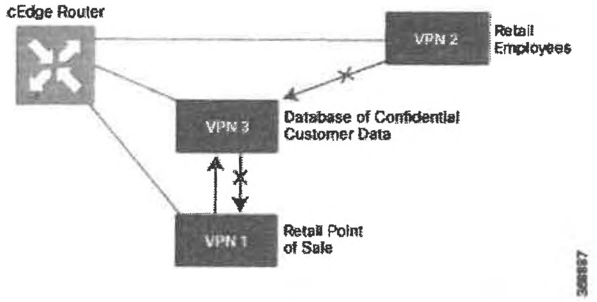
Zone configuration consists of the following components:

- Source zone—A grouping of VPNs where the data traffic flows originate. A VPN can be part of only one zone.
- Destination zone—A grouping of VPNs where the data traffic flows terminate. A VPN can be part of only one zone.
- Firewall policy—A security policy, similar to a localized security policy, that defines the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone. Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied.
- Zone pair—A container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

Matching flows that are accepted can be processed in two different ways:

- Inspect—The packet's header can be inspected to determine its source address and port.
- Pass—Allow the packet to pass to the destination zone without inspecting the packet's header at all.

The following figure shows a simple scenario in which three VPNs are configured on a XE SD-WAN Router. One of the VPNs, VPN 3, has shared resources that you want to restrict access to. These resources could be printers or confidential customer data. For the remaining two VPNs in this scenario, only users in one of them VPN 1, are allowed to access the resources in VPN 3, while users in VPN 2 are denied access to these resources In this scenario, we want data traffic to flow from VPN 1 to VPN 3, but we do not want traffic to flow in the other direction, from VPN 3 to VPN 1.



Firewall policies perform stateful inspection of TCP, UDP, and ICMP flows between zones. They examine the source and destination IP addresses and ports in the packet headers, as well as the packet's protocol. Then, based on the configured zone-based policy, they allow traffic to pass between the zones or they drop the traffic.

The implementation of firewall policies varies slightly to that of localized security policy. Where you configure and apply localized security policy based only on VPNs, you configure and apply firewall policies to one or more VPNs that have been grouped into a zone. You activate localized security policy by applying it to individual interfaces on the XE SD-WAN Routers. When you activate firewall policies, they apply to the specific VPNs in the zones, without regard to any specific interfaces.

Application Firewall

The Application Firewall inspects and blocks traffic based on applications or application-family. This application-aware firewall feature provides the following benefits:

- Application visibility and granular control
- Classification of 1400+ layer 7 applications
- Blocks traffic by application or application-family

You can create lists of individual applications or application families. A sequence that contains a specified application or application family list can be inspected. This inspect action is a Layer 4 action. Matching applications are blocked/denied.

vEdge Router provides Application Layer Gateway (ALG) FTP support with Network Address Translation – Direct Internet Access (NAT-DIA), Service NAT, and Enterprise Firewall. Service NAT support is added for FTP ALG on the client and not on the FTP Server.

- Configure Firewall Policies, on page 2
- Zone-Based Firewall Configuration Examples, on page 4

Configure Firewall Policies

In vManage NMS, you configure firewall policies from the **Configuration** > **Security** screen, using a policy configuration wizard. In the CLI, you configure these firewalls on the XE SD-WAN Router.

Configuration Components

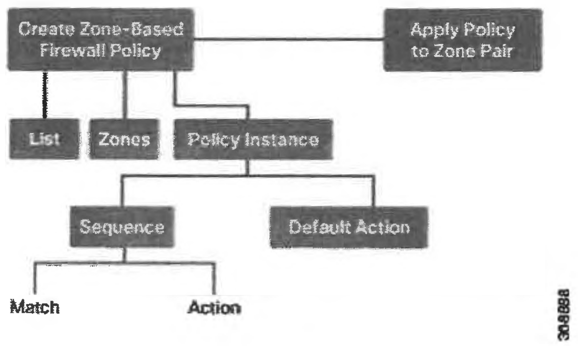
For firewall policies, you configure zones and a policy to apply to those zones.

Each zone consists of one of more VPNs in the overlay network. You define a source zone, which identifies the VPNs from which data traffic originates, and a destination zone, which identifies the VPNs to which the traffic is being sent.

The firewall policy consists of a series of numbered (ordered) sequences of match–action pairs that are evaluated in order, from lowest sequence number to highest sequence number. When a data packet matches the match conditions, the associated action or actions are taken and policy evaluation on that packet stops. Keep this process in mind as you design your policies to ensure that the desired actions are taken on the items subject to policy.

If a packet matches no parameters in any of the policy sequences, you define a default action to be taken on the packet.

The following figure illustrates the configuration components for firewall policies:



To create an application firewall policy, you include the following components in the configuration for a XE SD-WAN Router:

Component	Description	vManage Configuration	CLI Configuration Command
Lists	Groupings of related items that you reference in the match portion of the firewall policy configuration.	Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Application Configuration ▶ Security ▶ Custom Options ▶ Lists ▶ Zones	**policy lists**
Firewall policy	Container for a firewall policy.	Configuration ▶ Security ▶ Add Security Policy ▶ *<Scenario>* ▶ Add Firewall Policy	**policy zone-based-policy**
Numbered sequences of match–action pairs	Sequences establish the order in which the policy components are applied.	Configuration ▶ Security ▶ Add Security Policy ▶ *<Scenario>* ▶ Add Firewall Policy ▶ Sequence Rule	**policy zone-based-policy sequence**
Application Match parameters	Conditions that packets must match to be considered for a security policy.	Configuration ▶ Security ▶ Add Security Policy ▶ *<Scenario>* ▶ Add Firewall Policy ▶ Sequence Rule ▶ Match ▶ Application/Application Family List	**policy zone-based-policy sequence match app-list**

Component	Description	vManage Configuration	CLI Configuration Command
Actions	For a sequence that contains an application or application family list, packets can be inspected. Matching applications are blocked/denied.	Configuration ▶ Security ▶ Add Security Policy ▶ *<Scenario>* ▶ Add Firewall Policy ▶ Sequence Rule ▶ Actions ▶ Inspect	**policy zone-based-policy sequence action inspect**
Default action	Action to take if a packet matches none of the match parameters in any of the sequences. By default, non matching packets are dropped.	Configuration ▶ Security ▶ Add Security Policy ▶ *<Scenario>* ▶ Add Firewall Policy ▶ Sequence Rule ▶ Actions	**policy zone-based-policy default-action drop**
Apply firewall policy to a zone pair	For a firewall policy to take effect, you include it in the definition of a zone pair.	Configuration ▶ Security ▶ Add Security Policy ▶ *<Scenario>* ▶ Apply Policy	**policy zone-pair**

General vManage Configuration Procedure

To configure firewall policies, use the vManage policy configuration wizard. The wizard is a UI policy builder that lets you configure policy components:

- Create Lists—Create lists that group together related items and that you call in the match condition of a firewall policy.
- Firewall Policy—Define the match and action conditions of the firewall policy.
- Apply Configuration—Define zone pairs.

You must configure all these components to create a firewall policy. If you are modifying an existing firewall, you can skip a component by clicking the **Next** button at the bottom of the screen. To return to a component, click the **Back** button at the bottom of the screen.

Zone-Based Firewall Configuration Examples

This topic provides an example of configuring a simple zone-based firewall using the CLI or vManage.

Isolating Two VPNs

In this zone-based firewall configuration example, we have a scenario where a router is connected to three service-side networks:

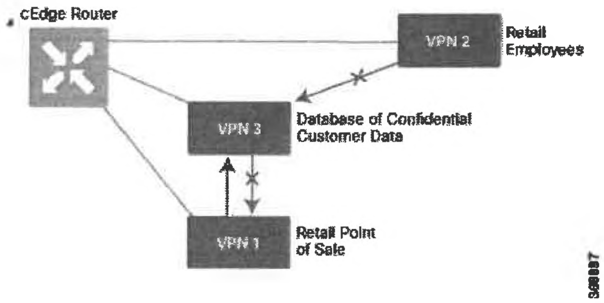
- Guest network that provides point-of-sale (PoS) services
- Employee network
- Network that provides shared services, including shared printers and the customer database

We want users in the employee and guest networks to be able to access the shared services, but we do not [illegible] traffic to be exchanged between the employee and guest networks. Similarly, we do not want any

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

traffic that originates in the shared services network to enter into either the employee network or the guest network. The following figure illustrates this scenario:



In this figure:

- VPN 1 is the guest network used for PoS services.
- VPN 2 is the network used by the enterprise's employees.
- VPN 3 contains the shared services, including printers and customer databases.

The configuration consists of three sections:

- Define the zones.
- Define the zone-based firewall policy.
- Apply the zone-based firewall policy to a source zone and destination zone pair.

CLI Configuration

First, we define the zones for this scenario:

```
vEdge(config)# policy
vEdge(config-policy)# zone pos-zone vpn 1
vEdge(config-policy)# zone employee-zone vpn 2
vEdge(config-policy)# zone services-zone vpn 3
```

In this simple example, each zone corresponds to a single VPN. If you were to later add a second VPN for a discrete group of employees (let's say this is VPN 20) and you wanted this VPN to be subject to the same firewall policy, you could simply add this VPN to the employee zone:

```
vEdge(config-policy)# zone employee-zone vpn 20
vEdge(config-policy)# show full-configuration
policy zone employee-zone
  vpn 2
  vpn 20
 !
!
```

Next, we configure the zone-based firewall policy. The policy matches all traffic that is destined for VPN 3, which is the services zone, and which has an IP prefix of 10.2.2.0/24. Because we want the policy to allow traffic to flow from VPN 1 and VPN 2 to VPN 3, but we do not want traffic to flow in the reverse direction, we set the action to pass.

```
vEdge(config-policy)# zone-based-policy vpn-isolation-policy(config-zone-based-policy)#
sequence 10(config-sequence)# match destination-ip 10.2.2.0/24
vEdge(config-sequence)# action pass
```

ВЯРНО С ОРИГИНАЛА
A1
EAA

We want to drop any traffic that does not match the zone-based filrewall policy:

```
vEdge(config-zone-based-policy)# default-action drop
```

In the final step of the configuration process, we apply the zone-based firewall policy to the zones. Here is the zone pairing between the guest and PoS zone and the services zone:

```
vEdge(config-policy)# zone-pair pos-services-pairing
vEdge(config-zone-pair)# source-zone pos-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-policy vpn-isolation-policy
```

And here is the pairing between the employee zone and the services zone:

```
vEdge(config-policy)# zone-pair employee-services-pairing
vEdge(config-zone-pair)# source-zone employee-zone
vEdge(config-zone-pair)# destination-zone services-zone
vEdge(config-zone-pair)# zone-pair employee-services-pairing
```

Here is a view of the entire policy:

```
vEdge(config-policy)# show full-configuration
 policy
 zone employee-zone
  vpn 2
! zone pos-zone
  vpn 1
 ! zone services-zone
  vpn 3
!
zone-pair employee-services-pairing
  source-zone      employee-zone
  destination-zone services-zone
  zone-policy      vpn-isolation-policy
 !
zone-pair services-pairing
  source-zone      pos-zone
  destination-zone services-zone
  zone-policy      vpn-isolation-policy
 !
zone-based-policy vpn-isolation-policy
  sequence 10
   match
   destination-ip 10.2.2.0/24
   !
   action pass
   !
!
 default-action drop
!
!
```

vManage Configuration

To configure this zone-based firewall policy in vManage NMS:

1. Select **Configuration** > **Security**.
2. Click **Add Policy**. The zone-based firewall configuration wizard opens.

Configure data prefix groups and zones in the Create Groups of Interest screen:

ВЯРНО С ОРИГИНАЛА

1. In the left pane, select **Data Prefix**.
2. In the right pane, click **New Data Prefix List**.
3. Enter a name for the list.
4. Enter the data prefix or prefixes to include in the list.
5. Click **Add**.

Configure zones in the Create Groups of Interest screen:

1. In the left pane, select **Zones**.
2. In the right pane, click **New Zone List**.
3. Enter a name for the list.
4. Enter the number of the zone or zones to include in the list. Separate numbers with a comma.
5. Click **Add**.
6. Click **Next** to move to Zone-Based Firewall in the zone-based firewall configuration wizard.

Configure zone-based firewall policies:

1. Click **Add Configuration**, and select **Create New**.
2. Enter a name and description for the policy.
3. In the left pane, click **Add Sequence**.
4. In the right pane, click **Add Sequence Rule**.
5. Select the desired match and action conditions.
6. Click **Same Match and Actions**.
7. In the left pane, click **Default Action**.
8. Select the desired default action.
9. Click **Save Zone-Based Policy**.

Click **Next** to move to the Apply Configuration in the zone-based firewall configuration wizard.

1. Enter a name and description for the zone-based firewall zone pair.
2. Click **Add Zone Pair**.
3. In the Source Zone drop-down, select the zone from which data traffic originates.
4. In the Destination Zone drop-down, select the zone to which data traffic is sent.
5. Click **Add**.
6. Click **Save Policy**. The **Configuration** > **Security** screen is then displayed, and the zone-based firewalls table includes the newly created policy.

ВЯРНО С ОРИГИНАЛА

ВЯРНО С ОРИГИНАЛА

Превод от английски език

Копиране на пакети за шумни канали

Копиране на пакети за шумни канали

Таблица 1: История на функциите

Име на функция	Информация за издаване	Описание
Копиране на пакети за шумни канали	Версия на SD-WAN на Cisco 19.2.1	Тази функция помага за намаляване на загубата на пакети по шумни канали, като по този начин поддържа високо QoE приложение за глас и видео.

- Информация за копиране на пакети, на страница 1
- Конфигурирайте копиране на пакети, на страница 1
- Наблюдавайте копиране на пакети на приложение, на страница 2

Информация за копиране на пакети

Устройствата на Cisco vEdge използват дублиране на пакети, за да преодолеят загубата на пакет.

Дублирането на пакети изпраща копия на пакети на алтернативни налични пътища, за да достигне до устройства на Cisco vEdge . Ако един от пакетите е загубен, копие на пакета се препраща към сървъра. Получаването на устройства на Cisco vEdge изхвърля копията на пакета и препраща един пакет към сървъра.

Дублирането на пакети е подходящо за ръбове с множество връзки за достъп. След като дублирането на пакети е конфигурирано и избутано към вашето устройство, можете да видите статистическите данни за дублиране на пакети в тунела.

Конфигурирайте копиране на пакети

Стъпка 1 Изберете **Конфигурация> Политики.**

Стъпка 2 Изберете **Централизирана политика** в горната част на страницата и след това щракнете върху Добавяне на политика.

Стъпка 3 Кликнете върху **Напред** два пъти, за да изберете Конфигуриране на правила за движение.

Стъпка 4 Изберете **Данни за трафика** и от падащото меню Добавяне на политика изберете щракнете върху **Създаване на нов.**

Стъпка 5 Кликнете върху **Тип последователност** в левия панел.

Стъпка 6 От изскачащото меню Добавяне на политика за данни изберете **QoS**.

Стъпка 7 Кликнете върху **Правило за последователност**.

Стъпка 8 В списъка със **приложения/списък на приложения/префикс на данни** изберете едно или повече приложения или списъци.

Стъпка 9 Кликнете върху **Действия** и изберете **Корекция на загубата.**

Стъпка 10 В областта Действия изберете опцията за **копиране на пакети**, за да активирате функцията за копиране на пакети.

- **FEC Адаптивно** — изпраща информация за корекция на грешки напред (FEC) само когато системата открие загуба на пакет.
- **FEC Винаги** — Винаги изпращайте информация за FEC при всяко предаване.
- **Няма** — Използвайте, когато не е необходима защита от загуби.
- **Копиране на пакети** — Активирайте, когато пакетите трябва да бъдат дублирани и изпратени на следващите налични връзки, за да се намали загубата на пакет.

Стъпка 11 Кликнете върху **Запазване на съвпадението и действията.**

Стъпка 12 Кликнете върху Запазване на политиката за данни.

Стъпка 13 Кликнете върху **Напред** и предприемете тези действия, за да създадете централизирана политика:

- Въведете име и описание.
- Изберете **Политика за данни за трафика.**
- Изберете **VPN/списък на сайтове** за политиката.
- Запазете правилата.

Наблюдение на дублиране на пакети на приложение

Стъпка 1 Изберете **Монитор > Мрежа.**

Стъпка 2 Изберете група устройства.

Стъпка 3 В левия панел кликнете върху **Приложения**.

Стъпка 4 В раздела Използване на приложения изберете семейството на приложенията и щракнете върху списъка със семейство на приложения.

Стъпка 5 Ако дублирането на пакети е разрешено за всяко приложение, vManage показва ефективността на доставката на пакети като ДОБРО, УМЕРЕНО или ЛОШО, или полето се показва като N/A.

Стъпка 6 ДОБРОТО и УМЕРЕНО изпълнение е връзка с възможност за кликване. Когато щракнете върху връзката, състоянието изскача прозорец.

Стъпка 7 В изскачащия прозорец виждате приложение, ефективност на доставката на пакети, като цяло за приложението, средна скорост на отпадане и като цяло за информацията за приложението. Графиката на времевия слот представлява пакетите, предавани с различни налични цветове на връзката, и общата производителност, изчислена, когато е активирано дублирането на пакети.

Стъпка 8 Ако задържите курсора на мишката върху времевия интервал, можете да видите състоянието на производителността и средната степен на спад за всяка връзка.

Аз, долуподписаният, Явор Стоянов Профиров, удостоверявам верността на направения от мен превод от английски на български език на приложения документ. Преводът се състои от 3 страници.

Преводач: [redacted] *фиров*

[redacted]

[redacted]

Packet Duplication for Noisy Channels

Table 1: Feature History

Feature Name	Release Information	Description
Packet Duplication for Noisy Channels	Cisco SD-WAN Release 19.2.1	This feature helps mitigate packet loss over noisy channels, thereby maintaining high application QoE for voice and video.

Information about Packet Duplication

Cisco vEdge devices use packet duplication to overcome packet loss.

Packet duplication sends copies of packets on alternate available paths to reach Cisco vEdge devices. If one of the packets is lost, a copy of the packet is forwarded to the server. Receiving Cisco vEdge devices discard copies of the packet and forward one packet to the server.

Packet duplication is suitable for edges with multiple access links. Once packet duplication is configured and pushed to your device, you can see the tunnel packet duplication statistics.

Configure Packet Duplication

Step 1 Select **Configuration > Policies**.

Step 2 Select **Centralized Policy** at the top of the page and then click **Add Policy**.

Step 3 Click **Next** twice to select Configure Traffic Rules.

Step 4 Select **Traffic Data**, and from the Add Policy drop-down menu, select click **Create New**.

Step 5 Click **Sequence Type** in the left panel.

Step 6 From the Add Data Policy pop-up menu, select **QoS**.

Step 7 Click **Sequence Rule**.

Step 8 In the **Applications/Application Family List/Data Prefix**, Select one or more applications or lists..

ВЯРНО С ОРИГИНАЛА

Step 9 Click **Actions** and select **Loss Correction**.

Step 10 In the Actions area, select the **Pack Duplication** option to enable the packet duplication feature.

- **FEC Adaptive**—Only send Forward Error Correction (FEC) information when the system detects a packet loss.
- **FEC Always**—Always send FEC information with every transmission.
- **None**—Use when no loss protection is needed.
- **Packet Duplication**—Enable when packets need to be duplicated and sent on the next available links to reduce packet loss.

Step 11 Click **Save Match and Actions**.

Step 12 Click **Save Data Policy**.

Step 13 Click **Next** and take these actions to create a Centralized Policy:

- Enter a Name and a Description.
- Select **Traffic Data Policy**.
- Choose **VPNs/site list** for the policy.
- Save the policy.

Monitor Packet Duplication Per Application

Step 1 Select **Monitor** > **Network**.

Step 2 Select a device group.

Step 3 In the left panel, click **Applications**.

Step 4 On the Application usage tab, select the application family of interest, and click on the Application family listed.

Step 5 If packet duplication is enabled for any application, vManage displays Packet Delivery Performance as GOOD, MODERATE, or POOR or the field displays as N/A.

Step 6 GOOD and MODERATE performance is a clickable link. When clicking on the link, the status pops up a window.

Step 7 On the pop-up window, you see Application, Packet Delivery Performance, Overall for the Application, Average Drop Rate, and Overall for the Application information. The time slot graph represents the packets transmitted with different available link colors and the overall performance calculated when packet duplication is enabled.

Step 8 If you hover over the time slot, you can see the performance status and the average drop rate for each link.

ВЯРНО С ОРИГИНАЛА

Превод от английски език

Преглед на политиката

[redacted]офия 1504, ул. "Св. Климент Охридски" №42
тел.: 02/ 946 13 92; тел./факс: 02/ 943 86 65
e-mail: office@fides.bg
[redacted]ides.bg

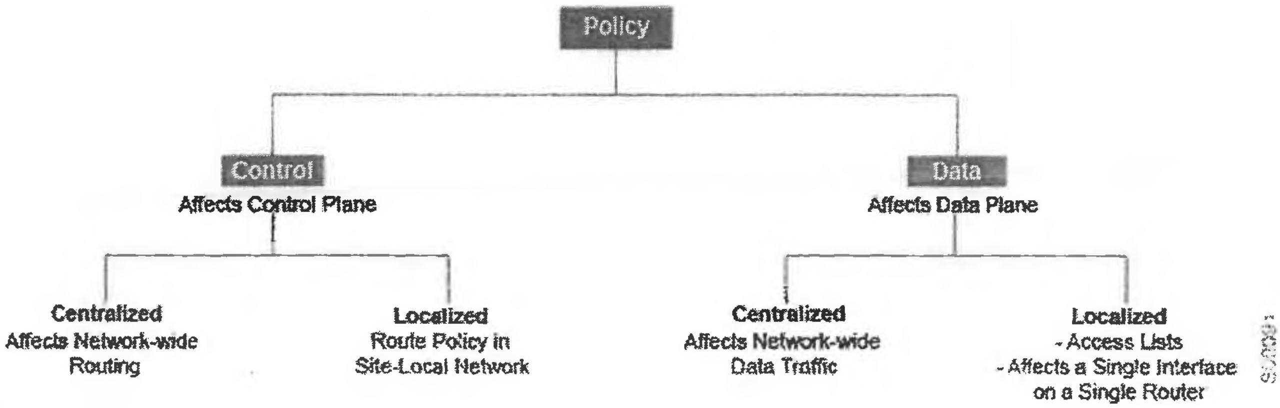
Преглед на политиката

Политиката се използва за влияние върху потока на трафик на данни между vEdge рутери в мрежата на наслагване. Политиката включва:

- *Политика за маршрутизиране*, която влияе на потока от информация за маршрутизация в контролната равнина на мрежата
- *Политика за данни*, която влияе на потока на трафика на данни в равнината на данни на мрежата

За да внедрите специфични за предприятието изисквания за контрол на трафика, създавате основни политики и внедрявате разширени функции на софтуера Viptela, които се активират с помощта на инфраструктурата за конфигуриране на политики.

Точно както мрежовата архитектура на наслагването на Viptela ясно отделя контролната равнина от равнината на данни и ясно разделя контрола между централизирани и локализирани функции, софтуерът за политиката на Viptela е чисто разделен: политиките се прилагат или за трафик на контролна равнина или за равнина на данни и се конфигурират или централно (на vSmart контролери) или локално (на vEdge рутери). Следващата фигура илюстрира разделението между политиката за контрол и данни и между централизираната и местната политика.



Дизайнът на софтуера на политиката Viptela прави разлика между основна и напреднала политика. Основната политика ви позволява да влияете или да определяте основния трафик на потока през мрежата на наслагване. Тук изпълнявате стандартни задачи за политика, като например управление на пътищата, по които трафикът се пренасочва през мрежата, и разрешаване или блокиране на трафик въз основа на полета адрес, порт и DSCP в IP заглавката на пакета. Можете също така да контролирате потока на трафик на данни към и извън интерфейсите на маршрутизатора на vEdge, като активирате функции, като клас на обслужване и опашка, огледално оформяне и управление на полицията.

Разширените функции на софтуера за политики Viptela предлагат специализирани мрежови приложения, базирани на политики. Примерите за тези приложения включват следното:

- Верижно обслужване, което пренасочва трафика на данни към споделени устройства в мрежата, като защитна стена, откриване и предотвратяване на проникване (IDS), балансиращо натоварване и други устройства, преди трафикът да бъде доставен до местоназначението си. Верижното обслужване премахва необходимостта да има отделно устройство на всеки клон сайт.

- Маршрутизиране, съобразено с приложенията, което избира най-добрия път за трафик въз основа на характеристиките на мрежата и ефективността на пътя в реално време.
- Cflowd, за следене на трафика.
- Преобразуването на vEdge рутер в NAT устройство, за да се позволи трафик, предназначен за Интернет или друга обществена мрежа, може да излезе директно от рутера vEdge.

По подразбиране никаква политика от всякакъв вид не е конфигурирана на устройства Viptela, нито на централизираните контролери vSmart или на локалните рутери vEdge . Когато трафикът на самолета за контрол, който разпространява информация за маршрута, не е политически :

- Цялата информация за маршрута, която OMP разпространява сред Viptela устройства, се споделя, немодифицирана, между всички vSmart контролери и всички vEdge рутери в домейна на наслагване.
- Няма BGP или OSPF маршрутни правила, които да повлияят на информацията за маршрута, която рутерите vEdge разпространяват в локалната си мрежа.

Когато трафикът на информационната равнина е неполитичен , целият трафик на данни се насочва към местоназначението си въз основа единствено на записите в маршрутната таблица на локалния vEdge маршрутизатор и всички VPN в мрежата за наслагване могат да обменят трафик на данни.

Тази статия разглежда структурните компоненти на маршрутизацията и политиката на данни в мрежата за наслагване на Viptela.

Централизирана и локализирана политика

Софтуерният дизайн на политиката Viptela осигурява ясно разделение между централизирана и локализирана политика. Накратко, централизираната политика се предоставя на централизираните контролери vSmart в мрежата на наслагване, а локализираната политика се предоставя на рутерите vEdge , които седят на ръба на мрежата между клон или предприятие и транспортна мрежа, като например Интернет, MPLS или метро Ethernet.

Централизирана политика

Централизираната политика се отнася до политиката, предвидена за vSmart контролери, които са централизираните контролери в мрежата за наслагване на Viptela. Централизираната политика включва два компонента:

- Политика за контрол, която влияе върху маршрутизирането на трафика в цялата мрежа
- Политика за данни, която влияе на потока на трафик на данни в VPN сегментите в мрежата

Политиката за централизирано управление се прилага за маршрутизиране на трафика в цялата мрежа, като влияе на информацията, която се съхранява в маршрутна таблица на контролера vSmart и която се рекламира на рутерите vEdge. Ефектите от политиката на централизирано управление се виждат в това как рутерите vEdge насочват трафика на данни на наслагваната мрежа към местоназначението им. Самата конфигурация на централизираната контролна политика остава на контролера vSmart и никога не се натиска към локални рутери.

Централизираната политика за данни се прилага за потока от трафик на данни през VPN-ите в мрежата на наслагване. Тези правила могат да разрешават и ограничават достъпа въз основа или на 6-кратно съвпадение (източник и дестинация IP адреси и портове, DSCP полета и протокол) или на членство в VPN. Тези правила са изтласкани към засегнатите рутери vEdge .

Локализирана политика

Локализираната политика се отнася до политика, която се предлага локално, на рутерите vEdge в мрежата за наслагване

Локализираната политика за контрол, която също се нарича маршрутна политика, влияе върху поведението на маршрутизация BGP и OSPF в локалната мрежа на сайта.

Локализираната политика за данни ви позволява да предоставите списъци за достъп и да ги прилагате към определен интерфейс или интерфейси на рутера. Простите списъци за достъп позволяват и ограничават достъпа въз основа на 6-кратно съвпадение (източник и дестинация IP адреси и портове, DSCP полета и протокол) по същия начин, както при централизираната политика за данни. Списъците за достъп също позволяват предоставяне на клас на обслужване (CoS), управление на полицията и огледално огледало, които контролират как изтича трафикът на данни към и към интерфейсите на маршрутизатора и интерфейсните опашки.

Политика за контрол и данни

Дизайнът на мрежовата политика на Viptela осигурява чисто разделяне между политиката за контрол и политиката на данни, за да се приведе в съответствие с мрежовата архитектура, в която равнините за управление и данни са чисто разделени. Политиката за контрол е еквивалентна на политиката на протокола за маршрутизиране, а политиката за данни е еквивалентна на това, което обикновено се нарича списъци за контрол на достъпа (ACL) и филтри на защитната стена.

Политика за контрол

Политиката за управление, която е подобна на стандартната политика за маршрутизиране, работи на маршрути и информация за маршрутизация в контролната равнина на мрежата за наслагване. Централизираната политика за управление, която се предлага на контролера vSmart , е техниката Viptela за персонализиране на решения за маршрутизиране в цялата мрежа, които определят или влияят на маршрутите за маршрутизиране през мрежата на наслагване.

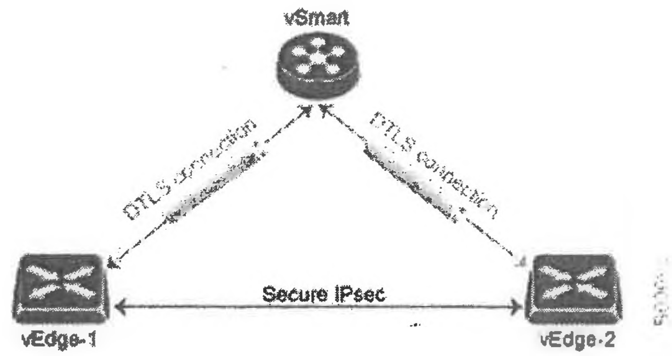
Политиката за локален контрол, която се предлага на рутер vEdge , позволява персонализиране на решения за маршрутизиране, взети от BGP и OSPF в локални клонове или корпоративни мрежи на сайта.

Информацията за маршрута, която е в основата на политиката за централизирано управление, се съдържа в маршрутни реклами на Viptela, които се предават на DTLS или TLS контролни връзки между vSmart контролери и vEdge рутери.

Политиката за централизирано управление определя кои маршрути и информация за маршрута се поставят в централизираната таблица на маршрутите на контролера vSmart и кои маршрути и информация за маршрута се рекламират на рутерите vEdge в мрежата на наслагване. Основната политика за централизирано управление създава инженерно движение, за да зададе пътя, който трафикът преминава през мрежата.

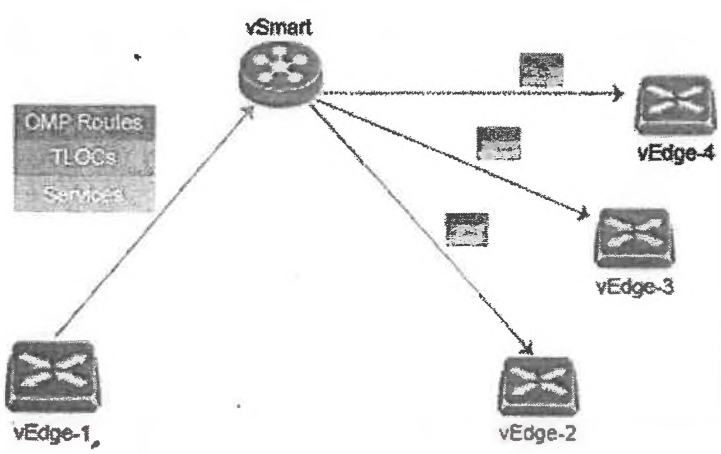
Политиката за усъвършенстван контрол поддържа редица функции, включително верижно обслужване, което позволява на VEdge рутери в мрежата за наслагване да споделят мрежови услуги, като защитни стени и балансиращи натоварвания.

Централизираната политика за управление засяга OMP маршрутите, които се разпределят от vSmart контролера в цялата мрежа на наслагване. В vSmart контролера научава наслагване мрежова топология на от OMP маршрути, които се рекламират от vEdge рутери през OMP сесии във вътрешността на DTLS или TLS връзките между vSmart контролера и рутери. (Връзките DTLS са показани в оранжево на фигурата вдясно).



Три типа OMP маршрути носят информацията, която контролерът vSmart използва за определяне на мрежовата топология:

- Viptela OMP маршрутите, които са подобни на рекламите за IP маршрути, рекламират информация за маршрутизация, която рутерите vEdge са научили от своя местен сайт и локалните протоколи за маршрутизиране (BGP и OSPF) на контролера vSmart . Тези маршрути се наричат също OMP маршрути или vRoutes .
- TLOC маршрутите носят специфични за локатора свойства на наслагване, включително IP адреса на интерфейса, който се свързва с транспортната мрежа, цвят на връзката, който идентифицира трафик на потока и типа на капсулиране. (TLOC или транспортно местоположение е физическото място, където маршрутизатор vEdge се свързва към транспортна мрежа. Той се идентифицира основно чрез IP адрес, цвят на връзката и капсулиране, но редица други свойства са свързани с TLOC .)
- Сервизните маршрути рекламират мрежовите услуги, като защитните стени, достъпни за членове на VPN на локалния сайт на рутера vEdge .



По подразбиране не се предвижда централизирана политика за контрол. В този гол, unpolicied мрежа, всички OMP маршрути са поставени в vSmart маса маршрут контролера, както е сега, а vSmart контролера рекламира всички OMP маршрути, какъвто е, за всички vEdge рутери в една и съща VPN в домейна мрежа.

Чрез предоставяне на централизирана политика за управление можете да повлияете кои маршрути на OMP се поставят в маршрутна таблица на контролера vSmart , каква информация за маршрута се рекламира

на рутерите vEdge и
дали маршрутите на OMP са променени,
преди да бъдат поставени в таблицата на
маршрутите или преди да бъдат
рекламирани.

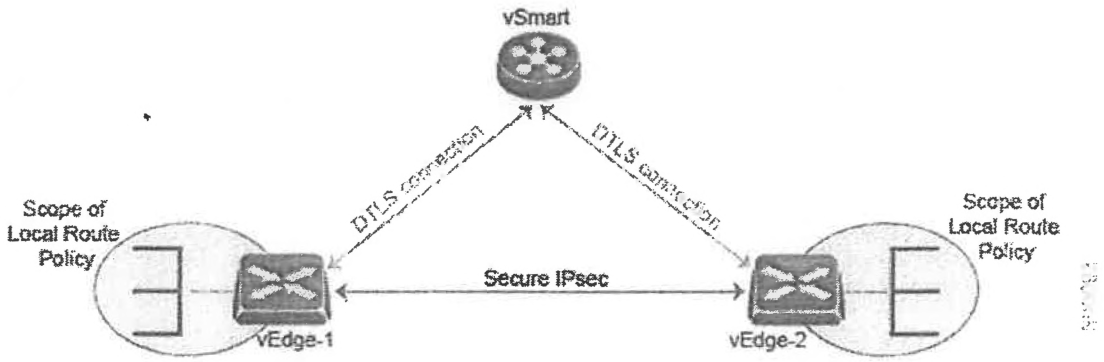
vEdge рутерите поставят цялата информация за маршрута, научена от vSmart контролерите, както е в техните локални маршрутни таблици, за използване при пренасочване на трафик на данни. Тъй като ролята на контролера vSmart е да бъде централизираната система за маршрутизиране в мрежата, vEdge рутерите никога не могат да променят информацията за маршрута на OMP , която учат от контролерите vSmart .

В vSmart контролера редовно получава OMP маршрут реклами от vEdge рутери и след преизчисляване и актуализиране на маршрутизирането на пътищата чрез мрежата за наслагване, то рекламира новата информация за маршрутизиране на vEdge рутери.

Политиката за централизирано управление, която предоставяте на контролера vSmart, остава на контролера vSmart и никога не се изтегля на рутерите vEdge . Решенията за маршрутизация, които са резултат от политиката за централизиран контрол, се предават на рутерите vEdge под формата на реклами за маршрути и така влиянието на политиката за управление се отразява в начина, по който рутерите vEdge насочват трафика на данни към местоназначението си.

Тип централизирана политика за управление, наречена верига за обслужване, позволява трафикът на данни да се препраща през една или повече мрежови услуги, като защитна стена, балансиращо натоварване и устройства за откриване и предотвратяване на проникване (IDP) по пътя към местоназначението му.

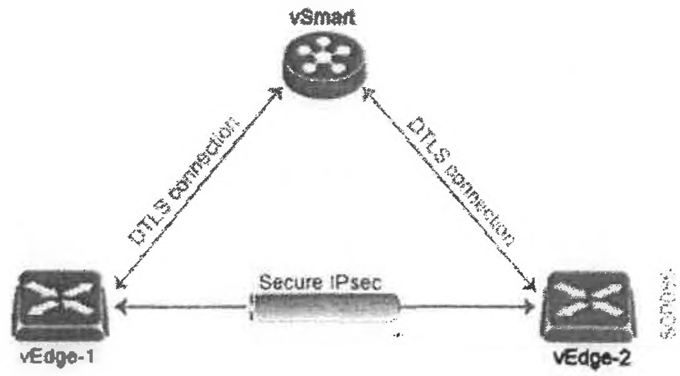
Локализираната политика за контрол, която се предлага локално на рутерите vEdge , се нарича маршрутна политика. Тази политика е подобна на политиките за маршрутизиране, които конфигурирате на обикновен рутер, което ви позволява да модифицирате поведението на маршрутизация BGP и OSPF в локалната мрежа на сайта. Докато централизираната политика за контрол засяга поведението на маршрутизация в цялата мрежа на наслагване, политиката на маршрута се прилага само за маршрутизиране в местния клон.



Политика за данни

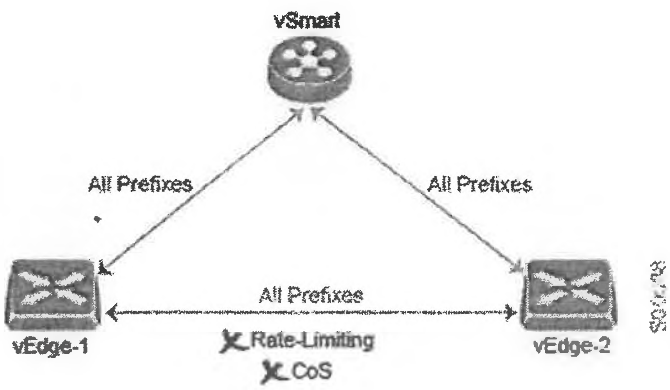
Политиката за данни влияе върху потока от трафик на данни, обикалящ мрежата въз основа или на полета в IP заглавката на пакетите, или на интерфейса на рутера, по който се предава или получава трафик. Трафикът на данни пътува по IPsec връзките между рутери vEdge , показани в лилаво на съседната фигура.

Архитектурата на Viptela реализира два типа политика на данни:



- Централизираната политика за данни контролира потока на трафик на данни въз основа на адреса на източника и местоназначението и портовете и DSCP полета в IP заглавката на пакета (наричан 5-пакетна) и въз основа на сегментиране на мрежата и членство в VPN. Тези типове политики за данни се предлагат централизирано на контролера vSmart и влияят на потока на трафика през цялата мрежа.
- Локализираната политика за данни контролира потока от данни трафик към и извън интерфейси и интерфейсни опашки на vEdge рутер. Този тип политики за данни се предлагат локално, на рутера vEdge , като се използват списъци за достъп. Тя ви позволява да класифицирате трафика и да картографирате различни класове към различни опашки. Той също така ви позволява да огледате трафика и да контролирате скоростта, с която трафикът на данни се предава и получава.

По подразбиране не се предвижда централизирана политика за данни. Резултатът е, че всички префикси в рамките на VPN са достъпни от всяка точка на VPN. Предоставянето на централизирана политика за данни ви позволява да приложите 6-кортов филтър, който контролира достъпа между източници и дестинации.



Както при централизираната политика на управление, вие предоставяте централизирана политика за данни на vSmart контролера и тази конфигурация остава на vSmart контролера. Ефектите от политиката за данни се отразяват в начина, по който рутерите vEdge насочват трафика на данни към местоназначението им. За разлика от политиката за контрол обаче централизираните полици за данни се избутват към рутерите vEdge по начин, който е само за четене. Те не се добавят към конфигурационния файл на рутера, но можете да ги видите от CLI на рутера.

Без списъци за достъп, предоставени на рутер vEdge , целият трафик на данни се предава със скорост на линия и с еднакво значение, като се използва една от опашките на интерфейса. Използвайки списъци за достъп, можете да осигурите клас услуги, който ви позволява да класифицирате трафика на данни по важност, да го разпределите по различни опашки на интерфейса и да контролирате скоростта, с която се предават

[redacted]

различните класове трафик. Можете също така да осигурите огледално огледало и полиране.

Основна и разширена политика

И накрая, дизайнът на софтуера на политиката Viptela прави разлика между основна и напреднала политика. Основната политика ви позволява да влияете или да определяте основния трафик на потока през мрежата на наслагване. Тук изпълнявате стандартни задачи за политика, като например управление на пътищата, по които трафикът се пренасочва през мрежата, като влияете на маршрутите OMP , BGP и OSPF, и разрешавате или блокирате трафика въз основа на полета адрес, порт и DSCP в пакетите IP заглавка. Можете също така да контролирате потока на трафик на данни към и извън интерфейсите на маршрутизатора на vEdge, като активирате функции, като клас на обслужване и опашка, огледално оформяне и управление на полицията.

Разширените функции на софтуера за политики Viptela предлагат специализирани мрежови приложения, базирани на политики. Примерите за тези приложения включват следното:

- Верижно обслужване, което позволява трафикът на данни да бъде пренасочен към споделена защитна стена, откриване и предотвратяване на проникване (IDS), балансиращо натоварване и други устройства, преди да бъдат доставени до местоназначението им, вместо да се изисква устройство на всеки клон сайт.
- Маршрутизиране, съобразено с приложенията, което избира най-добрия път за трафик въз основа на характеристиките на мрежата и ефективността на пътя в реално време.
- Cflowd, за следене на трафика.
- Преобразуването на vEdge рутер в NAT устройство, за да се позволи трафик, предназначен за Интернет или друга обществена мрежа, може да излезе директно от рутера vEdge.

Допълнителна информация

Централизирана политика за контрол
Централизирана политика за данни
Локализирана политика за контрол
Локализирана политика за данни

Аз, долуподписаният, Явор Стоянов Профиров, удостоверявам верността на направения от мен превод от английски на български език на приложения документ. Преводът се състои от 8 страници.

Преводач: [redacted] *Явор Стоянов Профиров*

[redacted]

[redacted]

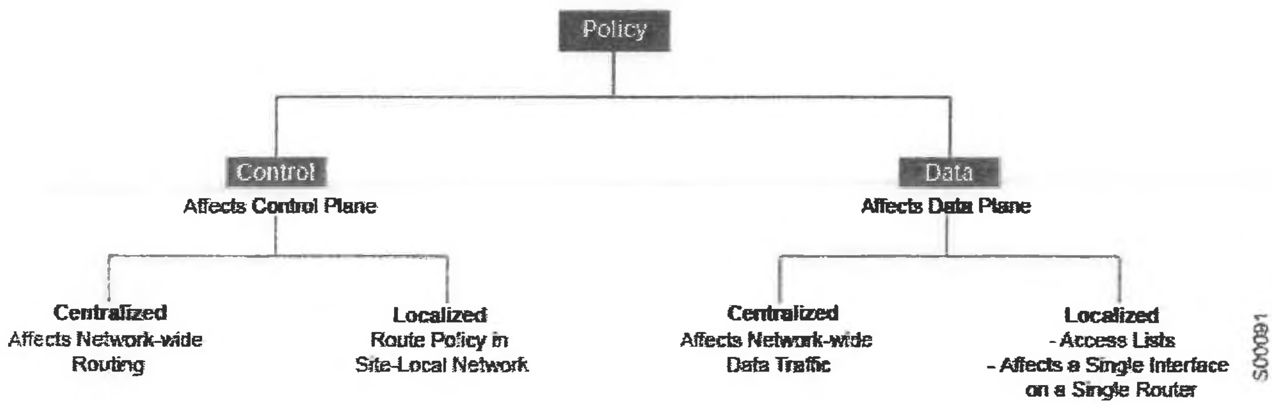
Policy Overview

Policy is used to influence the flow of data traffic among the vEdge routers in the overlay network. Policy comprises:

- *Routing policy*, which affects the flow of routing information in the network's control plane
- *Data policy*, which affects the flow of data traffic in the network's data plane

To implement enterprise-specific traffic control requirements, you create basic policies, and you deploy advanced features of the Viptela software that are activated by means of the policy configuration infrastructure.

Just as the Viptela overlay network architecture clearly separates the control plane from the data plane and clearly separates control between centralized and localized functions, the Viptela policy software is cleanly separated: policies apply either to control plane or data plane traffic, and they are configured either centrally (on vSmart controllers) or locally (on vEdge routers). The following figure illustrates the division between control and data policy, and between centralized and local policy.



The design of the Viptela policy software distinguishes between basic and advanced policy. Basic policy allows you to influence or determine basic traffic flow through the overlay network. Here, you perform standard policy tasks, such as managing the paths along which traffic is routed through the network, and permitting or blocking traffic based on the address, port, and DSCP fields in the packet's IP header. You can also control the flow of data traffic into and out of a vEdge router's interfaces, enabling features such as class of service and queuing, mirroring, and policing.

Advanced features of Viptela policy software offer specialized policy-based network applications. Examples of these applications include the following:

- Service chaining, which redirects data traffic to shared devices in the network, such as firewall, intrusion detection and prevention (IDS), load balancer, and other devices, before the traffic is delivered to its destination. Service chaining obviates the need to have a separate device at each branch site.

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

- Application-aware routing, which selects the best path for traffic based on real-time network and path performance characteristics.
- Cflowd, for monitoring traffic flow.
- Converting a vEdge router into a NAT device, to allow traffic destined for the Internet or other public network can exit directly from the vEdge router.

By default, no policy of any kind is configured on Viptela devices, either on the centralized vSmart controllers or the local vEdge routers. When control plane traffic, which distributes route information, is unpolicied:

- All route information that OMP propagates among the Viptela devices is shared, unmodified, among all vSmart controllers and all vEdge routers in the overlay network domain.
- No BGP or OSPF route policies are in place to affect the route information that vEdge routers propagate within their local site network.

When data plane traffic is unpolicied, all data traffic is directed towards its destination based on solely on the entries in the local vEdge router's route table, and all VPNs in the overlay network can exchange data traffic.

This article examines the structural components of routing and data policy in the Viptela overlay network.

Centralized and Localized Policy

The Viptela policy software design provides a clear separation between centralized and localized policy. In short, centralized policy is provisioned on the centralized vSmart controllers in the overlay network, and localized policy is provisioned on the vEdge routers, which sit at the network edge between a branch or enterprise site and a transport network, such as the Internet, MPLS, or metro Ethernet.

Centralized Policy

Centralized policy refers to policy provisioned on vSmart controllers, which are the centralized controllers in the Viptela overlay network. Centralized policy comprises two components:

- Control policy, which affects the overlay network–wide routing of traffic
- Data policy, which affects the data traffic flow throughout the VPN segments in the network

Centralized control policy applies to the network-wide routing of traffic by affecting the information that is stored in the vSmart controller's route table and that is advertised to the vEdge routers. The effects of centralized control policy are seen in how vEdge routers direct the overlay network's data traffic to its destination. The centralized control policy configuration itself remains on the vSmart controller and is never pushed to local routers.

Centralized data policy applies to the flow of data traffic throughout the VPNs in the overlay network. These policies can permit and restrict access based either on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol) or on VPN membership. These policies are pushed to the affected vEdge routers.

Localized Policy

Localized policy refers to policy that is provisioned locally, on the vEdge routers in the overlay network

Localized control policy, which is also called route policy, affects the BGP and OSPF routing behavior on the site-local network.

Localized data policy allows you to provision access lists and apply them to a specific interface or interfaces on the router. Simple access lists permit and restrict access based on a 6-tuple match (source and destination IP addresses and ports, DSCP fields, and protocol), in the same way as with centralized data policy. Access lists also allow provisioning of class of service (CoS), policing, and mirroring, which control how data traffic flows out of and in to the router's interfaces and interface queues.

Control and Data Policy

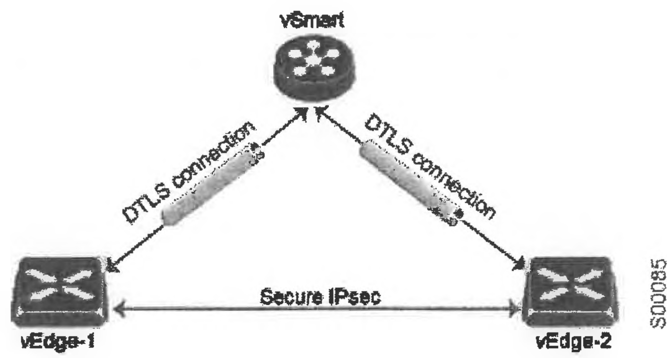
The Viptela network policy design provides a clean separation between control policy and data policy, to align with the network architecture in which the control and data planes are cleanly separated. Control policy is the equivalent of routing protocol policy, and data policy is equivalent to what are commonly called access control lists (ACLs) and firewall filters.

Control Policy

Control policy, which is similar to standard routing policy, operates on routes and routing information in the control plane of the overlay network. Centralized control policy, which is provisioned on the vSmart controller, is the Viptela technique for customizing network-wide routing decisions that determine or influence routing paths through the overlay network. Local control policy, which is provisioned on a vEdge router, allows customization of routing decisions made by BGP and OSPF on site-local branch or enterprise networks.

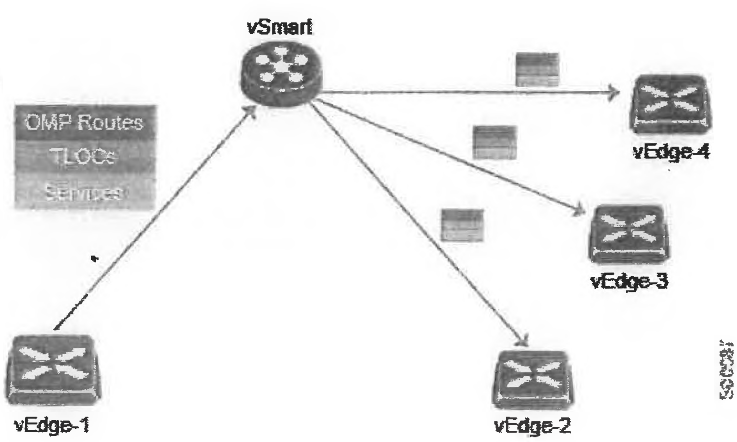
The routing information that forms the basis of centralized control policy is carried in Viptela route advertisements, which are transmitted on the DTLS or TLS control connections between vSmart controllers and vEdge routers. Centralized control policy determines which routes and route information are placed into the centralized route table on the vSmart controller and which routes and route information are advertised to the vEdge routers in the overlay network. Basic centralized control policy establish traffic engineering, to set the path that traffic takes through the network. Advanced control policy supports a number of features, including service chaining, which allows vEdge routers in the overlay network to share network services, such as firewalls and load balancers.

Centralized control policy affects the OMP routes that are distributed by the vSmart controller throughout the overlay network. The vSmart controller learns the overlay network topology from OMP routes that are advertised by the vEdge routers over the OMP sessions inside the DTLS or TLS connections between the vSmart controller and the routers. (The DTLS connections are shown in orange in the figure to the right).



Three types of OMP routes carry the information that the vSmart controller uses to determine the network topology:

- Viptela OMP routes, which are similar to IP route advertisements, advertise routing information that vEdge routers have learned from their local site and the local routing protocols (BGP and OSPF) to the vSmart controller. These routes are also referred to as OMP routes or vRoutes.
- TLOC routes carry overlay network–specific locator properties, including the IP address of the interface that connects to the transport network, a link color, which identifies a traffic flow, and the encapsulation type. (A TLOC, or transport location, is the physical location where a vEdge router connects to a transport network. It is identified primarily by IP address, link color, and encapsulation, but a number of other properties are associated with a TLOC.)
- Service routes advertise the network services, such as firewalls, available to VPN members at the vEdge router's local site.



By default, no centralized control policy is provisioned. In this bare, unpolicied network, all OMP routes are placed in the vSmart controller's route table as is, and the vSmart controller advertised all OMP routes, as is, to all vEdge routers in the same VPN in the network domain.

By provisioning centralized control policy, you can affect which OMP routes are placed in the vSmart controller's route table, what route information is advertised to the vEdge routers, and whether the OMP routes are modified before being put into the route table or before being advertised.

vEdge routers place all the route information learned from the vSmart controllers, as is, into their local route tables, for use when forwarding data traffic. Because the vSmart controller's role is to be the centralized routing system in the network, vEdge routers can never modify the OMP route information that they learn from the vSmart controllers.

The vSmart controller regularly receives OMP route advertisements from the vEdge routers and, after recalculating and

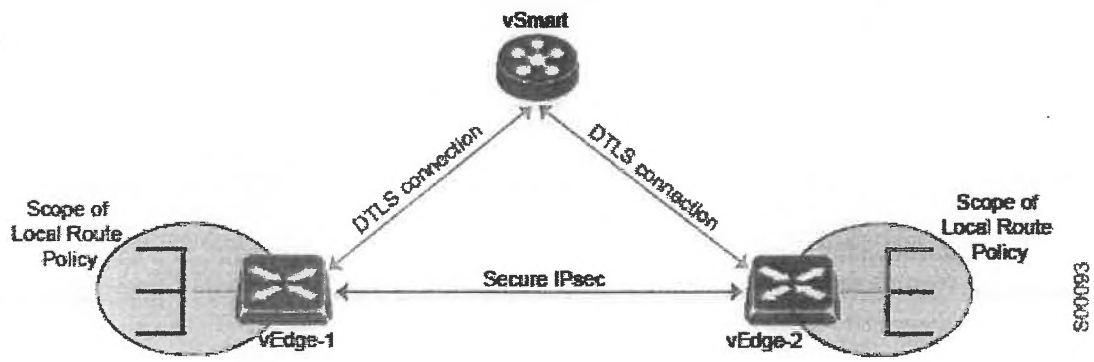
ВЯРНО С ОРИГИНАЛА

updating the routing paths through the overlay network, it advertises new routing information to the vEdge routers.

The centralized control policy that you provision on the vSmart controller remains on the vSmart controller and is never downloaded to the vEdge routers. However, the routing decisions that result from centralized control policy are passed to the vEdge routers in the form of route advertisements, and so the affect of the control policy is reflected in how the vEdge routers direct data traffic to its destination.

A type of centralized control policy called service chaining allows data traffic to be routed through one or more network services, such as firewall, load balancer, and intrusion detection and prevention (IDP) devices, en route to its destination.

Localized control policy, which is provisioned locally on the vEdge routers, is called route policy. This policy is similar to the routing policies that you configure on a regular router, allowing you to modify the BGP and OSPF routing behavior on the site-local network. Whereas centralized control policy affects the routing behavior across the entire overlay network, route policy applies only to routing at the local branch.

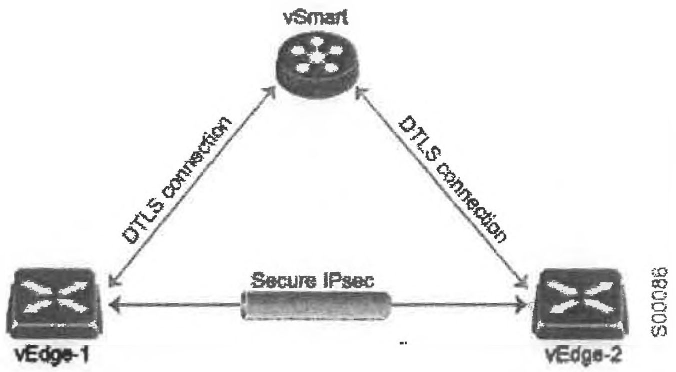


Data Policy

Data policy influences the flow of data traffic traversing the network based either on fields in the IP header of packets or the router interface on which the traffic is being transmitted or received. Data traffic travels over the IPsec connections between vEdge routers, shown in purple in the adjacent figure.

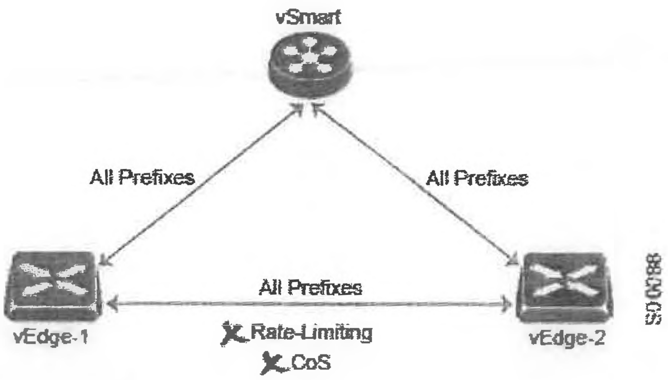
The Viptela architecture implements two types of data policy:

- Centralized data policy controls the flow of data traffic based on the source and destination addresses and ports and DSCP fields in the packet's IP header (referred to as a 5-tuple), and based on network segmentation and VPN membership. These types of data policy are provisioned centrally, on the vSmart controller, and they affect traffic flow across the entire network.



- Localized data policy controls the flow of data traffic into and out of interfaces and interface queues on a vEdge router. This type of data policy is provisioned locally, on the vEdge router, using access lists. It allows you to classify traffic and map different classes to different queues. It also allows you to mirror traffic and to police the rate at which data traffic is transmitted and received.

By default, no centralized data policy is provisioned. The result is that all prefixes within a VPN are reachable from anywhere in the VPN. Provisioning centralized data policy allows you to apply a 6-tuple filter that controls access between sources and destinations.



As with centralized control policy, you provision centralized data policy on the vSmart controller, and that configuration remains on the vSmart controller. The effects of data policy are reflected in how the vEdge routers direct data traffic to its destination. Unlike control policy, however, centralized data polices are pushed to the vEdge routers in a read-only fashion. They are not added to the router's configuration file, but you can view them from the CLI on the router.

With no access lists provisioned on a vEdge router, all data traffic is transmitted at line rate and with equal importance, using one of the interface's queues. Using access lists, you can provision class of service, which allows you to classify data traffic by importance, spread it across different interface queues, and control the rate at which different classes of traffic are transmitted. You can also provision packet mirroring and policing.

Basic and Advanced Policy

Finally, the design of the Viptela policy software distinguishes between basic and advanced policy. Basic policy allows you to influence or determine basic traffic flow through the overlay network. Here, you perform standard policy tasks, such as managing the paths along which traffic is routed through the network by influencing the OMP, BGP, and OSPF routes, and permitting or blocking traffic based on the address, port, and DSCP fields in the packet's IP header. You can also control the flow of data traffic into and out of a vEdge router's interfaces, enabling features such as class of service and queuing, mirroring, and policing.

Advanced features of Viptela policy software offer specialized policy-based network applications. Examples of these applications include the following:

- Service chaining, which allows data traffic to be redirected to shared firewall, intrusion detection and prevention (IDS), load balancer, and other devices before being delivered to its destination, rather than requiring a device at each branch site.
- Application-aware routing, which selects the best path for traffic based on real-time network and path performance characteristics.
- Cflowd, for monitoring traffic flow.
- Converting a vEdge router into a NAT device, to allow traffic destined for the Internet or other public network can exit directly from the vEdge router.

Additional Information

Centralized Control Policy
Centralized Data Policy
Localized Control Policy
Localized Data Policy

Превод от английски език

Преглед на сигурността

[redacted]

ВЯРНО С ОРИГИНАЛА

[redacted]

Преглед на сигурността

Сигурността е критичен елемент на днешната мрежова инфраструктура. Администраторите на мрежата и служителите по сигурността са силно притиснати да защитават мрежата си от атаки и нарушения. В резултат на хибридни облаци и отдалечена свързаност на служителите периметърът на сигурност около мрежите изчезва. Има много проблеми с традиционните начини за осигуряване на мрежи, включително:

- Много малък акцент се поставя върху гарантирането на автентичността на устройствата, участващи в комуникацията.
- Осигуряването на връзките между двойка устройства включва досадна и ръчна настройка на ключове и споделени пароли.
- Решенията за мащабируемост и висока наличност често противоречат помежду си.

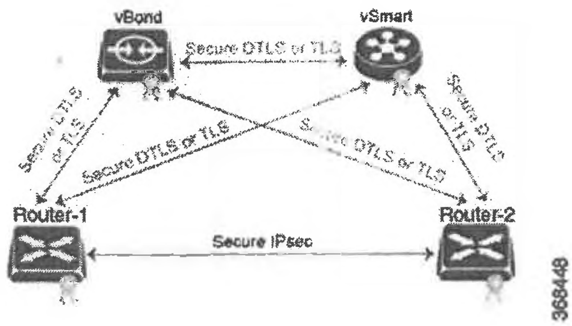
Тази глава съдържа следните теми:

Компоненти за сигурност на Cisco SD-WAN

Решението на Cisco SD-WAN използва коренно различен подход към сигурността, като основата на основния му дизайн се основава на следните предписания:

- Удостоверяване - Решението гарантира, че само автентични устройства могат да изпращат трафик един към друг.
- Шифроване - цялата комуникация между всяка двойка устройства е автоматично защитена, напълно елиминирайки режийните разходи, свързани с осигуряването на връзките.
- Цялостност - При обезопасяването на инфраструктурата не участват групови ключове или проблеми с ключовите сървъри.

Тези три компонента - автентификация, криптиране и интегритет - са ключови за осигуряването на [redacted]нфраструктура на Cisco SD-WAN.



Темите за Общ преглед на безопасността на контролната равнина и Преглед на защитата на равнината на данни изследват как автентификацията, криптирането и целостта се прилагат в цялата мрежа на наслагване на Cisco SD-WAN. Дискусията за сигурност се отнася до следната илюстрация на компонентите на Cisco SD-WAN мрежата - vSmart контролер, vBond оркестратор и рутери. Връзките между тези устройства формират контролната равнина (в оранжево) и равнината на данни (в лилаво) и именно тези връзки трябва да бъдат защитени с подходящи мерки, за да се гарантира сигурността на мрежовите устройства и целия мрежов трафик.

Сигурност, осигурена от NAT устройства

Докато основната цел на NAT устройствата е да позволяват на устройства с частни IP адреси в локална мрежа (LAN) да комуникират с устройства в публични адресни пространства, като например Интернет, NAT устройствата по своята същност осигуряват ниво на сигурност, функциониращи като хардуерни защитни стени, за да се предотврати преминаването на нежелан трафик на данни през рутерите и към LAN мрежите в мрежите от страна на услугата, свързани към рутера.

За да подобрите сигурността в клоновите сайтове, можете да поставите рутера зад NAT устройство. Маршрутизаторът може да взаимодейства с NAT устройства, конфигурирани със следните помощни програми за сесионна траверса за NAT (STUN), както са дефинирани в RFC 5389:

- NAT с пълно конус, NAT или един към един — Този метод картографира вътрешен адрес и двойка портове към външен адрес и порт. Всеки външен хост може да изпраща пакети до LAN устройства зад рутера, като ги адресира до външния адрес и порт.
- NAT-ограничен конус NAT или ограничен конус NAT — Този метод също картографира вътрешен адрес и порт към и външен адрес и порт. Въпреки това, външен хост може да изпраща пакети до вътрешното устройство само ако външният адрес (и всеки порт на този адрес) е получил пакет от вътрешния адрес и порт.
- NAT-ограничен конус NAT - Този метод е по-строга версия на NAT с ограничен конус, в която външен хост може да изпраща пакети до вътрешния адрес и порт само ако външният адрес и двойката порт са получили пакет от този вътрешен адрес и порт , Външното устройство трябва да изпраща пакети от конкретния порт до конкретния вътрешен порт.
- Симетричен NAT — с този метод всяка заявка от един и същ вътрешен IP адрес и порт към външен IP адрес и порт се картографира на уникален IP адрес и порт на външен източник. Ако един и същ вътрешен хост изпрати пакет със същия адрес на източник и порт, но до различна дестинация, NAT устройството създава различно картографиране. Само външен хост, който получава пакет от вътрешен хост, може да изпрати пакет обратно. Рутерите поддържат симетричен NAT само от едната страна на тунела WAN. Тоест само едно от NAT устройствата в двата края на тунела може да използва симетричен NAT. Когато рутер работи зад NAT устройство, работещо със симетричен NAT, само едно от NAT устройствата в двата края на тунела може да използва симетричен NAT. Рутерът, който е зад симетричен NAT, не може да установи BFD тунел с

A1 България ЕАД

отдалечен рутер, който стои зад симетричен NAT, NAT-ограничен NAT или NAT-ограничен NAT. За да позволите на рутер да функционира зад симетричен NAT, трябва да конфигурирате връзките за контрол на vManage и vSmart контролер, за да използвате TLS. DTLS контролните връзки не работят чрез симетричен NAT.

Сигурност за връзки към външни устройства

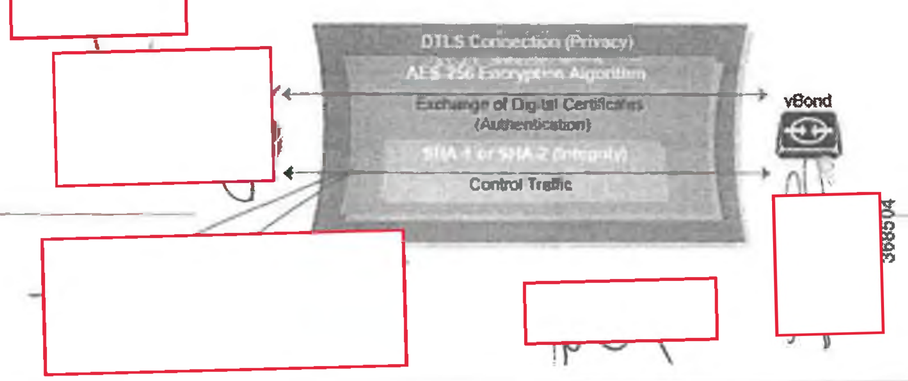
SD-WAN маршрутизаторите на Cisco могат да използват базиран на стандарти протокол за интернет обмен на ключове (IKE) при установяване на IPsec тунели между устройство в мрежата на наслагване и устройство, което е външно към мрежата за наслагване, като например услуга, хоствана в облак или дистанционно потребител. Софтуерът на Cisco SD-WAN поддържа IKE версия 2, която осъществява взаимна идентификация и създава и поддържа асоциации за сигурност (SA). IPsec осигурява конфиденциалност, цялостност на данните, контрол на достъпа и удостоверяване на източника на данни за трафика, който се обменя през тунела IPsec.

Преглед на сигурността на контролната равнина

Контролната равнина на всяка мрежа е свързана с определянето на топологията на мрежата и определянето на начина на насочване на пакетите. В традиционната мрежа операциите на контролната равнина на изграждане и поддържане на маршрутизационни и пренасочващи таблици и насочване на пакети към тяхното местоназначение се обработват чрез маршрутизиране и превключване на протоколи, които обикновено предлагат малко или никакви механизми за удостоверяване на устройства или за криптиране на актуализации за маршрутизация и друга информация за контрол. Освен това традиционните методи за осигуряване на сигурност са силно ръчни и не мащабират. Като примери, сертификатите обикновено се инсталират ръчно, а не по автоматизиран начин и използването на предварително зададени клавиши не е много сигурен подход за осигуряване на сигурност на устройството.

Контролната равнина на Cisco SD-WAN е проектирана с цел защита на мрежата и устройствата. Основата на контролната равнина е един от два протокола за сигурност, извлечени от SSL (Secure Sockets Layer) — протоколът за сигурност на транспортния слой на дейтаграмата (DTLS) и протоколът за сигурност на транспортния слой (TLS). В vSmart контролер, който е централизирана мозъка на Cisco SD-WAN решения, създава и поддържа DTLS или TLS връзки до всички Cisco SD-Уан устройства в мрежата за наслагване: към маршрутизаторите, оркестраторите vBond , към Cisco vManage и към други контролери vSmart . Тези връзки носят трафик на контролната равнина. DTLS или TLS осигурява поверителност на комуникацията между устройствата на Cisco SD-WAN в мрежата, използвайки алгоритъма за криптиране на Advanced Encryption Standard (AES-256) за криптиране на целия контролен трафик, изпратен през връзките.

Поверителността и криптирането в контролната равнина, предлагани от DTLS и TLS, осигуряват сигурна и сигурна основа за другите два компонента за сигурност, автентичност и цялост. За да извършат удостоверяване, Cisco SD-WAN устройствата обменят цифрови сертификати. Тези сертификати, които са инсталирани или от софтуера, или твърдо кодирани в хардуера, в зависимост от устройството, идентифицират устройството и позволяват на самите устройства автоматично да определят кои от тях принадлежат в мрежата и кои са импозанти. За цялост DTLS или TLS връзките изпълняват AES-256-GCM, криптографски защитен хеш алгоритъм, който гарантира, че целият контрол и трафикът на данни, изпратен през връзките, не е бил подправен.



По-долу са компонентите за сигурност на контролната равнина, които функционират в поверителността, осигурена от DTLS или TLS връзки:

- Алгоритъмът **AES-256-GCM** предоставя услуги за криптиране.
- **Цифровите сертификати** се използват за удостоверяване.
- **AES-256-GCM** е отговорен за гарантирането на целостта.

DTLS и TLS инфраструктура

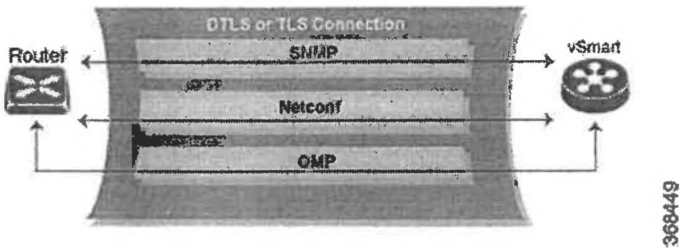
Протоколите за сигурност, получени от SSL, осигуряват основата за инфраструктурата на контролната равнина на Cisco SD-WAN.

Първият е протоколът DTLS , който е протокол за поверителност на транспорта за протоколи без връзка с дейтаграми, като UDP , осигурява основата за инфраструктурата на равнината за управление на Cisco SD-WAN. Той се базира на протоколно-ориентирания протокол за защита на транспортния слой (TLS), който осигурява сигурност за TCP-базиран трафик. (Самият TLS е еволюирал от SSL.) Дизайнът на инфраструктурата на Cisco SD-WAN използва DTLS, изпълняващ UDP, за да избегне някои проблеми с TCP, включително закъсненията, свързани с поточните протоколи и някои проблеми със сигурността. Въпреки това, тъй като UDP не извършва ръкостискане и не изпраща потвърждения, DTLS трябва да се справя с възможно пренареждане на пакети, загуба на дейтаграми и данни, по-големи от размера на пакета с дейтаграми.

Инфраструктурата на контролната равнина също може да бъде конфигурирана да работи над TLS. Това може да е желателно в ситуации, когато защитата на TCP превишава проблемите му. Например, защитните стени обикновено предлагат по-добра защита за TCP сървърите, отколкото за UDP сървърите.

Софтуерът Cisco SD-WAN реализира стандартната версия на DTLS с UDP , която е дефинирана в RFC 6347. DTLS за използване с други протоколи е дефиниран в редица други RFC. За TLS софтуерът Cisco SD-WAN реализира стандартната версия, дефинирана в RFC 5246.

В архитектурата на Cisco SD-WAN, Cisco SD-WAN устройствата използват DTLS или TLS като протокол за тунелиране, който е протокол за тунелиране на ниво приложение (Layer 4). Когато vSmart контролери, vBond Оркестратори, Cisco vManages и рутери се включат в мрежата, те създават временни DTLS или TLS тунели между тях, като част от процеса на удостоверяване на устройството. След като процесът на удостоверяване приключи успешно, временните тунели между маршрутизаторите и контролерите vSmart и тези между vBond оркестраторите и vSmart контролерите стават постоянни и продължават да работят, докато устройствата са активни в мрежата. Именно тези удостоверени, защитени DTLS или TLS тунели се използват от всички приложения за протоколи, работещи на устройствата на Cisco SD-WAN, за да транспортират трафика си. Например OMP сесия на рутер комуникира с OMP сесия на vSmart контролер, като изпраща обикновен IP трафик през защитения DTLS или TLS тунел между двете устройства. Протоколът за управление на Overlay е протоколът за управление на Cisco SD-WAN, използван за обмен на маршрутизация, политика и информация за управление между устройствата на Cisco SD-WAN, както е описано в Общ преглед на маршрутизиране на Overlay.



Демон на Cisco SD-WAN, работещ на всеки vSmart контролер и рутер, създава и поддържа защитените DTLS или TLS връзки между устройствата. Този демон се нарича vdaemon и е разгледан по-нататък в тази статия. След установяване на DTLS или TLS на контролната равнина между тези устройства, множество протоколи могат да създават сесии за стартиране и маршрутизиране на трафика им през тези връзки - включително OMP , Simple Network Management Protocol (SNMP) и протокол за конфигуриране на мрежата (Netconf) - без да се нуждаят да се занимава с въпроси, свързани със сигурността. Трафикът, свързан със сесията, е просто насочен през защитената връзка между рутерите и контролерите vSmart .

Удостоверяване на контролната равнина

Контролната равнина на Cisco SD-WAN използва цифрови сертификати с 2048-битови RSA ключове за удостоверяване на маршрутизаторите на Cisco SD-WAN в мрежата. Цифровите сертификати се създават, управляват и обменят от стандартни компоненти на инфраструктурата на публичния ключ (PKI):

- **Публични ключове** — Тези ключове са общоизвестни.
- **Частни ключове** — Тези клавиши са частни. Те пребивават на всеки Cisco SD-WAN рутер и не могат да бъдат изтеглени от рутера.
- **Сертификати**, подписани от орган за сертифициране на корен (CA) — веригата на доверие, свързана с root CA, трябва да присъства на всички маршрутизатори на Cisco SD-WAN.

В допълнение към стандартните PKI компоненти, в процесите на удостоверяване се използват серийните номера на маршрутизатора на Cisco SD-WAN и номерата на шасито на рутера.

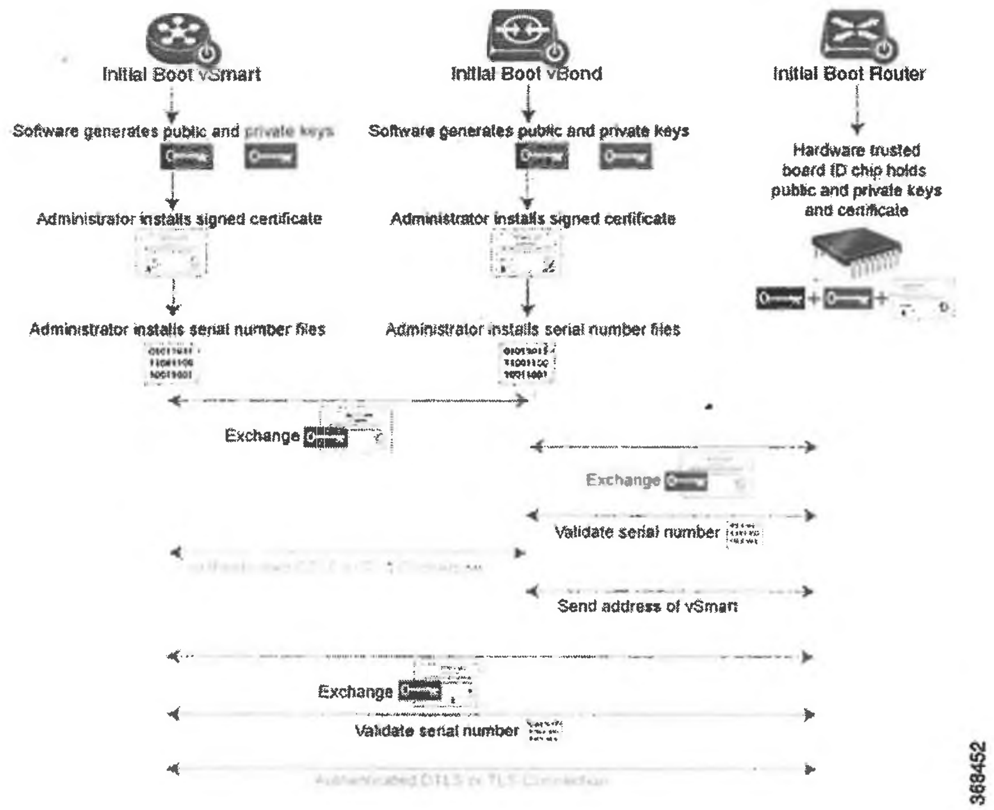
Нека първо разгледаме PKI компонентите, които участват в удостоверяването на рутера.
На маршрутизаторите vEdge 100, 1000 и 2000 публичните и частните ключове и сертификатите се управляват автоматично от чип на Trusted Board ID, който е вграден в рутера. За vEdge 5000 вместо чип на Trusted Board ID се използва модул на доверената платформа (TPM). Когато рутерите са произведени, този чип се програмира с подписан сертификат. Този сертификат включва публичния ключ на рутера, неговия сериен номер и частния ключ на рутера. Когато маршрутизаторите се зареждат и се присъединят към мрежата, те обменят своите сертификати (включително публичния ключ и сериен номер на рутера) с други маршрутизатори на Cisco SD-WAN като част от процеса на автентификация на рутера. Обърнете внимание, че личният ключ на рутера винаги остава вграден в чипа на рутера и той никога не се разпространява, нито може да бъде извлечен от рутера. Всъщност всеки опит за груба сила да прочете частния ключ причинява неуспех на чипа, като по този начин деактивира целия достъп до рутера.

За vSmart контролери, vBond Оркестратори и Cisco vManage системи, публичните и частните ключове и сертификатите се управляват ръчно. Когато стартирате тези рутери за първи път, софтуерът Cisco SD-WAN генерира уникален двойка частен ключ - публичен ключ за всяко изображение на софтуера. Публичният ключ трябва да бъде подписан от root root. Системният администратор след това поиска подписан сертификат и ръчно да го и веригите удостоверение за инсталира vSmart контролери, vBond Оркестратори и Cisco vManage системи. Типичната мрежа може да има само малка шепа vSmart контролери, vBond оркестратори и Cisco vManage, така че тежестта от ръчно управление на ключовете и сертификатите на тези рутери е малка.

За да увеличи тези стандартни PKI компоненти, софтуерът Cisco SD-WAN използва серийните номера на рутера при извършване на автоматично удостоверяване на рутера. По-конкретно, той използва серийните номера на рутера и vSmart и номерата на шасито на рутера. Когато се изпрати партида рутери, производителят изпраща текстов файл, в който са изброени серийните номера на рутерите и съответните номера на шасито. За контролерите на vSmart , когато администраторът на мрежата получи подписания сертификат, те трябва да извлекат серийните номера от сертификатите и да ги поставят в един текстов файл, по един сериен номер на ред. Тогава мрежовият администратор инсталира ръчно тези два файла. Файлът, получен от производителя, който изброява всички валидни серийни номера на рутера и ходовата част, се качва и инсталира на vSmart контролери. Както упълномощеният файл със сериен номер, така и файлът, в който са изброени серийните номера на vSmart, се качват и инсталират на оркестри на vBond . След това, по време на процеса на автоматично удостоверяване, когато двойки устройства (рутери и контролери) установяват DTLS контролни връзки, всяко устройство сравнява серийните номера (а за рутери - номерата на шасито) с тези във файловете, инсталирани на рутера. Рутерът позволява да се установи връзка само ако серийният номер или комбинацията от сериен номер на шасито (за рутер) съвпадат.

Можете да покажете инсталиран vSmart упълномощен серийни номера с помощта на **показване на контрол валиден — vsmarts** командването на vSmart контролер или рутер и **показване на оркестратор валиден- vsmarts** заповядам на vBond артист-оркестрант. Можете също така да стартирате **show sdwan control valid- vsmarts** на устройства Cisco IOS XE SD-WAN. Можете да покажете инсталираните маршрутизатори, оторизирани серийни и номера на шаси, като използвате командата **показване на контрол валидни- vedges** на контролер vSmart и командата **показване на оркестратор валидни — устройства** на vBond оркестратор

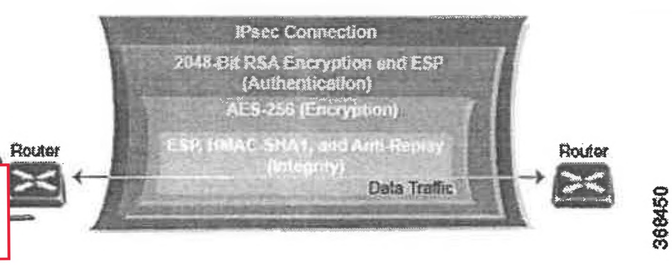
Сега, нека да разгледаме как компонентите за удостоверяване на PKI и серийните номера на рутера и номера на ходовата част се използват за удостоверяване на рутер в мрежата на Cisco SD-WAN overlay. Когато vSmart контролерите, vBond оркестраторите и рутерите първо се зареждат, те установяват защитени DTLS или TLS връзки между vSmart контролерите и рутерите. Чрез тези връзки устройствата се удостоверяват взаимно, като използват публичните и частните ключове, подписаните сертификати и сериалните номера на рутерите и извършват серия операции за ръкостискане, за да гарантират, че всички устройства в мрежата са валидни и не са импозатори. Следващата фигура илюстрира размяната на ключове и сертификати, които се случват, когато устройствата на Cisco SD-WAN се зареждат. За подробности относно установяване на истинността, която се проявява по време на bringup процеса, вижте Bringup последователност от събития.



Шифроване на контролната равнина

Криптирането на контролната равнина се извършва или от DTLS , който се основава на протокола TLS, или TLS. Тези протоколи криптират трафика на контролната равнина, който се изпраща през връзките между устройствата на Cisco SD-WAN, за да се потвърди целостта на данните. TLS използва асиметрична криптография за автентификация на обмена на ключове, симетрично криптиране за конфиденциалност и идентификационни кодове за съобщения за целостта на съобщението.

Едно устройство на Cisco SD-WAN може да има DTLS или TLS връзки към множество устройства на Cisco SD-WAN, така че vdaemon създава маршрут на ядрото за всяка дестинация. Например, рутер обикновено има един маршрут на ядрото и следователно една DTLS или TLS връзка за всеки vSmart контролер. По същия начин, vSmart контролерът ще има един маршрут на ядрото и една DTLS или TLS връзка за всеки рутер в своята област.



Цялостност на контролната равнина

Дизайнът на Cisco SD-WAN реализира целостта на контролната равнина, като комбинира два защитни елемента: SHA-1 или SHA-2 дайджести на съобщения и публични и частни ключове.

SHA-1 и SHA-2 са криптографски хеш функции, които генерират дайджести на съобщения (понякога наричани просто дайджести) за всеки пакет, изпратен през връзка на контролна равнина. SHA-1 генерира 160-битов дайджест на съобщения.
SHA-2 е фамилия, която се състои от шест хеш функции с дайджести, които са 224, 256, 384 или 512 бита. След това приемникът генерира дайджест за пакета и ако двата съвпадат, пакетът се приема като валиден. Както SHA-1, така и SHA-2 позволяват да се провери дали съдържанието на пакета не е било подправено.

Вторият компонент на целостта на контролната равнина е използването на публични и частни ключове. Когато се установява връзка за контролна равнина, локално устройство на Cisco SD-WAN изпраща предизвикателство към отдалечено устройство. Отдалеченото устройство криптира предизвикателството, като го подпише със своя частен ключ и връща подписаното предизвикателство на локалното устройство. Тогава локалното устройство използва публичния ключ на отдалеченото устройство, за да провери дали полученото предизвикателство съответства на изпратеното предизвикателство.

След това, след като връзката на контролната равнина е включена, ключовете се използват, за да се гарантира, че пакетите са изпратени от надежден хост и не са поставени по средата от ненадежден източник. Автентичността на всеки пакет се проверява чрез криптиране и декриптиране със симетрични ключове, които се обменят по време на процеса на установяване на контролната връзка.

Преглед на защитата на равнината на данни

Плоскостта на данни на всяка мрежа е отговорна за обработката на пакети данни, които се транспортират през мрежата. (Плоскостта на данни понякога се нарича самолет за пренасочване.) В традиционната мрежа пакетите с данни обикновено се изпращат директно през Интернет или друг тип обществен IP облак или могат да бъдат изпращани през MPLS тунели. Ако маршрутизаторите в мрежата за наслагване на Cisco SD-WAN трябваше да изпращат трафик през публичен IP облак, предаването ще бъде несигурно. Всеки би могъл да подуши трафика и би било лесно да се изпълняват различни видове атаки, включително атаки човек в средата (MITM).

Основата на сигурността в равнината на данни на Cisco SD-WAN е сигурността на контролната равнина. Тъй като контролната равнина е защитена - всички устройства са валидирани и трафикът на контрола е криптиран и не може да бъде подправен - можем да бъдем уверени в използването на маршрути и друга информация, научена от контролната равнина за създаване и поддържане на сигурни пътища за данни в мрежа от рутери.

Плоскостта за данни осигурява инфраструктурата за изпращане на трафик на данни между рутерите в мрежата за наслагване на Cisco SD-WAN. Трафикът на информационния самолет пътува в рамките на сигурни връзки към Интернет сигурност (IPsec). Планината за данни на Cisco SD-WAN реализира ключовите компоненти за защита на автентификацията, криптирането и целостта по следните начини:

- Удостоверяване - Както бе споменато по-горе, контролната равнина на Cisco SD-WAN допринася за основната инфраструктура за сигурност на равнината на данни. Освен това удостоверяването се налага от два други механизма:
    - В традиционния модел за обмен на ключове , vSmarts изпраща кодове за криптиране на IPsec на всяко крайно устройство.

В модела с двойни ключове vSmart изпраща обществени стойности на Diffie-Hellman към крайните устройства и те генерират двойни кодове за криптиране на IPsec, използвайки ECDH и P-384 крива. За повече информация вж. Pairwise ключове.

- По подразбиране IPsec тунелни връзки използват модифицирана версия на протокола Encapsulating Security Payload (ESP) за удостоверяване на IPsec тунели.

- **Криптиране** — Модифицирана версия на ESP защитава полезния товар на пакета данни. Тази версия на протокола проверява и външните IP и UDP заглавия. Следователно тази опция поддържа проверка на целостта на пакета, подобен на протокола за удостоверяване на аутентификация (AH). Шифроването на данни се извършва с помощта на AES-GCM-256 шифър.
- **Цялостност** — За да гарантира, че трафикът на данни се предава през мрежата, без да бъде подправян, информационната равнина реализира няколко механизма от пакета протоколи за защита на IPsec:
  - Модифицирана версия на протокола ESP капсулира полезния товар от пакети данни.
  - Модифицираната версия на ESP използва механизъм, подобен на AH, за да провери целостта на външните IP и UDP заглавки. Можете да конфигурирате методите за цялостност, поддържани на всеки рутер, и тази информация се обменя в TLOC свойствата на рутера. Ако двама връстници рекламират различни типове удостоверяване, те договарят типа, който да използват, като избират най-силния метод.
  - Схемата за повторно възпроизвеждане защитава от атаки, при които нападателят дублира криптирани пакети.

Удостоверяване и криптиране на равнината на данни

По време на въвеждането на наслагването, Cisco vSmart Controller установява информацията за крайните рутери за изпращане на данни един към друг. Въпреки това преди двойка рутери да могат да обменят трафик на данни, те установяват IPsec връзка между тях, която те използват като защитен канал за комуникация. Тъй като Cisco vSmart Controller е удостоверил устройствата, устройствата не се удостоверяват допълнително.

Комуникациите на контролната равнина позволиха на крайното устройство да има достатъчно информация за установяване на IPsec тунели. Крайните устройства просто изпращат данни през тунелите. Няма стъпка за удостоверяване.

В традиционна IPsec среда обменът на ключове се обработва от протокола за обмен на ключове в Интернет (IKE). IKE първо настройва защитени комуникационни канали между устройства и след това установява асоциации за сигурност (SA) между всяка двойка устройства, които искат да обменят данни. IKE използва алгоритъм за обмен на ключове Diffie-Hellman, за да генерира споделен ключ, който криптира по-нататъшната IKE комуникация. За да установите СА , всяко устройство (n) обменя ключовете с всяко друго устройство в мрежата и създава ключове за двойки, генерирайки уникален ключ за всяко отдалечено устройство. Тази схема означава, че в напълно мрежова мрежа всяко устройство трябва да управлява n2 обмен на клавиши и (n-1) ключове. Например, в 1000-възлова мрежа са необходими 1 000 000 обмена на ключове, за да удостоверявайте устройствата и всеки възел е отговорен за поддържането и управлението на 999 ключове.

Дискусията в предишния параграф посочва защо обменът на ключове в стил IKE не се разширява, тъй като размерът на мрежата се увеличава и защо IKE може да бъде тясно място при стартиране и поддържане на обмен на данни в голяма мрежа:

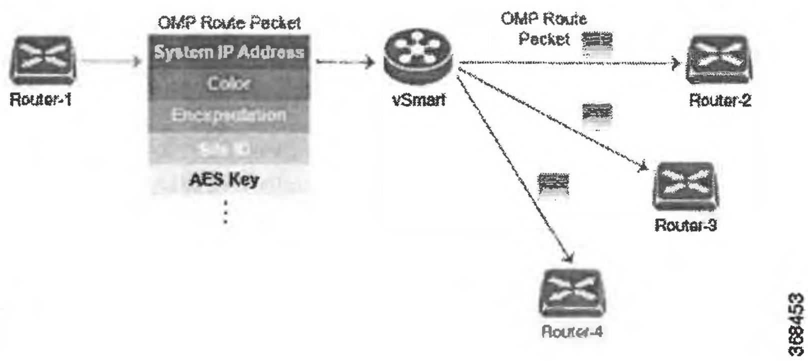
- Ръкостискането, необходимо за настройка на комуникационните канали, отнема време и изисква много ресурси.
- Обработката, необходима за обмена на ключове, особено в по-големите мрежи, може да напряга мрежовите ресурси и да отнеме много време.

Реализацията на Cisco SD-WAN за автентификация и криптиране на равнината на данни установява SAs между всяка двойка устройства, които искат да обменят данни, но изобщо не разполага с IKE. Вместо това, за да предостави мащабируемо решение за обмен на ключове от равнината на данни, решението Cisco SD-WAN се възползва от факта, че връзките на контролната равнина DTLS в мрежата за наслагване на Cisco SD-WAN са сигурни. Тъй като контролната равнина на Cisco SD-WAN установява автентифицирани, криптирани и непробивни връзки, няма нужда в равнината с данни да се настройват сигурни комуникационни канали за извършване на автентификация на равнината на данни.

В мрежата на Cisco SD-WAN за unicast трафик криптирането на данни се извършва от AES-256-GCM, алгоритъм на симетричен ключ, който използва същия ключ за криптиране на изходящите пакети и за декриптиране на входящите пакети. Всеки рутер периодично генерира AES ключ за своя път на данни (по-специално един ключ на TLOC) и предава този ключ на контролера vSmart в пакетите на маршрутите на OMP , които са подобни на актуализациите на маршрута на IP. Тези пакети съдържат информация, която контролерът vSmart използва за определяне на мрежовата топология, включително TLOC на рутера (пакет от системния IP адрес и цвят на трафика) и AES ключ. След това контролерът vSmart поставя тези OMP маршрутни пакети в реклами за достъпност, които изпраща на другите рутери в мрежата. По този начин клавишите AES за всички рутери се разпределят в мрежата. Въпреки че обменът на ключове е симетричен, рутерите го използват по асиметричен начин. Резултатът е прост и мащабируем процес на обмен на ключове, който използва контролера Cisco vSmart .

В Cisco SD-WAN Release 19.2.x и Cisco IOS XE SD-WAN Release 16.12.x нататък, Cisco SD-WAN поддържа IPSec двойни клавиши, които осигуряват допълнителна сигурност. Когато се използват двойни клавиши IPSec, ръбният рутер генерира публични и частни компоненти на Diffie-Hellman и изпраща публичната стойност към vSmart за разпространение към всички други крайни устройства. За повече информация вж. Общ преглед на клавиши IPSec

За многоадресен трафик криптирането на равнината на данни се извършва от AES-256-CBC с SHA1-HMAC.



Ако политиките за управление, конфигурирани на vSmart контролер, ограничават комуникационните канали между мрежовите устройства, рекламите за достъпност, изпратени от vSmart контролера, съдържат информация само за рутерите, с които им е разрешено да обменят данни. Така че, рутер научава ключовете само за онези рутери, с които им е позволено да комуникират.

За допълнително укрепване на автентичността и криптирането на равнината на данни, маршрутизаторите регенерират агресивно своите ключове AES (по подразбиране на всеки 24 часа). Също така, механизмът за регенериране на ключове гарантира, че не се изпуска трафик на данни при смяна на клавишите.

В мрежата за наслагване на Cisco SD-WAN, жизнеността на SA между връстници на рутери се проследява чрез наблюдение на BFD пакетите, които периодично се обменят по IPsec връзката между връстниците. IPsec предава състоянието на връзката към контролерите vSmart . Ако връзката между данни между двама връстници е загубена, обменът на BFD пакети спира и от това контролерът vSmart научава, че връзката е загубена.

Софтуерът IPsec няма изрично изчакване на празен ход на SA, което указва времето за изчакване преди изтриването на SA, свързани с неактивни връзки. Вместо това SA остава активен, докато IPsec връзката между две маршрутизаторите са нагоре, както се определя от периодичния обмен на BFD пакети между тях. Също така честотата, с която се регенерират SA клавишите, отменя необходимостта от внедряване на имплицитна SA време на празен ход.

В обобщение, удостоверяването на самолета за данни на Cisco SD-WAN предлага следните подобрения спрямо IKE:

- Тъй като са необходими само n +1 ключови пътища, а не n^2, изисквани от IKE, решението на Cisco SD-WAN се разширява по-добре с увеличаване на мрежата.
- Ключовете се генерират и освежават локално, а обменът на ключове се извършва през сигурна контролна равнина.

Цялостност на равнината на данни

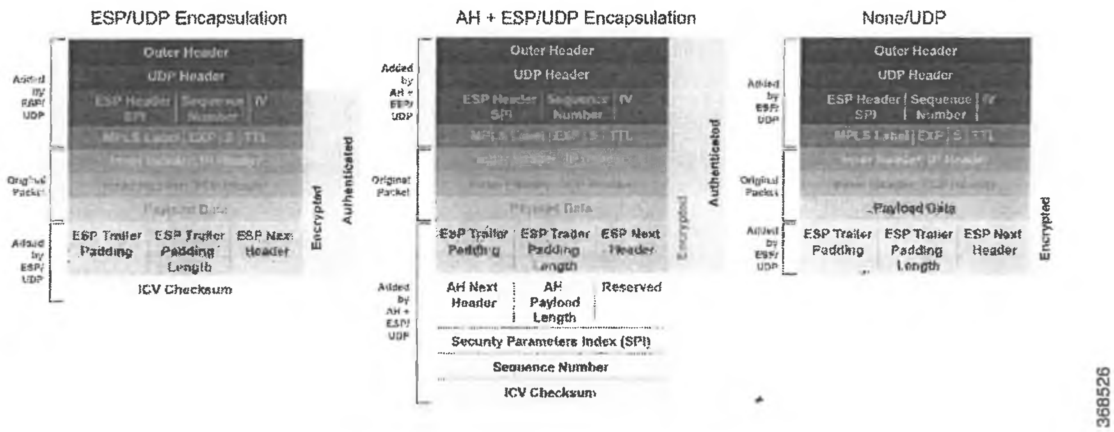
Следните компоненти допринасят за целостта на пакетите с данни в равнината на данни на Cisco SD-WAN:

- ESP, който е стандартен протокол за криптиране на IPsec, защитава (чрез криптиране и удостоверяване) вътрешната заглавна част, полезния товар на пакета данни и трейлъра на ESP във всички пакети данни. Модификациите на ESP също защитават външните IP и UDP заглавки
- Промени в ESP, които защитават (чрез удостоверяване) външните IP и UDP заглавки. Това имитира функционалността на AH протокола.
- Анти-повторното възпроизвеждане, което също е част от стандартния софтуерен пакет IPsec, осигурява механизъм за номериране на всички пакети данни и за да се гарантира, че получаващи рутери приемат само пакети с уникални номера.

Първият от тези компоненти, ESP, е стандартният протокол за криптиране на IPsec. ESP защитава полезния товар на пакета данни и неговите вътрешни IP заглавни полета както чрез криптиране, което става автоматично, така и чрез удостоверяване. За удостоверяване ESP извършва изчисляване на контролна сума върху полезния товар и вътрешния поле на заглавката на пакета от данни и поставя резултиращия хеш (наричан също дайджест) в 12-байтово HMAC-SHA1 поле в края на пакета. (Хешът е еднопосочна компресия.) Приемното устройство изпълнява същата контролна сума и сравнява изчисления си хеш с този в пакета. Ако двете контролни суми съвпадат, пакетът се приема. В противен случай се изпуска. На фигурата по-долу левият стек илюстрира капсулирането на ESP/UDP . ESP криптира и удостоверява вътрешните заглавки, полезния товар, етикета MPLS (ако има такъв) и полетата на трейлъра на ESP, поставяйки HMAC-SHA1 хеш в полето за контролна сума ICV в края на пакета. Външните полета на заглавия, добавени от ESP/UDP , не са нито кодирани, нито удостоверени.

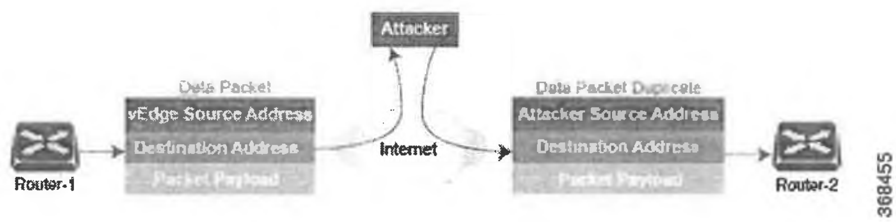
Втори компонент, който допринася за целостта на пакетите данни, са модификациите на ESP за имитиране на AH. Тази модификация изпълнява контролна сума, която включва изчисляване на контролната сума върху всички полета в пакета - полезния товар, вътрешното заглавие, както и всички не-изменяеми полета във външната IP заглавка. AH поставя резултиращия HHAC-SHA1 хеш в последното поле на пакета. Приемащото устройство изпълнява същата контролна сума и приема пакети, чиито контролни суми съвпадат. На фигурата по-долу централният стек илюстрира капсулирането, извършено от модифицираната версия на ESP. ESP отново криптира вътрешните заглавки, полезния товар, етикета MPLS (ако има такъв) и полетата на трейлъра на ESP и сега имитира AH чрез удостоверяване на целия пакет - външните IP и UDP заглавки, заглавката на ESP етикета MPLS (ако има), оригиналния пакет и трейлъра на ESP - и поставя изчислени си хеш HMAC-SHA1 в полето за проверка на ICV в края на пакета.

За ситуации, в които не се изисква удостоверяване на пакети данни, можете да деактивирате напълно удостоверяването на пакети данни. В този случай пакетите с данни се обработват само от ESP, който криптира оригиналния пакет, MPLS етикета (ако има такъв) и трейлъра на ESP. Тази схема е илюстрирана в десния стек на фигурата по-долу.

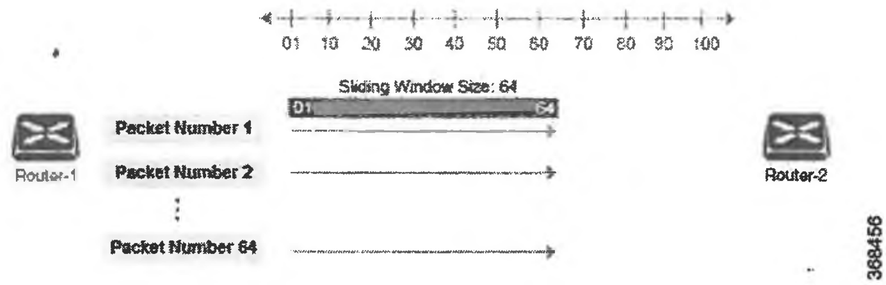


Обърнете внимание, че устройствата на Cisco SD-WAN обменят не само ключа за криптиране (който е симетричен), но и ключа за автентификация, който се използва за генериране на дайджест HMAC-SHA1. И двете се разпространяват като част от свойствата на TLOC за рутер.

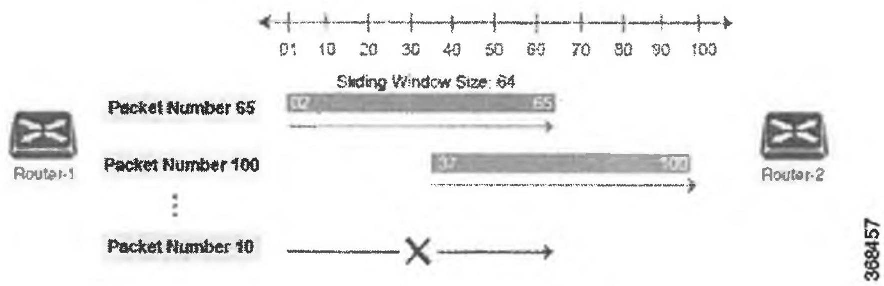
Въпреки че IPsec връзките, над които се обменя трафик на данни, са защитени, те често пътуват през обществено мрежово пространство, като например Интернет, където е възможно хакер да извърши атака при повторно изпълнение (наричана още човек-в-the- средна или MITM , атака) срещу IPsec връзката. При този тип атака противник атакува трафика на данни, като вмъква копие на съобщение, което преди това е изпратено от източника. Ако дестинацията не може да различи възпроизведеното съобщение от валидно съобщение, то може да удостовери противника като източник или може неправилно да предостави на противника неоторизиран достъп до ресурси или услуги.



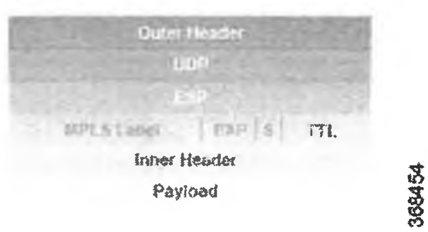
Като противодействие на подобни атаки, мрежовият софтуер на Cisco SD-WAN реализира IPsec протокола за повторно възпроизвеждане. Този протокол се състои от два компонента, които и двата защитават целостта на потока от данни. Първият компонент е да се свържат поредни номера с всеки пакет данни. Подателят вмъква пореден номер във всеки IPsec пакет, а дестинацията проверява поредния номер, приемайки само пакети с уникални, не дублиращи серийни номера. Вторият компонент е плъзгащ се прозорец, който определя диапазон от последователни числа, които са актуални. Плъзгащият се прозорец има фиксирана дължина. Дестинацията приема само пакети, чиито поредни номера попадат в текущия диапазон от стойности в плъзгащия се прозорец, а той изпуска всички останали. Използва се плъзгащ се прозорец, вместо да се приемат само пакети, чийто пореден номер е по-голям от последния известен пореден номер, тъй като често пакетите не пристигат в ред.



Когато дестинацията получи пакет, чийто пореден номер е по-голям от най-голямото число в плъзгащия се прозорец, той плъзга прозореца вдясно, като по този начин променя обхвата на валидни номера на последователности, които ще приеме. Тази схема предпазва от тип атака от тип MITM, тъй като, като изберете правилния размер на прозореца, можете да гарантирате, че ако дублиращ пакет е поставен в потока на трафик, неговият пореден номер ще бъде или в текущия диапазон, но ще бъде дубликат, или тя ще бъде по-малка от най-ниската стойност на тока на плъзгащия се прозорец. Така или иначе дестинацията ще изпусне дублиращия пакет. И така, номерирането на последователности в комбинация с плъзгащ се прозорец осигурява защита срещу атаки от типа MITM и гарантира целостта на потока от данни, протичащ в IPsec връзката.



Пренасяне на VPN информация в пакети с данни

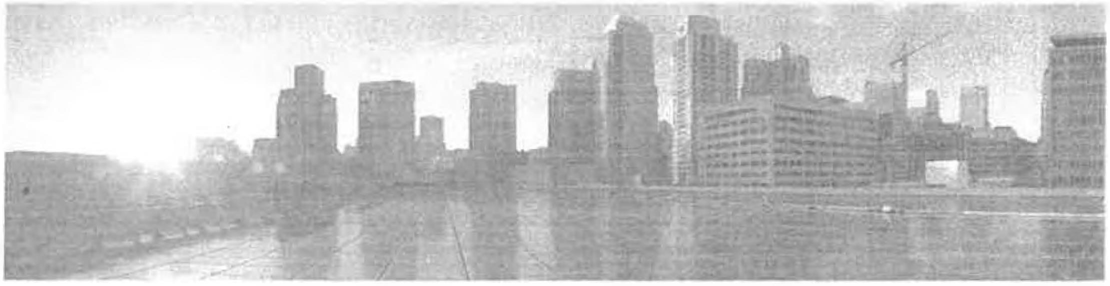


За широкоекранни VPN устройства Cisco SD-WAN устройства поддържат MPLS разширения до пакети данни, които се транспортират в IPsec връзки. Фигурата вдясно показва местоположението на MPLS информацията в заглавката на пакета данни. Тези разширения осигуряват сигурността на мрежовата сегментация (тоест за VPN-ите), която е необходима за поддържане на мулти-наемане в клон или сегментиране в кампус. Изпълнението на Cisco SD-WAN използва IPsec UDP базирани наслагване мрежа капсулиране протокол слой, както е определено в RFC 4023. Сигурността се осигурява чрез включване на вектора на инициализация (IV) в началото на данните за полезния товар в заглавката на ESP. IV стойността се изчислява от AES-256 шифър блок верига (CBC).

Аз, долуподписаният, Явор Стоянов Профиров, удостоверявам верността на направения от мен превод от английски на български език на приложения документ. Преводът се състои от 14 (четиринадесет) страници

Преводач: *Явор Стоянов Профиров*

A1 България ЕАД
СОФИЯ
КП 2



Security Overview

Security is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their network against attacks and breaches. As a result of hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing. There are multiple problems with the traditional ways of securing networks, including:

- Very little emphasis is placed on ensuring the authenticity of the devices involved in the communication.
- Securing the links between a pair of devices involves tedious and manual setup of keys and shared passwords.
- Scalability and high availability solutions are often at odds with each other.

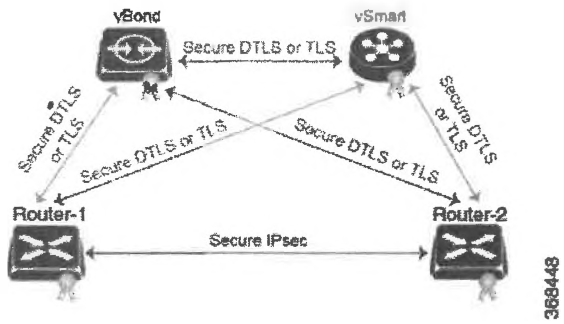
This chapter contains the following topics:

Cisco SD-WAN Security Components

The Cisco SD-WAN solution takes a fundamentally different approach to security, basing its core design around the following precepts:

- Authentication—The solution ensures that only authentic devices are allowed to send traffic to one another.
- Encryption—All communication between each pair of devices is automatically secure, completely eliminating the overhead involved in securing the links.
- Integrity—No group keys or key server issues are involved in securing the infrastructure.

These three components—authentication, encryption, and integrity—are key to securing the Cisco SD-WAN overlay network infrastructure.



The topics on Control Plane Security Overview and Data Plane Security Overview examine how authentication, encryption, and integrity are implemented throughout the Cisco SD-WAN overlay network. The security discussion refers to the following illustration of the components of the Cisco SD-WAN network—the vSmart controller, the vBond orchestrator, and the routers. The connections between these devices form the control plane (in orange) and the data plane (in purple), and it is these connections that need to be protected by appropriate measures to ensure the security of the network devices and all network traffic.

Security Provided by NAT Devices

While the primary purpose of NAT devices is to allow devices with private IP addresses in a local-area network (LAN) to communicate with devices in public address spaces, such as the Internet, NAT devices also inherently provide a level of security, functioning as hardware firewalls to prevent unwanted data traffic from passing through the routers and to the LAN networks in the service-side networks connected to the router.

To enhance the security at branch sites, you can place the router behind a NAT device. The router can interact with NAT devices configured with the following Session Traversal Utilities for NAT (STUN) methods, as defined in RFC 5389 :

- Full-cone NAT, or one-to-one NAT—This method maps an internal address and port pair to an external address and port. Any external host can send packets to LAN devices behind the router by addressing them to the external address and port.
- Address-restricted cone NAT, or restricted-cone NAT—This method also maps an internal address and port to and external address and port. However, an external host can send packets to the internal device only if the external address (and any port at that address) has received a packet from the internal address and port.
- Port-restricted cone NAT—This method is a stricter version of restricted-cone NAT, in which an external host can send packets to the internal address and port only if the external address and port pair has received a packet from that internal address and port. The external device must send packets from the specific port to the specific internal port.
- Symmetric NAT—With this method, each request from the same internal IP address and port to an external IP address and port is mapped to a unique external source IP address and port. If the same internal host sends a packet with the same source address and port but to a different destination, the NAT device creates a different mapping. Only an external host that receives a packet from an internal host can send a packet back. The routers support symmetric NAT only on one side of the WAN tunnel. That is, only one of the NAT devices at either end of the tunnel can use symmetric NAT. When a router operates behind a NAT device running symmetric NAT, only one of the NAT devices at either end of the tunnel can use symmetric NAT. The router that is behind a symmetric NAT cannot establish a BFD tunnel with

a remote router that is behind a symmetric NAT, an address-restricted NAT, or a port-restricted NAT. To allow a router to function behind a symmetric NAT, you must configure the vManage and vSmart controller control connections to use TLS. DTLS control connections do not work through a symmetric NAT.

Security for Connections to External Devices

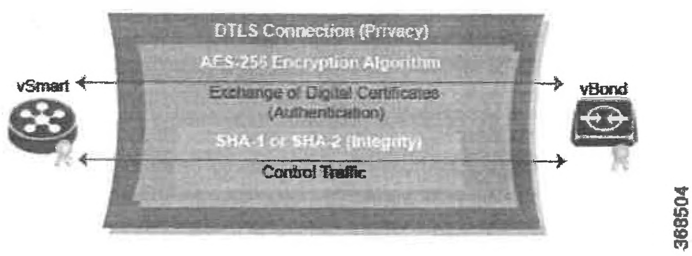
Cisco SD-WAN routers can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote user. The Cisco SD-WAN software supports IKE version 2, which performs mutual authentication and establishes and maintains security associations (SAs). IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

Control Plane Security Overview

The control plane of any network is concerned with determining the network topology and defining how to direct packets. In a traditional network, the control plane operations of building and maintaining routing and forwarding tables and directing packets towards their destination are handled by routing and switching protocols, which typically offer few or no mechanisms for authenticating devices or for encrypting routing updates and other control information. In addition, the traditional methods for providing security are highly manual and do not scale. As examples, certificates are typically installed manually rather than in an automated fashion, and using preshared keys is not a very secure approach for providing device security.

The Cisco SD-WAN control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from SSL (Secure Sockets Layer)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol. The vSmart controller, which is the centralized brain of the Cisco SD-WAN solution, establishes and maintains DTLS or TLS connections to all Cisco SD-WAN devices in the overlay network: to the routers, the vBond orchestrators, to Cisco vManage, and to other vSmart controllers. These connections carry control plane traffic. DTLS or TLS provides communication privacy between Cisco SD-WAN devices in the network, using the Advanced Encryption Standard (AES-256) encryption algorithm to encrypt all control traffic sent over the connections.

The privacy and encryption in the control plane offered by DTLS and TLS provide a safe and secure foundation for the other two security components, authentication and integrity. To perform authentication, the Cisco SD-WAN devices exchange digital certificates. These certificates, which are either installed by the software or hard-coded into the hardware, depending on the device, identify the device and allow the devices themselves to automatically determine which ones belong in the network and which are imposters. For integrity, the DTLS or TLS connections run AES-256-GCM, a cryptographic secure hash algorithm which ensures that all control and data traffic sent over the connections has not been tampered with.



ВЯРНО С ОРИГИНАЛА

The following are the control plane security components, which function in the privacy provided by DTLS or TLS connections:

- **AES-256-GCM** algorithm provides encryption services.
- **Digital certificates** are used for authentication.
- **AES-256-GCM** is responsible for ensuring integrity.

DTLS and TLS Infrastructure

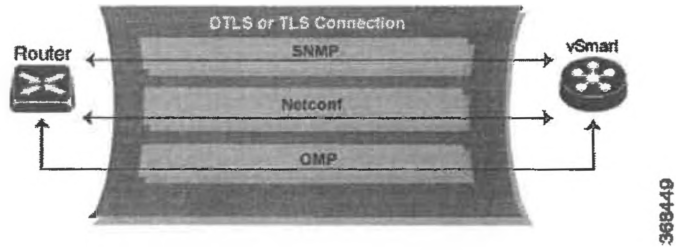
Security protocols derived from SSL provide the foundation for the Cisco SD-WAN control plane infrastructure.

The first is the DTLS protocol, which is a transport privacy protocol for connectionless datagram protocols such as UDP, provides the foundation for the Cisco SD-WAN control plane infrastructure. It is based on the stream-oriented Transport Layer Security (TLS) protocol, which provides security for TCP-based traffic. (TLS itself evolved from SSL.) The Cisco SD-WAN infrastructure design uses DTLS running over UDP to avoid some of the issues with TCP, including the delays associated with stream protocols and some security issues. However, because UDP performs no handshaking and sends no acknowledgments, DTLS has to handle possible packet re-ordering, loss of datagrams, and data larger than the datagram packet size.

The control plane infrastructure can also be configured to run over TLS. This might be desirable in situations where the protections of TCP outweigh its issues. For example, firewalls generally offer better protection for TCP servers than for UDP servers.

The Cisco SD-WAN software implements the standard version of DTLS with UDP, which is defined in RFC 6347 . DTLS for use with other protocols is defined in a number of other RFCs . For TLS, the Cisco SD-WAN software implements the standard version defined in RFC 5246.

In the Cisco SD-WAN architecture, the Cisco SD-WAN devices use DTLS or TLS as a tunneling protocol, which is an application-level (Layer 4) tunneling protocol. When the vSmart controllers, vBond orchestrators, Cisco vManages, and routers join the network, they create provisional DTLS or TLS tunnels between them as part of the device authentication process. After the authentication process completes successfully, the provisional tunnels between the routers and vSmart controllers, and those between the vBond orchestrators and vSmart controllers, become permanent and remain up as long as the devices are active in the network. It is these authenticated, secure DTLS or TLS tunnels that are used by all the protocol applications running on the Cisco SD-WAN devices to transport their traffic. For example, an OMP session on a router communicates with an OMP session on a vSmart controller by sending plain IP traffic through the secure DTLS or TLS tunnel between the two devices. The Overlay Management Protocol is the Cisco SD-WAN control protocol used to exchange routing, policy, and management information among Cisco SD-WAN devices, as described in Overlay Routing Overview.



A Cisco SD-WAN daemon running on each vSmart controller and router creates and maintains the secure DTLS or TLS connections between the devices. This daemon is called vdaemon and is discussed later in this article. After the control plane DTLS or TLS connections are established between these devices, multiple protocols can create sessions to run and route their traffic over these connections—including OMP, Simple Network Management Protocol (SNMP), and Network Configuration Protocol (Netconf)—without needing to be concerned with any security-related issues. The session-related traffic is simply directed over the secure connection between the routers and vSmart controllers.

Control Plane Authentication

The Cisco SD-WAN control plane uses digital certificates with 2048-bit RSA keys to authenticate the Cisco SD-WAN routers in the network. The digital certificates are created, managed, and exchanged by standard components of the public key infrastructure (PKI):

- **Public keys**— These keys are generally known.
- **Private keys**— These keys are private. They reside on each Cisco SD-WAN router and cannot be retrieved from the router.
- **Certificates** signed by a root certification authority (CA)— The trust chain associated with the root CA needs to be present on all Cisco SD-WAN router.

In addition to standard PKI components, the Cisco SD-WAN router serial numbers and the router chassis numbers are used in the authentication processes.

Let's first look at the PKI components that are involved in router authentication. On vEdge 100, 1000, and 2000 routers, the public and private keys and the certificates are managed automatically, by a Trusted Board ID chip that is built into the router. For vEdge 5000, instead of a Trusted Board ID chip, a Trusted Platform Module (TPM) is used. When the routers are manufactured, this chip is programmed with a signed certificate. This certificate includes the router's public key, its serial number, and the router's private key. When the routers boot up and join the network, they exchange their certificates (including the router's public key and serial number) with other Cisco SD-WAN routers as part of the router authentication process. Note that the router's private key always remains embedded in the router's chip, and it is never distributed, nor can it ever be retrieved from the router. In fact, any brute-force attempt to read the private key causes the chip to fail, thereby disabling all access to the router.

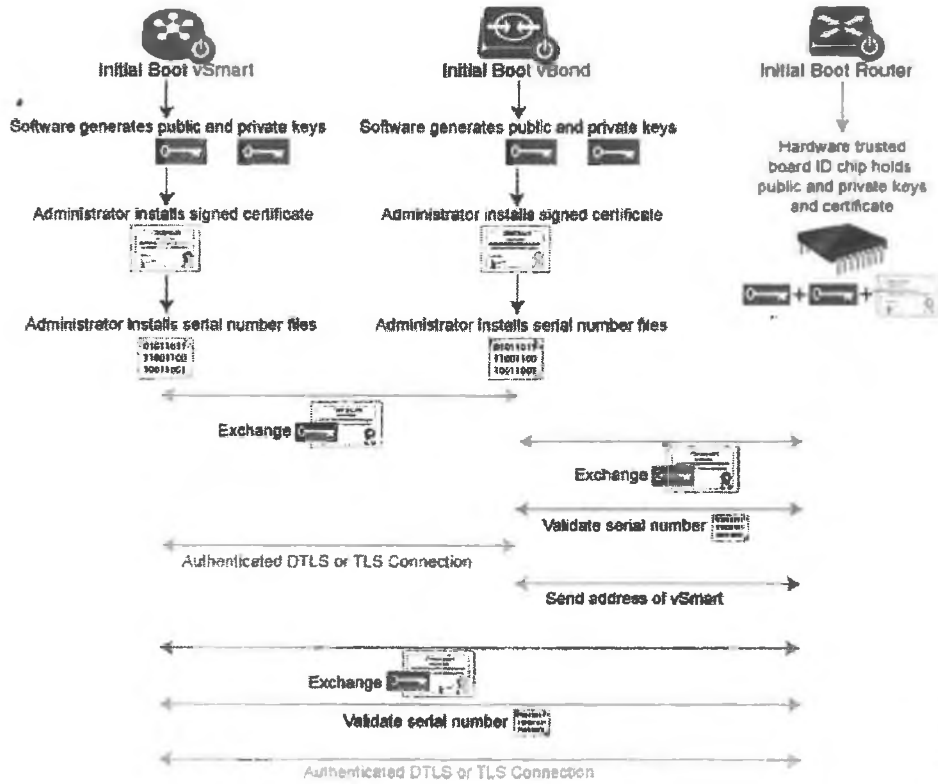
For vSmart controllers, vBond orchestrators, and Cisco vManage systems, the public and private keys and the certificates are managed manually. When you boot these routers for the first time, the Cisco SD-WAN software generates a unique private key–public key pair for each software image. The public key needs to be signed by the CA root. The network administrator then requests a signed certificate and manually installs it and the certificate chains on the vSmart controllers, vBond orchestrators, and Cisco vManage systems. A typical network might have only a small handful of vSmart controllers, vBond orchestrators, and Cisco vManages, so the burden of manually managing the keys and certificates on these routers is small.

ВЯРНО С ОРИГИНАЛА

To augment these standard PKI components, the Cisco SD-WAN software uses the router serial numbers in performing automatic router authentication. Specifically, it uses the router and vSmart serial numbers and the router chassis numbers. When a batch of routers is shipped, the manufacturer sends a text file that lists the serial numbers of the routers and the corresponding chassis numbers. For the vSmart controllers, when the network administrator receives the signed certificate, they should extract the serial numbers from the certificates and place them into a single text file, one serial number per line. Then the network administrator manually installs these two files. The file received from the manufacturer that lists all valid router serial and chassis numbers is uploaded and installed on vSmart controllers. Both the authorized serial number file and the file listing the vSmart serial numbers are uploaded and installed on vBond orchestrators. Then, during the automatic authentication process, as pairs of devices (routers and controllers) are establishing DTLS control connections, each device compares the serial numbers (and for routers, the chassis numbers) to those in the files installed on the router. A router allows a connection to be established only if the serial number or serial–chassis number combination (for a router) matches.

You can display the installed vSmart authorized serial numbers using the **show control valid-vsmarts** command on a vSmart controller or a router and the **show orchestrator valid-vsmarts** command on a vBond orchestrator. You can also run **show sdwan control valid-vsmarts** on Cisco IOS XE SD-WAN devices. You can display the installed router authorized serial and chassis number associations using the **show control valid-vedges** command on a vSmart controller and the **show orchestrator valid-devices** command on a vBond orchestrator

Now, let's look at how the PKI authentication components and the router serial and chassis numbers are used to authenticate router on the Cisco SD-WAN overlay network. When vSmart controllers, vBond orchestrators, and routers first boot up, they establish secure DTLS or TLS connections between the vSmart controllers and the routers. Over these connections, the devices authenticate each other, using the public and private keys, the signed certificates, and the routers serial numbers and performing a series of handshake operations to ensure that all the devices on the network are valid and not imposters. The following figure illustrates the key and certificate exchange that occurs when the Cisco SD-WAN devices boot. For details about the authentication that occurs during the bringup process, see Bringup Sequence of Events.



368452

Control Plane Encryption

Control plane encryption is done by either DTLS, which is based on the TLS protocol, or TLS. These protocol encrypt the control plane traffic that is sent across the connections between Cisco SD-WAN devices to validate the integrity of the data. TLS uses asymmetric cryptography for authenticating key exchange, symmetric encryption for confidentiality, and message authentication codes for message integrity.

A single Cisco SD-WAN device can have DTLS or TLS connections to multiple Cisco SD-WAN devices, so vdaemon creates a kernel route for each destination. For example, a router would typically have one kernel route, and hence one DTLS or TLS connection, for each vSmart controller. Similarly, a vSmart controller would have one kernel route and one DTLS or TLS connection for each router in its domain.

368450

ВЯРНО С ОРИГИНАЛА

A1 България ЕАД

Control Plane Integrity

The Cisco SD-WAN design implements control plane integrity by combining two security elements: SHA-1 or SHA-2 message digests, and public and private keys.

SHA-1 and SHA-2 are cryptographic hash functions that generate message digests (sometimes called simply digests) for each packet sent over a control plane connection. SHA-1 generates a 160-bit message digest. SHA-2 is a family that consists of six hash functions with digests that are 224, 256, 384, or 512 bits. The receiver then generates a digest for the packet, and if the two match, the packet is accepted as valid. Both SHA-1 and SHA-2 allow verification that the packet's contents have not been tampered with.

The second component of control plane integrity is the use of public and private keys. When a control plane connection is being established, a local Cisco SD-WAN device sends a challenge to a remote device. The remote device encrypts the challenge by signing it with its private key, and returns the signed challenge to the local device. The local device then uses the remote device's public key to verify that the received challenge matches the sent challenge.

Then, once a control plane connection is up, keys are used to ensure that packets have been sent by a trusted host and were not inserted midstream by an untrusted source. The authenticity of each packet is verified through encryption and decryption with symmetric keys that were exchanged during the process of establishing the control connection.

Data Plane Security Overview

The data plane of any network is responsible for handling data packets that are transported across the network. (The data plane is also sometimes called the forwarding plane.) In a traditional network, data packets are typically sent directly over the Internet or another type of public IP cloud, or they could be sent through MPLS tunnels. If the routers in the Cisco SD-WAN overlay network were to send traffic over a public IP cloud, the transmission would be insecure. Anyone would be able to sniff the traffic, and it would be easy to implement various types of attacks, including man-in-the-middle (MITM) attacks.

The underlying foundation for security in the Cisco SD-WAN data plane is the security of the control plane. Because the control plane is secure—all devices are validated, and control traffic is encrypted and cannot be tampered with—we can be confident in using routes and other information learned from the control plane to create and maintain secure data paths throughout a network of routers.

The data plane provides the infrastructure for sending data traffic among the routers in the Cisco SD-WAN overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Cisco SD-WAN data plane implements the key security components of authentication, encryption, and integrity in the following ways:

- Authentication—As mentioned above, the Cisco SD-WAN control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:
  - In the traditional key exchange model, the vSmarts sends IPsec encryption keys to each edge device.

In the pairwise keys model, the vSmart sends Diffie-Hellman public values to the edge devices and they generate pairwise IPsec encryption keys using ECDH and a P-384 curve. For more information, see Pairwise Keys.

- By default IPsec tunnel connections use a modified version of the Encapsulating Security Payload (ESP) protocol for authentication on IPsec tunnels.

- **Encryption**—A modified version of ESP protects the data packet's payload. This version of the protocol also checks the outer IP and UDP headers. Hence, this option supports an integrity check of the packet similar to the Authentication Header (AH) protocol. Data encryption is done using the AES-GCM-256 cipher.
- **Integrity**—To guarantee that data traffic is transmitted across the network without being tampered with, the data plane implements several mechanisms from the IPsec security protocol suite:
    - A modified version of the ESP protocol encapsulates the payload of data packets.
    - The modified version of ESP uses an AH-like mechanism to check the integrity of the outer IP and UDP headers. You can configure the integrity methods supported on each router, and this information is exchanged in the router's TLOC properties. If two peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.
    - The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

Data Plane Authentication and Encryption

During the bringup of the overlay, the Cisco vSmart Controller establishes the information for edge routers to send data to each other. However before a pair of routers can exchange data traffic, they establish an IPsec connection between them, which they use as a secure communications channel. Since the Cisco vSmart Controller has authenticated the devices, the devices do not further authenticate each other.

Control plane communications have allowed the edge device to have enough information to establish IPsec tunnels. Edge devices simply send data through the tunnels. There is no authentication step.

In a traditional IPsec environment, key exchange is handled by the Internet Key Exchange (IKE) protocol. IKE first sets up secure communications channels between devices and then establishes security associations (SAs) between each pair of devices that want to exchange data. IKE uses a Diffie-Hellman key exchange algorithm to generate a shared key that encrypts further IKE communication. To establish SAs, each device (n) exchanges keys with every other device in the network and creates per-pair keys, generating a unique key for each remote device. This scheme means that in a fully meshed network, each device has to manage n^2 key exchanges and (n-1) keys. As an example, in a 1,000-node network, 1,000,000 key exchanges are required to authenticate the devices, and each node is responsible for maintaining and managing 999 keys.

The discussion in the previous paragraph points out why an IKE-style key exchange does not scale as network size increases and why IKE could be a bottleneck in starting and in maintaining data exchange on a large network:

- The handshaking required to set up the communications channels is both time consuming and resource intensive.
- The processing required for the key exchange, especially in larger networks, can strain network resources and can take a long time.

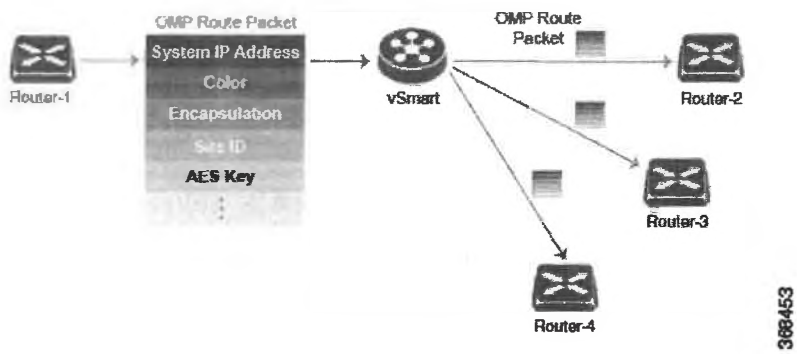
ВЯРНО С ОРИГИНАЛА

The Cisco SD-WAN implementation of data plane authentication and encryption establishes SAs between each pair of devices that want to exchange data, but it dispenses with IKE altogether. Instead, to provide a scalable solution to data plane key exchange, the Cisco SD-WAN solution takes advantage of the fact that the DTLS control plane connections in the Cisco SD-WAN overlay network are known to be secure. Because the Cisco SD-WAN control plane establishes authenticated, encrypted, and tamperproof connections, there is no need in the data plane to set up secure communications channels to perform data plane authentication.

In the Cisco SD-WAN network for unicast traffic, data plane encryption is done by AES-256-GCM, a symmetric-key algorithm that uses the same key to encrypt outgoing packets and to decrypt incoming packets. Each router periodically generates an AES key for its data path (specifically, one key per TLOC) and transmits this key to the vSmart controller in OMP route packets, which are similar to IP route updates. These packets contain information that the vSmart controller uses to determine the network topology, including the router's TLOC (a tuple of the system IP address and traffic color) and AES key. The vSmart controller then places these OMP route packets into reachability advertisements that it sends to the other routers in the network. In this way, the AES keys for all the routers are distributed across the network. Even though the key exchange is symmetric, the routers use it in an asymmetric fashion. The result is a simple and scalable key exchange process that uses the Cisco vSmart Controller.

In Cisco SD-WAN Release 19.2.x and Cisco IOS XE SD-WAN Release 16.12.x onwards, Cisco SD-WAN supports IPSec pairwise keys that provide additional security. When IPSec pairwise keys are used, the edge router generates public and private Diffie-Hellman components and sends the public value to the vSmart for distribution to all other edge devices. For more information, see IPSec Pairwise Keys Overview

For multicast traffic, data plane encryption is done by AES-256-CBC with SHA1-HMAC.



If control policies configured on a vSmart controller limit the communications channels between network devices, the reachability advertisements sent by the vSmart controller contain information only for the routers that they are allowed to exchange data with. So, a router learns the keys only for those routers that they are allowed to communicate with.

To further strengthen data plane authentication and encryption, routers regenerate their AES keys aggressively (by default, every 24 hours). Also, the key regeneration mechanism ensures that no data traffic is dropped when keys change.

In the Cisco SD-WAN overlay network, the liveness of SAs between router peers is tracked by monitoring BFD packets, which are periodically exchanged over the IPsec connection between the peers. IPsec relays the connection status to the vSmart controllers. If data connectivity between two peers is lost, the exchange of BFD packets stops, and from this, the vSmart controller learns that the connection has been lost.

The IPsec software has no explicit SA idle timeout, which specifies the time to wait before deleting SAs associated with inactive peers. Instead, an SA remains active as long as the IPsec connection between two

ВЯРНО С ОРИГИНАЛА

routers is up, as determined by the periodic exchange of BFD packets between them. Also, the frequency with which SA keys are regenerated obviates the need to implement an implicit SA idle timeout.

In summary, the Cisco SD-WAN data plane authentication offers the following improvements over IKE:

- Because only n +1 keypaths are required rather than the n^2 required by IKE, the Cisco SD-WAN solution scales better as the network grows large.
- Keys are generated and refreshed locally, and key exchange is performed over a secure control plane.

Data Plane Integrity

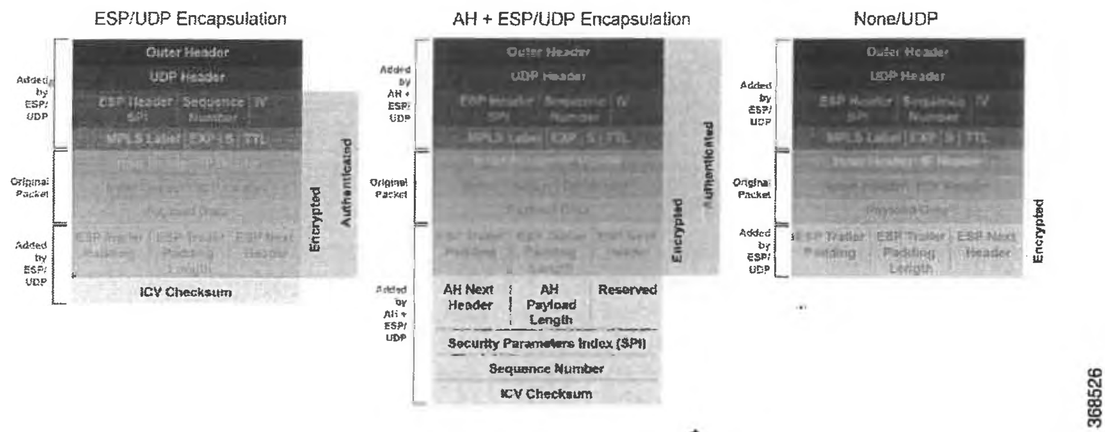
The following components contribute to the integrity of data packets in the Cisco SD-WAN data plane:

- ESP, which is a standard IPsec encryption protocol, protects (via encryption and authentication) the inner header, data packet payload, and ESP trailer in all data packets. The modifications to ESP also protect the outer IP and UDP headers
- Modifications to ESP, which protect (via authentication) the outer IP and UDP headers. This mimics the functionality of the AH protocol.
- Anti-replay, which is also part of the standard IPsec software suite, provides a mechanism to number all data packets and to ensure that receiving routers accept only packets with unique numbers.

The first of these components, ESP, is the standard IPsec encryption protocol. ESP protects a data packet's payload and its inner IP header fields both by encryption, which occurs automatically, and authentication. For authentication, ESP performs a checksum calculation on the data packet's payload and inner header fields and places the resultant hash (also called a digest) into a 12-byte HMAC-SHA1 field at the end of the packet. (A hash is a one-way compression.) The receiving device performs the same checksum and compares its calculated hash with that in the packet. If the two checksums match, the packet is accepted. Otherwise, it is dropped. In the figure below, the left stack illustrates the ESP/UDP encapsulation. ESP encrypts and authenticates the inner headers, payload, MPLS label (if present), and ESP trailer fields, placing the HMAC-SHA1 hash in the ICV checksum field at the end of the packet. The outer header fields added by ESP/UDP are neither encrypted nor authenticated.

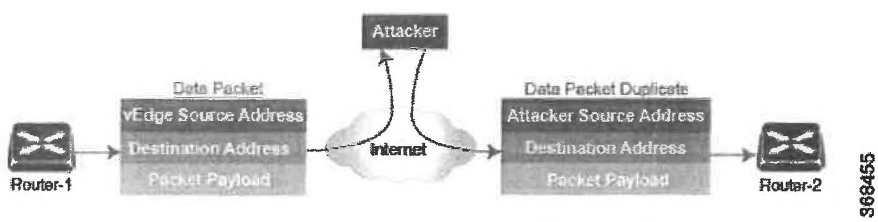
A second component that contributes to data packet integrity is the modifications to ESP to mimic AH. This modification performs a checksum that includes calculating the checksum over all the fields in the packet—the payload, the inner header, and also all the non-mutable fields in the outer IP header. AH places the resultant HMAC-SHA1 hash into the last field of the packet. The receiving device performs the same checksum, and accepts packets whose checksums match. In the figure below, the center stack illustrates the encapsulation performed by the modified version of ESP. ESP again encrypts the inner headers, payload, MPLS label (if present), and ESP trailer fields, and now mimics AH by authenticating the entire packet—the outer IP and UDP headers, the ESP header, the MPLS label (if present), the original packet, and the ESP trailer—and places its calculated HMAC-SHA1 hash into the ICV checksum field at the end of the packet.

For situations in which data packet authentication is not required, you can disable data packet authentication altogether. In this case, data packets are processed just by ESP, which encrypts the original packet, the MPLS label (if present), and the ESP trailer. This scheme is illustrated in the right stack in the figure below.



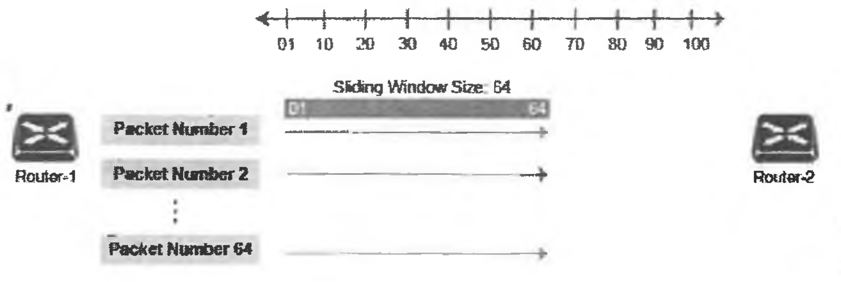
Note that Cisco SD-WAN devices exchange not only the encryption key (which is symmetric), but also the authentication key that is used to generate the HMAC-SHA1 digest. Both are distributed as part of the TLOC properties for a router.

Even though the IPsec connections over which data traffic is exchanged are secure, they often travel across a public network space, such as the Internet, where it is possible for a hacker to launch a replay attack (also called a man-in-the-middle, or MITM, attack) against the IPsec connection. In this type of attack, an adversary tampers with the data traffic by inserting a copy of a message that was previously sent by the source. If the destination cannot distinguish the replayed message from a valid message, it may authenticate the adversary as the source or may incorrectly grant to the adversary unauthorized access to resources or services.

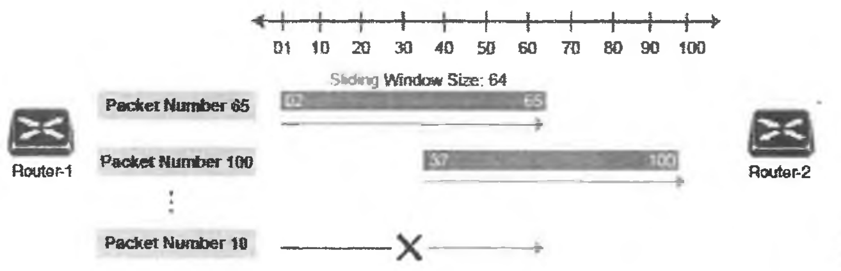


As a counter to such attacks, the Cisco SD-WAN overlay network software implements the IPsec anti-replay protocol. This protocol consists of two components, both of which protect the integrity of a data traffic stream. The first component is to associate sequence numbers with each data packets. The sender inserts a sequence number into each IPsec packet, and the destination checks the sequence number, accepting only packets with unique, non-duplicate sequence numbers. The second component is a sliding window, which defines a range of sequence numbers that are current. The sliding window has a fixed length. The destination accepts only packets whose sequence numbers fall within the current range of values in the sliding window, and it drops all others. A sliding window is used rather than accepting only packets whose sequence number is larger than the last known sequence number, because packets often do not arrive in order.

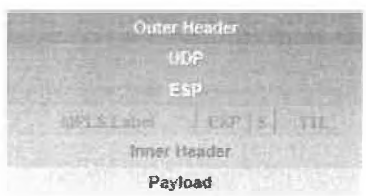
ВЯРНО С ОРИГИНАЛА



When the destination receives a packet whose sequence number is larger than the highest number in the sliding window, it slides the window to the right, thus changing the range of valid sequences numbers it will accept. This scheme protects against an MITM type of attack because, by choosing the proper window size, you can ensure that if a duplicate packet is inserted into the traffic stream, its sequence number will either be within the current range but will be a duplicate, or it will be smaller than the lowest current value of the sliding window. Either way, the destination will drop the duplicate packet. So, the sequence numbering combined with a sliding window provide protection against MITM type of attacks and ensure the integrity of the data stream flowing within the IPsec connection.



Carrying VPN Information in Data Packets



For enterprise-wide VPNs, Cisco SD-WAN devices support MPLS extensions to data packets that are transported within IPsec connections. The figure to the right shows the location of the MPLS information in the data packet header. These extensions provide the security for the network segmentation (that is, for the VPNs) that is needed to support multi-tenancy in a branch or segmentation in a campus. The Cisco SD-WAN implementation uses IPsec UDP-based overlay network layer protocol encapsulation as defined in RFC 4023. The security is provided by including the Initialization Vector (IV) at the beginning of the payload data in the ESP header. The IV value is calculated by the AES-256 cipher block chaining (CBC).

ВЯРНО С ОРИГИНАЛА

Превод от английски език

Шаблони

Превод от английски език

Шаблони

Използвайте екрана Шаблони, за да конфигурирате всички Viptela устройства в мрежата за наслагване, които се управляват от vManage NMS. За да направите това:

1. Създайте шаблон на устройство.

2. Прикачете устройства Viptela към шаблона на устройството.

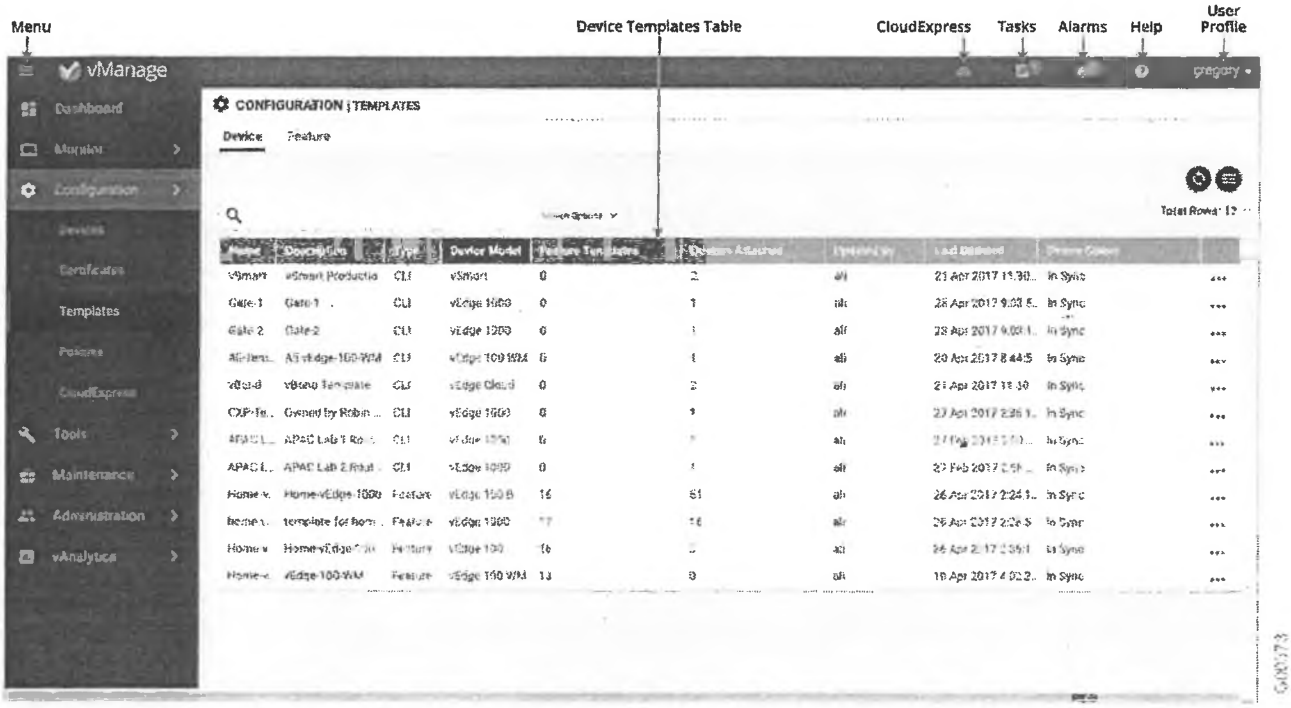
Бележка: За да създадете и промените конфигурацията на устройството, използвайте шаблони vManage , заедно с други екрани, свързани с конфигурацията в менютата за конфигурация и администриране на vManage . Не променяйте конфигурациите от интерфейса на командния ред (CLI), освен ако не сте изрично указани за това.

Елементи на екрана

- Горна лента — отляво са иконата на менюто за разширяване и свиване на менюто vManage и името на продукта vManage . Вдясно са редица икони и падащото меню на потребителския профил.
- Заглавна лента — Включва заглавието на екрана, Шаблони.
- Раздел Устройство — Създайте шаблони на устройства за конфигуриране на Viptela устройства.
    - Падащо меню Създаване на шаблон — Кликнете, за да създадете шаблони на устройства от шаблон на функция или от CLI.
    - Таблица с шаблони на устройството — Таблица на всички шаблони на устройства. За да подредите колоните, плъзнете заглавието на колоната до желаната позиция.
- Раздел Функция — Създайте шаблони на функции за конфигуриране на софтуерни функции, които можете да активирате на Viptela устройство.
    - Падащо меню Добавяне на шаблон — Кликнете, за да създадете шаблони за функции.
    - Таблица с шаблони с функции — Таблица с всички шаблони на функции. За да подредите колоните, плъзнете заглавието на колоната до желаната позиция.
- Поле за търсене — включва падащото меню Опции за търсене за низ от Съдържание или съвпадение.
- Икона за обновяване — Кликнете, за да опресните данните в таблицата на устройството с най-актуалните данни.
- Икона за показване на полета на таблицата — Кликнете, за да покажете или скриете колони от таблицата на устройството. По подразбиране се показват всички колони.

[redacted]

ЕАД



Създайте шаблон на устройство

Шаблоните на устройството определят пълната оперативна конфигурация на устройството. Шаблон на устройството се състои от няколко шаблона за функции. Всеки шаблон на функция определя конфигурацията за определена функция на софтуер Viptela.

Някои шаблони за функции са задължителни, обозначени със звездичка (*), а други са незадължителни. Всеки задължителен шаблон на функция и някои от незадължителните също имат шаблон по подразбиране. За софтуерни функции, които имат фабричен шаблон по подразбиране, можете да използвате или фабричния шаблон по подразбиране (наречен Factory_Default_*feature-name*_Template) или можете да създадете шаблон за персонализирана функция.

Създайте шаблон на устройство от шаблони за функции

За да създадете шаблон на устройство:

1. В раздела Устройство кликнете върху Създаване на шаблон.
2. От падащото меню Създаване на шаблон изберете От шаблон за функция.
3. От падащото меню Модел на устройството изберете типа устройство, за което създавате шаблона. vManage NMS показва всички шаблони на функции за този тип устройство. Необходимите шаблони за функции се обозначават със звездичка (*), а останалите шаблони са незадължителни. Шаблонът по подразбиране за всяка функция е избран по подразбиране.
4. В полето Име на шаблона въведете име за шаблона на устройството. Това поле е задължително и може да съдържа само главни и малки букви, цифрите от 0 до 9, тирета (-) и подчертавания (_). Не може да съдържа интервали или

всякакви други знаци.

5. В полето Описание въведете описание за шаблона на устройството. Това поле е задължително и може да съдържа всякакви знаци и интервали.

6. За да видите конфигурацията по подразбиране за шаблон на функция, изберете желания шаблон за функция и щракнете върху Преглед на шаблона. Кликнете върху Отказ, за да се върнете към екрана на шаблона за конфигурация.

7. За да създадете персонализиран шаблон за функция, изберете желания шаблон за фабрични настройки по подразбиране и Кликнете върху Създаване на шаблон. Формата на шаблона се показва. Горната част на формуляра съдържа полета за именуване на шаблона, а долната съдържа полета за определяне на параметрите на характеристиките.

8. В полето Име на шаблона въведете име за шаблон на функция. Това поле е задължително и може да съдържа само главни и малки букви, цифрите от 0 до 9, тирета (-) и подчертавания (_). Не може да съдържа интервали или други символи.

9. В полето за описание въведете описание на шаблона с функции. Това поле е задължително и може да съдържа всякакви знаци и интервали.

10. За всяко поле въведете желаната стойност. Може да се наложи да кликнете върху раздел или знак плюс (+), за да се покажат допълнителни полета.

11. Когато за първи път отворите шаблон за функция, за всеки параметър, който има стойност по подразбиране, обхватът е зададен по подразбиране (обозначен с отметка) и се показва настройката или стойността по подразбиране. За да промените по подразбиране или да въведете стойност, Кликнете върху падащото поле вляво от полето за параметър и изберете едно от следните:

Параметър обхват	Обхват Описание
Устройство Специфичн (посочено от икона на хост)	Използвайте специфична за устройството стойност за параметъра. За специфични за устройството параметри не можете стойност в шаблон за функция. Вие въвеждате стойността, когато прикачите Viptela устройство към устройство шаблон. Когато Кликнете върху Специфично за Устройство, се отваря полето Въведете ключ. Това поле показва ключ, който е уникален низ, който идентифицира параметъра във CSV файл, който създавате. Този файл е таблица в Excel, която съдържа по една колона за всеки ключ. Редът на заглавката съдържа имената на ключовете (един ключ на колона) и всеки ред след това съответства на устройство и определя стойностите на клавишите за това устройство. Вие качете CSV файла, когато прикачите устройство Viptela към шаблон на устройство. За повече информация вижте Създайте електронна таблица с променливи за шаблони. За да промените ключа по подразбиране, въведете нов низ и преместете курсора от полето Въведете ключ. Примери за специфични за устройството параметри са системният IP адрес, името на хоста, GPS местоположението и идентификационния номер на сайта.
Глобално (обозначено с икона на глобус)	Въведете стойност за параметъра и го приложете към всички устройства. Примери за параметри, които бихте могли да приложите глобално към група устройства са DNS сървър, syslog сървър и MTU на интерфейс

12. Кликнете върху Запазване.

13. Повторете стъпки 7 до 12, за да създадете персонализиран шаблон за всяка допълнителна функция на софтуера. За подробности относно създаването на шаблони за специфични функции вижте шаблоните, изброени в Налични шаблони за функции.

14. Кликнете върху Създаване. Новият конфигурационен шаблон се показва в таблицата на шаблона на устройството. Графата Шаблони за функции показва броя на шаблоните на функции, които са включени в шаблона на устройството, а колоната Вид показва „Функция", за да посочи, че шаблонът на устройството е създаден от колекция от шаблони на функции.

Друг начин за създаване на шаблони на устройства от шаблони на функции е първо да създадете един или повече персонализирани шаблони за функции и след това да създадете шаблони на устройства. Можете да създадете няколко шаблона за една и съща функция. За списък на шаблони за функции вж. Налични шаблони за функции.

1. От заглавната лента на шаблоните изберете Функция.

2. Кликнете върху Добавяне на шаблон.

3. В левия прозорец от Изберете Устройство изберете типа устройство, за което създавате шаблон. Можете да създадете един шаблон за функции за функции, които са достъпни на няколко типа устройства. Трябва обаче да създадете отделни шаблони на функции за софтуерни функции, които са достъпни само за типа устройство, което конфигурирате.

4. В десния прозорец изберете шаблон за функция. Формата на шаблона се показва. Горната част на формуляра съдържа полета за именуване на шаблона, а долната съдържа полета за определяне на необходимите параметри. Ако функцията има незадължителни параметри, в долната част на формата на шаблона се показва знак плюс (+) след задължителните параметри.

5. В полето Име на шаблона въведете име за шаблон на функция. Това поле е задължително и може да съдържа само главни и малки букви, цифрите от 0 до 9, тирета (-) и подчертавания (_). Не може да съдържа интервали или други символи.

6. В полето за описание въведете описание на шаблона с функции. Това поле е задължително и може да съдържа всякакви знаци и интервали.

7. За всеки необходим параметър изберете желаната стойност и, ако е приложимо, изберете обхвата на параметъра. Изберете обхвата от падащото меню вляво от полето със стойност на всеки параметър

8. Кликнете знакът (+) по-долу под необходимите параметри, за да зададете стойностите на незадължителните параметри.

9. Кликнете върху Запазване.

10. Повторете стъпки от 2 до 9 за всеки допълнителен шаблон за функция, който искате да създадете.

11. От заглавната лента на шаблоните изберете Устройство.

12. Кликнете върху Създаване на шаблон и от падащия списък изберете От шаблон за функция.

13. От падащото меню Модел на устройството изберете типа устройство, за което създавате през шаблона. vManage NMS показва всички шаблони на функции за типа устройство, което сте избрали. Необходимите шаблони за функции се обозначават със звездичка (*). Останалите шаблони не са задължителни.

14. В полето Име на шаблона въведете име за шаблона на устройството. Това поле е задължително и може да съдържа само главни и малки букви, цифрите от 0 до 9, тирета (-) и подчертавания (_). Не може да съдържа интервали или други символи.

15. В полето Описание въведете описание за шаблона на устройството. Това поле е задължително и може да съдържа всякакви знаци и интервали.

16. За да видите конфигурацията по подразбиране за шаблон на функция, изберете желания шаблон за функция и щракнете върху Преглед на шаблона. Кликнете върху Отказ, за да се върнете към екрана на шаблона за конфигурация.

17. За да използвате конфигурацията по подразбиране, Кликнете върху Създай, за да създадете шаблона на устройството. Новият шаблон на устройството се показва в таблицата на шаблона на устройството. Графата Шаблони за функции показва броя на шаблоните на функции, които са включени в шаблона на устройството, а колоната Вид показва „Функция", за да посочи, че шаблонът на устройството е създаден от колекция от шаблони на функции.

18. За да промените конфигурационната конфигурация по подразбиране, изберете шаблона на функциите, за който не желаете да използвате фабричния шаблон по подразбиране. От падащия списък на наличните шаблони на функции изберете шаблон за функция, който сте създали.

19. Повторете стъпка 18 за всеки шаблон за функции по подразбиране, който искате да промените.

20. Кликнете върху Създаване. Новият конфигурационен шаблон се показва в таблицата на шаблона на устройството. Графата Шаблони за функции показва броя на шаблоните на функции, които са включени в шаблона на устройството, а колоната Вид показва „Функция", за да посочи, че шаблонът на устройството е създаден от колекция от шаблони на функции.

Създайте шаблон на устройство от CLI

За да създадете шаблон на устройство чрез въвеждане на конфигурация в стила на CLI текст директно в vManage NMS:

1. В раздела Устройство кликнете върху Създаване на шаблон.
2. От падащото меню Създаване на шаблон изберете CLI шаблон.
3. От падащото меню Тип устройство изберете типа устройство, за което създавате шаблона.
4. В полето Име на шаблона въведете име за шаблона на устройството. Това поле е задължително и може да съдържа само главни и малки букви, цифрите от 0 до 9, тирета (–) и подчертавания (_). Не може да съдържа интервали или други символи.
5. В полето Описание въведете описание за шаблона на устройството. Това поле е задължително и може да съдържа всякакви знаци и интервали.
6. В полето CLI Конфигурация въведете конфигурацията или като го напишете, изрежете и поставите или качите файл.
7. За да преобразувате действителна стойност на конфигурация в променлива, изберете стойността и Кликнете върху Създай променлива. Въведете името на променливата и Кликнете върху Създаване на променлива. Можете също така да въведете името на променливата директно във формата {{*variable-name*}}; например, {{hostname}}.
8. Кликнете върху Добавяне. Новият шаблон на устройството се показва в таблицата на шаблона на устройството. Графата Функция Templates показва броя на шаблоните на функции, които са включени в шаблона на Шаблони , а колоната Type показва „CLI", за да посочи, че шаблонът на устройството е създаден от CLI текст.

Редактиране на шаблон

1. В раздела Устройство или Функция изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и кликнете върху Редактиране.

Преглед на шаблон

1. В раздела Устройство или Функция изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Преглед.

Изтрийте шаблон

1. В раздела Устройство или Функция изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Изтриване.
3. Кликнете върху OK, за да потвърдите изтриването на шаблона.

Преглед на шаблони на устройства, прикачени към шаблон за функция

1. В раздела Функция изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Покажи прикачени шаблони на устройства.

Отваря се изскачащият прозорец Преглед на шаблони за прикачено устройство, показващ имената на шаблоните на устройството, към които е прикачен шаблонът за функции.

Преглед на устройства, прикачени към шаблон на устройство

За шаблон на устройство, който сте създали от шаблони за функции:

1. В раздела Устройство изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и кликнете Прикачи устройства.
3. В прозореца Прикачване на устройства Кликнете върху раздела Прикачени устройства.

За шаблон на устройство, който сте създали от шаблон на CLI:

1. В раздела Устройство изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Покажи прикачени устройства.

Извършете операции с паралелни шаблони

На рутерите vEdge можете да извършвате същите операции паралелно от един или повече vManage сървъри. Можете да извършвате следните шаблони операции паралелно:

- Прикачете устройства към шаблон на устройство
- Отстранете устройствата от шаблон на устройство
- Променете стойностите на променливите за шаблон на устройство, което има прикрепени към него устройства

За операциите с шаблони се прилагат следните правила:

- Когато шаблон на устройство вече е прикачен към устройство, можете да промените един от неговите шаблони на функции. След това, когато Кликнете върху Актуализиране ► Конфигуриране на устройства, всички други операции с шаблони — включително свързване на устройства, отделяне на устройства и редактиране на стойности на устройството — се заключват на всички сървъри на vManage , докато операцията за актуализиране не завърши. Това означава, че потребител на друг vManage сървър не може да извършва никакви операции с шаблон, докато актуализацията не завърши.
- Можете да извършвате операции за свързване и отделяне на шаблони на устройства на различни устройства, от един или повече vManage сървъри едновременно. Ако обаче някоя от тези операции се изпълнява на един vManage сървър, не можете да редактирате шаблони за функции на който и да е от сървърите, докато операцията за прикачване или отделяне не завърши.

Прикачете устройства към шаблон на устройство

За да прикачите едно или повече устройства към шаблон на устройство:

1. В раздела Устройство изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и кликнете Прикачи устройства. Диалоговият прозорец „Прикачване на устройства“ се отваря с избрания раздел „Избор на устройства“
3. В колоната Налични устройства вляво изберете група и потърсете едно или повече устройства, изберете устройство от списъка или Кликнете върху Избор на всички.
4. Кликнете върху стрелката, сочеща надясно, за да преместите устройството в графа Избрани устройства вдясно.
5. Кликнете върху Прикачи.
6. Ако шаблонът съдържа променливи, въведете липсващите стойности на променливите за всяко избрано от вас устройство по един от следните начини:
   - Въведете ръчно стойностите за всяко устройство или в колоната на таблицата или като Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Редактиране на шаблона на устройството.
   - Кликнете върху Импортиране на файл в горния десен ъгъл на екрана, за да качите CSV файл, който изброява всички променливи и определя стойността на всяка променлива за всяко устройство.

[redacted]

След като предоставите стойности за всички променливи, колоната Статус за всеки ред на устройството показва зелена отметка.

7. Кликнете върху Напред.
8. В левия прозорец изберете устройството, за да визуализирате конфигурацията, която е готова за избутване към устройството. В десния прозорец се показва конфигурацията на устройството и се избира раздела Преглед на конфигурация в горния десен ъгъл. Кликнете върху раздела Разлики в конфигурацията, за да прегледате разликите между тази конфигурация и конфигурацията, която работи в момента на устройството, ако е приложимо.
   Кликнете върху бутона Назад, за да редактирате променливите стойности, въведени в предишния екран.
9. Кликнете върху Конфигуриране на устройства, за да избутате конфигурацията към устройствата.
   Графата за състоянието показва дали конфигурацията е успешно избутана. Кликнете върху скобата на десния ъгъл отляво на реда, за да се покажат подробности за операцията с избутване.

Копирайте шаблон

1. В раздела Устройство или Функция изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Копиране.
3. Въведете ново име и описание на шаблон.
4. Кликнете върху Копиране.

Редактиране на шаблон на CLI устройство

1. В раздела Устройство изберете шаблон.
2. Кликнете върху иконата Още действия вдясно на реда и кликнете върху Редактиране.
3. В прозореца на шаблона на устройството CLI редактирайте шаблона.
4. Кликнете върху Актуализиране.

Експортирайте таблица с променливи във формат CSV за шаблон

1. В раздела Устройство изберете шаблон на устройство.
2. Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Експортиране на CSV.

Промяна на променливи стойности за устройство

За да промените стойностите на променливите за шаблон на устройство, което има прикрепени към него устройства:

1. В раздела Устройство изберете шаблон.

2. Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Промяна на стойностите на устройството.

3. Редактирайте стойностите на променливите, които преди сте въвели за устройството, по един от следните начини:

   - Кликнете върху иконата Още действия вдясно на реда и Кликнете върху Редактиране на шаблона на устройството. В прозореца за актуализиране на шаблона на устройството редактирайте стойностите според нуждите и Кликнете върху Актуализиране. Повторете за всяко устройство, за което искате да редактирате променливите стойности.

   - Кликнете върху Импортиране на файл в горния десен ъгъл на екрана, за да качите CSV файл, който изброява всички променливи и определя стойността на всяка променлива за всяко устройство.

   След като предоставите стойността за всички променливи, колоната Статус за всеки ред устройства показва зелена отметка.

4. Кликнете върху Напред.

5. В левия прозорец изберете устройството, за да визуализирате конфигурацията, която е готова за избутване към устройството. В десния прозорец се показва конфигурацията на устройството и се избира раздела Преглед на конфигурация в горния десен ъгъл.
   Кликнете върху раздела Разлики в конфигурацията, за да прегледате разликите между тази конфигурация и конфигурацията, която работи в момента на устройството, ако е приложимо.
   Кликнете върху бутона Назад, за да редактирате променливите стойности, въведени в предишния екран.

6. Кликнете върху Конфигуриране на устройства, за да избутате конфигурацията към устройствата.
   Графата за състоянието показва дали конфигурацията е успешно избутана. Кликнете върху скобата на десния ъгъл отляво на реда, за да се покажат подробности за операцията с избутване.

Налични шаблони за функции

vManage NMS предоставя следните шаблони на функции за конфигуриране на Viptela устройства в мрежата за наслагване:

- AAA
- Архив
- Банер
- BFD
- BGP
- Мост
- Клетъчен профил
- DHCP-сървър
- IGMP
- Настаняване

- Мултикаст
- NTP
- OMP
- OSPF
- PIM
- Сигурност
- SNMP
- Система
- VPN
- VPN-Интерфейс-мост
- VPN-Интерфейс-Клетъчен
- VPN-Интерфейс-Ethernet
- VPN-Interface-GRE
- VPN-Интерфейс-NAT-Екип
- VPN-Interface-PPP
- VPN-Интерфейс-PPP-Ethernet
- WiFi Радио
- WiFi SSID

Аз, долуподписаният, Явор Стоянов Профиров, удостоверявам верността на направения от мен превод от английски на български език на приложения документ. Преводът се състои от 11 страници.

Преводач: Явор Стоянов Профиров

Templates

Use the Templates screen to configure all Viptela devices in the overlay network that are managed by the vManage NMS. To do so:

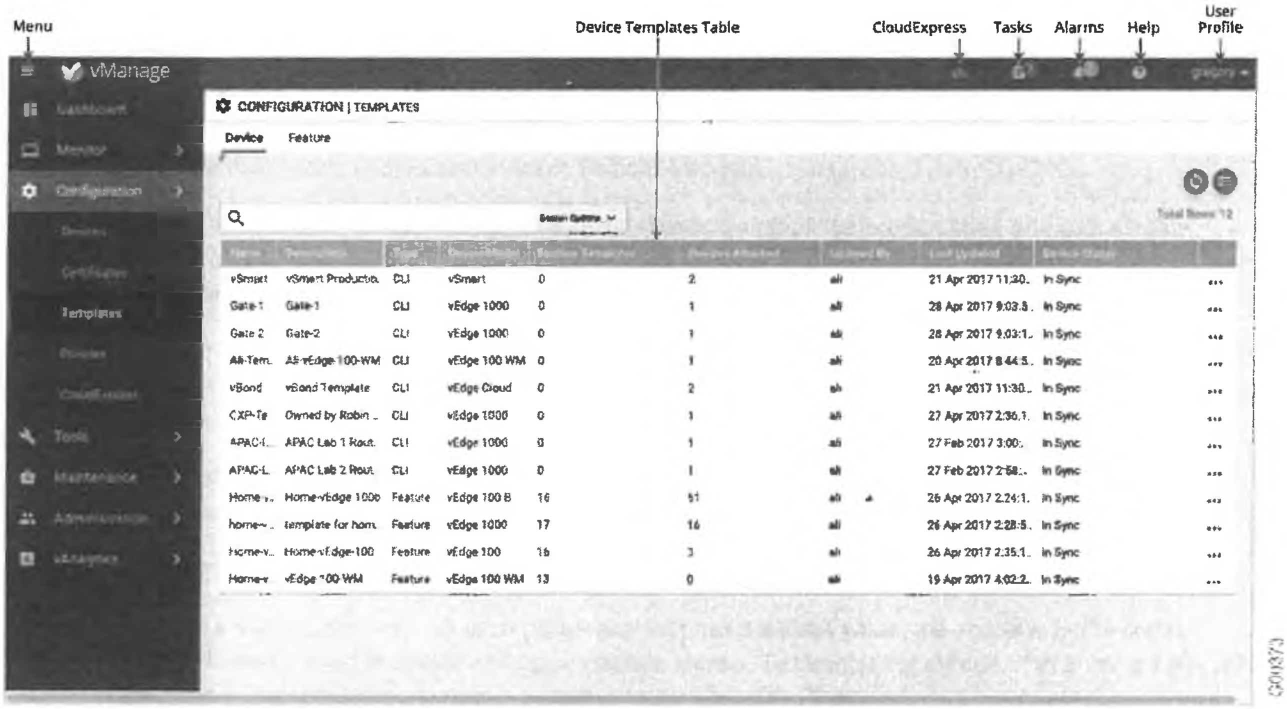
1. Create a device template.
2. Attach Viptela devices to the device template.

Note: To create and modify a device's configuration, use vManage templates, along with other configuration-related screens in the vManage Configuration and Administration menus. Do not modify configurations from the command-line interface (CLI) unless you are explicitly directed to do so.

Screen Elements

- Top bar—On the left are the menu icon, for expanding and collapsing the vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Templates.
- Device tab—Create device templates for configuring Viptela devices.
    - Create Template drop-down—Click to create device templates from feature template or the CLI.
    - Device template table—Table of all device templates. To re-arrange the columns, drag the column title to the desired position.
- Feature tab—Create feature templates for configuring software features that you can enable on a Viptela device.
    - Add Template drop-down—Click to create feature templates.
    - Feature template table—Table of all feature templates. To re-arrange the columns, drag the column title to the desired position.
- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Show Table Fields icon—Click to display or hide columns from the device table. By default, all columns are displayed.

ВЯРНО С ОРИГИНАЛА



Create a Device Template

Device templates define a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular Viptela software feature. Some feature templates are mandatory, indicated with an asterisk (*), and some are optional. Each mandatory feature template, and some of the optional ones too, have a factory-default template. For software features that have a factory-default template, you can use either the factory-default template (named Factory_Default_*feature-name*_Template) or you can create a custom feature template.

Create a Device Template from Feature Templates

To create a device template:

1. In the Device tab, click Create Template.
2. From the Create Template drop-down, select From Feature Template.
3. From the Device Model drop-down, select the type of device for which you are creating the template. vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.
4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces o

ВЯРНО С ОРИГИНАЛА

any other characters.

5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

6. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.

7. To create a custom template for a feature, select the desired factory-default feature template and click Create Template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining feature parameters.

8. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

9. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.

10. For each field, enter the desired value. You may need to click a tab or the plus sign (+) to display additional fields.

11. When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Viptela device to a device template. When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Viptela device to a device template. For more information, see Create a Template Variables Spreadsheet. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

ВЯРНО С ОРИГИНАЛА

12. Click Save.

13. Repeat Steps 7 through 12 to create a custom template for each additional software feature. For details on creating specific feature templates, see the templates listed in Available Feature Templates.

14. Click Create. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Another way to create device templates from feature templates is to first create one or more custom feature templates and then create device templates. You can create multiple feature templates for the same feature. For a list of feature templates, see Available Feature Templates.

1. From the Templates title bar, select Feature.

2. Click Add Template.

3. In the left pane, from Select Devices, select the type of device for which you are creating a template. You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.

4. In the right pane, select the feature template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining required parameters. If the feature has optional parameters, the bottom of the template form shows a plus sign (+) after the required parameters.

5. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the Description field, enter a description for the feature template. This field is mandatory, and it can contain any characters and spaces.

7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu to the left of each parameter's value box

8. Click the plus sign (+) below the required parameters to set the values of optional parameters.

9. Click Save.

10. Repeat Steps 2 to 9 for each additional feature template you wish to create.

11. From the Templates title bar, select Device.

12. Click Create Template, and from the drop-down list select From Feature Template.

13. From the Device Model drop-down, select the type of device for which you are creating the device template. vManag NMS displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (*). The remaining templates are optional.

14. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

ВЯРНО С ОРИГИНАЛА

15. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.

16. To view the factory-default configuration for a feature template, select the desired feature template and click View Template. Click Cancel to return to the Configuration Template screen.

17. To use the factory-default configuration, click Create to create the device template. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

18. To modify the factory-default configuration, select the feature template for which you do not wish to use the factory-default template. From the drop-down list of available feature templates, select a feature template that you created.

19. Repeat Step 18 for each factory-default feature template you wish to modify.

20. Click Create. The new configuration template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Create a Device Template from the CLI

To create a device template by entering a CLI text-style configuration directly on the vManage NMS:

1. In the Device tab, click Create Template.
2. From the Create Template drop-down, select CLI Template.
3. From the Device Type drop-down, select the type of device for which you are creating the template.
4. In the Template Name field, enter a name for the device template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
5. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
6. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.
7. To convert an actual configuration value to a variable, select the value and click Create Variable. Enter the variable name, and click Create Variable. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.
8. Click Add. The new device template is displayed in the Device Template table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

ВЯРНО С ОРИГИНАЛА

Edit a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Edit.

View a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click View.

Delete a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Delete.
3. Click OK to confirm deletion of the template.

View Device Templates Attached to a Feature Template

1. In the Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Device Templates.

The View Attached Device Templates popup window opens displaying the names of the device templates to which the feature template is attached.

View Devices Attached to a Device Template

For a device template that you created from feature templates:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices.
3. In the Attach Devices window, click the Attached Devices tab.

For a device template that you created from a CLI template:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Show Attached Devices.

ВЯРНО С ОРИГИНАЛА

ЕАД

Perform Parallel Template Operations

On vEdge routers, you can perform the same operations, in parallel, from one or more vManage servers. You can perform the following template operations in parallel:

- Attach devices to a device template
- Detach devices from a device template
- Change the variable values for a device template that has devices attached to it

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. Then when you click Update ► Configure Devices, all other template operations—including attach devices, detach devices, and edit device values—are locked on all vManage servers until the update operation completes. This means that a user on another vManage server cannot perform any template operations until the update completes.
- You can perform the attach and detach device template operations on different devices, from one or more vManage servers, at the same time. However, if any one of these operations is in progress on one vManage server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

Attach Devices to a Device Template

To attach one or more devices to a device template:

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Attach Devices. The Attach Devices dialog box opens with the Select Devices tab selected
3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click Select All.
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.
5. Click Attach.
6. If the template contains variables, enter the missing variable values for each device you selected in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking the More Actions icon to the right of the row and clicking Edit Device Template.
   - Click Import File in the upper right corner of the screen to upload a CSV file that lists all the variables and defines each variable's value for each device.

ВЯРНО С ОРИГИНАЛА

Once you provide values for all variables, the Status column for each device row displays a green check mark.

7. Click Next.

8. In the left pane, select the device to preview the configuration that is ready to be pushed to the device. The right pane displays the device's configuration and the Config Preview tab in the upper right corner is selected.
   Click the Config Diff tab to preview the differences between this configuration and the configuration currently running on the device, if applicable.
   Click the Back button to edit the variable values entered in the previous screen.

9. Click Configure Devices to push the configuration to the devices.
   The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

Copy a Template

1. In the Device or Feature tab, select a template.
2. Click the More Actions icon to the right of the row and click Copy.
3. Enter a new template name and description.
4. Click Copy.

Edit a CLI Device Template

1. In the Device tab, select a template.
2. Click the More Actions icon to the right of the row and click Edit.
3. In the Device CLI Template window, edit the template.
4. Click Update.

Export a Variables Spreadsheet in CSV Format for a Template

1. In the Device tab, select a device template.
2. Click the More Actions icon to the right of the row and click Export CSV.

Change Variable Values for a Device

To change the variable values for a device template that has devices attached to it:

1. In the Device tab, select a template.

ВЯРНО С ОРИГИНАЛА

2. Click the More Actions icon to the right of the row and click Change Device Values.

3. Edit the variable values that you previously entered for the device in one of the following ways:

    - Click the More Actions icon to the right of the row and click Edit Device Template. In the Update Device Template window, edit the values as needed and click Update. Repeat for each device for which you wish to edit the variable values.

    - Click Import File in the upper right corner of the screen to upload a CSV file that lists all the variables and defines each variable's value for each device.

    Once you provide the value for all variables, the Status column for each device row displays a green check mark.

4. Click Next.

5. In the left pane, select the device to preview the configuration that is ready to be pushed to the device. The right pane displays the device's configuration and the Config Preview tab in the upper right corner is selected.
   Click the Config Diff tab to preview the differences between this configuration and the configuration currently running on the device, if applicable.
   Click the Back button to edit the variable values entered in the previous screen.

6. Click Configure Devices to push the configuration to the devices.
   The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to the left of the row to display details of the push operation.

Available Feature Templates

vManage NMS provides the following feature templates to configure Viptela devices in the overlay network:

- AAA
- Archive
- Banner
- BFD
- BGP
- Bridge
- Cellular-Profile
- DHCP-Server
- IGMP
- Logging

ВЯРНО С ОРИГИНАЛА

- Multicast
- NTP
- OMP
- OSPF
- PIM
- Security
- SNMP
- System
- VPN
- VPN-Interface-Bridge
- VPN-Interface-Cellular
- VPN-Interface-Ethernet
- VPN-Interface-GRE
- VPN-Interface-NAT-Pool
- VPN-Interface-PPP
- VPN-Interface-PPP-Ethernet
- WiFi Radio
- WiFi SSID

ВЯРНО С ОРИГИНАЛА

ПРЕДЛАГАНИ ЦЕНОВИ ПАРАМЕТРИ

от

А1 България ЕАД

за участие в обществена поръчка, с предмет:

„ДОСТАВКА НА КОМУНИКАЦИОННО ОБОРУДВАНЕ, ХАРДУЕР И СОФТУЕР, НЕОБХОДИМИ ЗА ОБНОВЯВАНЕ НА ИНФОРМАЦИОННИ И КОМУНИКАЦИОННИ СИСТЕМИ НА НАЦИОНАЛНА АГЕНЦИЯ ЗА ПРИХОДИТЕ“

[redacted]

За участие по Обособена позиция № 2 с предмет: „Доставка на софтуерно дефинирана мрежа за пренос на данни

[redacted]

13.07.2020 год.

[redacted]

ПРИЛОЖЕНИЕ № 3.2

ДО

„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД

ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2

ЦЕНОВО ПРЕДЛОЖЕНИЕ

Наименование на обществената поръчка:	***„Доставка на комуникационно оборудване, хардуер и софтуер, необходими за обновяване на информационни и комуникационни системи на Национална агенция за приходите“***
Наименование на обособена позиция, за която участникът подава оферта	***Обособена позиция № 2: „Доставка на софтуерно дефинирана мрежа за пренос на данни“***
Наименование на участника:	*А1 БЪЛГАРИЯ ЕАД*
Правно-организационна форма на участника:	*Еднолично Акционерно дружество* *(физическо или юридическо лице, обединение или друго образувание, което има право да изпълнява доставки съгласно законодателството на държавата, в която е установено)*
Седалище по регистрация и адрес на управление:	гр. София, Община „Илинден“, ж.к. „Захарна фабрика“, п.к.1309, ул. „Кукуш“ №1
ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:	ЕИК 131468980
Представляващ	МАРТИН ДИМИТРОВ ЙОРДАНОВ- Акаунт Мениджър “Държавни структури”- упълномощено лице *(законен представител или лице, специално упълномощено за участие в процедурата[1]*

[redacted]

[1] Съгласно чл. 41, ал. 5 от Правилника за прилагане на Закона за обществените поръчки (ППЗОП) когато документи, свързани с участие в обществени поръчки се подават от лице, което представя участника по пълномощие, в Единния европейски документ за обществени поръчки (ЕЕДОП) се посочва информация относно обхвата на представителната му власт.

[redacted]

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След запознаване с документацията за участие в обществената поръчка с горепосочения предмет, ние предоставяме следното ценово предложение по горецитираната обособена позиция:

1. Предлагаме да изпълним доставката, предмет на горецитираната процедура за възлагане на обществена поръчка при цени, както следва:

№	Описание	Количество	Единична цена в лв. без ДДС	Обща цена в лв. без ДДС
I.	II.	III.	IV.	V.
1.	Софтуерно дефиниран маршрутизатор тип 1	36 броя	11 885.00	**427 860.00**
2.	Софтуерно дефиниран маршрутизатор тип 2	42 броя	29 328.00	**1 231 776.00**
3.	Софтуерно дефиниран маршрутизатор тип 3	36 броя	53 874.00	**1 939 464.00**
4.	Софтуерно дефиниран маршрутизатор тип 4	2 броя	136 094.00	**272 188.00**
5.	Софтуер за управление на софтуерно дефинирана мрежа	1 брой	215 355.00	**215 355.00**
			Обща цена в лева без ДДС	**4 086 643.00**

2. В цените по т. 1 са включени всички разходи за изпълнение на поръчката. Потвърждаваме, че възложителят няма да дължи заплащането на каквито и да е други разноски, направени от нас като изпълнител.

3. Потвърждаваме, че цените по т. 1 са постоянни за целия срок на договора и не подлежат на промяна за времето на изпълнение на договора, освен в случаите когато това е в полза на възложителя.

Приложения: …….

Забележка:

1. *Предложените от участника цени следва да са в български лева без ДДС, закръглени* [redacted] *втория знак на десетичната запетая.*

2. *Участник, който допусне аритметична грешка, се отстранява от участие в процедурата по съответната обособена позиция.*

3. *Участник, който предложи обща цена, която е по-висока от прогнозната стойност на съответната обособена позиция, се отстранява от по-нататъшно участие в процедурата по съответната обособена позиция.*

4. *Липсата на ценово предложение, както и предоставянето на ценово предложение, което не отговаря на изискванията на документацията за обществената поръчка, е основание за отстраняване от по-нататъшно участие в процедурата по съответната обособена позиция.*

Дата на подписване:	[redacted] **2020 г.**
Подпис и печат:	**……………[redacted]……………**
Име и фамилия	**Мартин Йорданов**
Длъжност	**Акаунт Мениджър "Държавни структури"**
Наименование на участника	**А1 БЪЛГАРИЯ ЕАД**

[redacted]