***ДО***

***„ИНФОРМАЦИОННО ОБСЛУЖВАНЕ“ АД***

***ГР. СОФИЯ, УЛИЦА „ПАНАЙОТ ВОЛОВ“ № 2***

***Т Е Х Н И Ч Е С К О П Р Е Д Л О Ж Е Н И Е***

|  |  |
| --- | --- |
| **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:** |  |
| **Правно-организационна форма на участника:** | *(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:** |  |
| **ЕИК / Код по регистър БУЛСТАТ/ регистрационен номер или друг идентификационен код:** |  |
| **Представляващ** | *(законен представител или лице, специално упълномощено за участие в процедурата[[1]](#footnote-1)* |

**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:

1. **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. Декларирам, че представляваният от мен участник ще изпълни поръчката, съобразявайки се с условията по изпълнение, посочени от възложителя в документацията за обществената поръчка.
   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.
   3. Задължаваме се да извършим 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“), 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.
      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.
   4. Подробно описание на вида, количеството и техническите характеристики на доставеното от нас оборудване, хардуер и софтуер, е описано, както следва:
      1. **Софтуерно дефиниран маршрутизатор тип 1 – 36 броя.**

|  |  |  |
| --- | --- | --- |
| **Изискано от Възложителя** | | **Предложено от участника** |
| **А.** | | **Б.** |
| **Обща информация** | | |
|  | Захранване –в диапазона от минимум 100 до 240 VAC. |  |
|  | Работен температурен диапазон от 0º до +40 ºC. |  |
|  | Безшумна работа – без вентилатори. |  |
|  | Минимум четири интерфейса 100/1000BASE-T. |  |
|  | Брой USB портове - минимум един, версия 3.0 или по-висока. |  |
|  | Сериен конзолен порт - минимум един. |  |
|  | Минимум 4GB DRAM. |  |
|  | Минимум 4 GB Flash. |  |
|  | Производителност от минимум 500Mbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройствo трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя. |  |
|  | Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание. |  |
|  | Да поддържа IPv4 и IPv6 WAN транспортни мрежи. |  |
|  | Да поддържа изграждането на SDWAN overlay с използването на IPSec върху различни WAN мрежи – Internet и MPLS. |  |
|  | Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика. |  |
|  | Да поддържа IPseс AH с използване на минимум HMAC-SHA1 алгоритъм. |  |
|  | Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys. |  |
|  | Да поддържа изграждане на GRE тунели до външни системи за сигурност. |  |
|  | Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SDWAN контролерите. |  |
|  | Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати. |  |
|  | Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност. |  |
|  | Да поддържа използване на сертификати от CA на възложителя. |  |
|  | Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните. |  |
|  | Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация. |  |
|  | Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел. |  |
|  | Да поддържа автоматично маршутизиране на ниво приложения през различни WAN връзки на база динамичните параметрите на IPSec WAN тунелите – packet loss, jitter и delay. |  |
|  | Да има вграден zone firewall. |  |
|  | Да има application firewall с вградено разпознаване на приложенията. |  |
|  | Да поддържа филтриране на трафика чрез ACL. |  |
|  | Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите. |  |
|  | Да поддържа управляеми SDWAN IPSec топологии – hub-and-spoke, full mesh и комбинации между двете. |  |
|  | Да поддържа отделна, виртуална, топология за всеки сегмент. |  |
|  | Да поддържа следните протоколи за интеграция с външни мрежи:   * Static route * OSPF * BGP |  |
|  | Да поддържа PIM. |  |
|  | Да поддържа следните видове NAT услуги   * статичен NAT * симетричен NAT * NAT64 * NAT pools * PAT |  |
|  | Да поддържа изграждане на SD-WAN IPSec през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay. |  |
|  | Да поддържа QoS:   * CoS маркиране * Минимум 8 пакетни опашки на интерфейс * LLQ опашка * Управление на пакетните опашки с WRР или подобен алгоритъм * Управление на задрсътванията с RED и WRED алгоритми * Traffic policing * Traffic shaping |  |
|  | Да поддържа packet duplication – изпращане на един пакет по два или повече отделни SDWAN IPSec тунела до приемащия SD-WAN маршрутизатор. |  |
|  | 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. |  |
|  | 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. |  |
|  | Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя; |  |
|  | Устройството да е окомплектовано с SDWAN лицензи за минимум 100Мbps WAN трафик. |  |
| **Гаранция и поддръжка:** | |  |
|  | Срок на хардуерната гаранция - минимум 5 (пет) години. |  |
|  | Срок на техническа поддържка – минимум 5 (пет) години. |  |
|  | Получаване на нови версии на софтуера - минимум 5 (пет) години. |  |
|  | Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години |  |

* + 1. **Софтуерно дефиниран маршрутизатор тип 2 – 42 броя.**

|  |  |  |
| --- | --- | --- |
| **Изискано от Възложителя** | | **Предложено от участника** |
| **А.** | | **Б.** |
| **Обща информация** | | |
|  | Захранване –в диапазона от минимум 100 до 240 VAC. |  |
|  | Работен температурен диапазон от 0º до +40 ºC |  |
|  | Безшумна работа – без вентилатори. |  |
|  | Минимум четири интерфейса 100/1000BASE-T и два интерфейса SFP. |  |
|  | Брой USB портове - минимум един, версия 3.0 или по-висока. |  |
|  | Сериен конзолен порт - минимум един. |  |
|  | Минимум 4GB DRAM. |  |
|  | Минимум 4 GB Flash. |  |
|  | Производителност от минимум 1Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройствo трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя. |  |
|  | Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание. |  |
|  | Да поддържа IPv4 и IPv6 WAN транспортни мрежи. |  |
|  | Да поддържа изграждането на SDWAN overlay с използването на IPSec. |  |
|  | Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика. |  |
|  | Да поддържа IPseс AH с използване на минимум HMAC-SHA1 алгоритъм. |  |
|  | Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys. |  |
|  | Да поддържа изграждане на GRE тунели до външни системи за сигурност. |  |
|  | Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите. |  |
|  | Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати. |  |
|  | Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност. |  |
|  | Да поддържа използване на сертификати от CA на възложителя. |  |
|  | Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните. |  |
|  | Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация. |  |
|  | Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел. |  |
|  | 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. |  |
|  | Да има вграден zone firewall. |  |
|  | Да има application firewall с вградено разпознаване на приложенията. |  |
|  | Да поддържа филтриране на трафика чрез ACL. |  |
|  | Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите. |  |
|  | Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете. |  |
|  | Да поддържа отделна, виртуална, топология за всеки сегмент |  |
|  | Да поддържа следните протоколи за интеграция с външни мрежи:   * Static route * OSPF * BGP * VRRP |  |
|  | Да поддържа 802.1Q |  |
|  | Да поддържа обединяване на интерфейси в bridge групи |  |
|  | Да поддържа IGMP v1 и v2 |  |
|  | Да поддържа PIM |  |
|  | Да поддържа следните видове NAT услуги   * статичен NAT * динамичен NAT * NAT64 * NAT pools * PAT |  |
|  | Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay |  |
|  | Да поддържа QoS:   * CoS маркиране * Минимум 8 пакетни опашки на интерфейс * LLQ опашка * Управление на пакетните опашки с WRР или подобен алгоритъм * Управелние на задрсътванията с RED и WRED алгоритми * Traffic policing * Traffic shaping |  |
|  | Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор. |  |
|  | 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 |  |
|  | 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. |  |
|  | Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя; |  |
|  | Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик. |  |
| **Гаранция и поддръжка:** | |  |
|  | Срок на хардуерната гаранция - минимум 5 (пет) години. |  |
|  | Срок на техническа поддържка – минимум 5 (пет) години. |  |
|  | Получаване на нови версии на софтуера - минимум 5 (пет) години. |  |
|  | Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години. |  |

* + 1. **Софтуерно дефиниран маршрутизатор тип 3 – 36 броя.**

|  |  |  |
| --- | --- | --- |
| **Изискано от Възложителя** | | **Предложено от участника** |
| **А.** | | **Б.** |
| **Обща информация** | | |
|  | Захранване –в диапазона от минимум 100 до 240 VAC. |  |
|  | Работен температурен диапазон от 0º до +40 ºC |  |
|  | Шаси за монтаж в 19“ шкаф |  |
|  | Два токозахранващи модула |  |
|  | Минимум четири интерфейса, които поддържат 100/1000BASE-T и SFP |  |
|  | Брой USB портове - минимум 1, |  |
|  | Конзолен порт - 1 |  |
|  | Минимум 8GB DRAM |  |
|  | Възможност за добавяне на модул с LTE cat. 6 модем |  |
|  | Възможност за добавяне на минимум осем 1000Base-T порта |  |
|  | Производителност от минимум 3Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройствo трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя |  |
|  | Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание |  |
|  | Да поддържа IPv4 и IPv6 WAN транспортни мрежи |  |
|  | Да поддържа изграждането на SDWAN overlay с използването на IPSec |  |
|  | Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика |  |
|  | Да поддържа IPseс AH с използване на минимум HMAC-SHA1 алгоритъм |  |
|  | Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys |  |
|  | Да поддържа изграждане на GRE тунели до външни системи за сигурност |  |
|  | Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите |  |
|  | Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати |  |
|  | Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност |  |
|  | Да поддържа използване на сертификати от CA на възложителя |  |
|  | Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните. |  |
|  | Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация |  |
|  | Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация. |  |
|  | Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел. |  |
|  | 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 |  |
|  | Да има вграден zone firewall |  |
|  | Да има application firewall с вградено разпознаване на приложенията |  |
|  | Да поддържа филтриране на трафика чрез ACL |  |
|  | Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите |  |
|  | Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете |  |
|  | Да поддържа отделна, виртуална, топология за всеки сегмент |  |
|  | Да поддържа следните протоколи за интеграция с външни мрежи:   * Static route * OSPF * BGP * VRRP |  |
|  | Да поддържа 802.1Q |  |
|  | Да поддържа IGMP v2 и v3 |  |
|  | Да поддържа минимум PIM SSM |  |
|  | Да поддържа PIM rendezvous point |  |
|  | Да поддържа статичен и динамичен NAT и NAT pool |  |
|  | Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay |  |
|  | Да поддържа QoS:   * Минимум 8 пакетни опашки на интерфейс * LLQ опашка * Управление на пакетните опашки с WRР 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 |  |
|  | Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор |  |
|  | Да има вграден IPS |  |
|  | Да има вградена Anti Malware защита |  |
|  | Да има URL филтриране по категории |  |
|  | Да осигурява декриптиране на SSL и TLS за инспектиране на криптиран трафик |  |
|  | 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 |  |
|  | 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 |  |
|  | 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. |  |
|  | Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя; |  |
|  | Устройството да е окомплектовано с SDWAN лицензи за минимум 1Gbps WAN трафик |  |
| **Гаранция и поддръжка:** | |  |
|  | Срок на хардуерната гаранция - минимум 5 (пет) години. |  |
|  | Срок на техническа поддържка – минимум 5 (пет) години. |  |
|  | Получаване на нови версии на софтуера - минимум 5 (пет) години. |  |
|  | Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години |  |

* + 1. **Софтуерно дефиниран маршрутизатор тип 4 – 2 броя.**

|  |  |  |
| --- | --- | --- |
| **Изискано от Възложителя** | | **Предложено от участника** |
| **А.** | | **Б.** |
| **Обща информация** | | |
|  | Захранване –в диапазона от минимум 100 до 240 VAC |  |
|  | Работен температурен диапазон от 0º до +40 ºC |  |
|  | Шаси за монтаж в 19“ шкаф |  |
|  | Два токозахранващи модула |  |
|  | Минимум шест 1000BaseT и два SFP+ порта. |  |
|  | Устройството да бъде доставено с четири 10GBASE-SR SFP+ модула |  |
|  | Брой USB портове - минимум 1, |  |
|  | Сериен конзолен порт - минимум 1 |  |
|  | Минимум 8GB DRAM |  |
|  | Производителност от минимум 6Gbps throughput за IPSec SDWAN трафик с 1400 байта, или по-големи, пакети. Производителността на предлаганото устройствo трябва да бъде удостоверена чрез брошура, технически ръководство или декларация от производителя |  |
|  | Да участва в SDWAN мрежа под управление на SDWAN контролерите в това задание |  |
|  | Да поддържа IPv4 и IPv6 WAN транспортни мрежи |  |
|  | Да поддържа изграждането на SDWAN overlay с използването на IPSec |  |
|  | Да поддържа минимум AES-256 GCM алгоритъм за криптиране на трафика |  |
|  | Да поддържа IPseс AH с използване на минимум HMAC-SHA1 алгоритъм |  |
|  | Да използва уникална двойка ключове за всеки IPSec тунел в мрежата – IPSec pairwise keys |  |
|  | Да поддържа изграждане на GRE тунели до външни системи за сигурност |  |
|  | Да поддържа TLS или DTLS протоколи за изграждане на контролните връзки до SD-WAN контролерите |  |
|  | Да поддържа удостоверяване на идентичността между контролерите и маршрутизаторите с цифрови сертификати |  |
|  | Да има инсталиран от производителя цифров сертификат в TPM модул или да използва хардуерно решение за защита на сертификатите и ключовете с подобна функционалност |  |
|  | Да поддържа използване на сертификати от CA на възложителя |  |
|  | Да поддържа минимум AES-256 GCM агоритъм за шифроване на контролните връзки до SD-WAN контролерите и верификация на интегритета на данните. |  |
|  | Да поддържа изолирането на трафика от определени вътрешни интерфейси чрез използване на VRF, MPLS или подобен протокол за сегментация |  |
|  | Да поддържа сегментиране на трафика при SDWAN преноса чрез VRF, MPLS или подобен протокол за сегментация. |  |
|  | Да поддържа автоматично измерване на packet loss, jitter и delay за всеки SDWAN IPSec тунел. |  |
|  | 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 |  |
|  | Да има вграден zone firewall |  |
|  | Да има application firewall с вградено разпознаване на приложенията |  |
|  | Да поддържа филтриране на трафика чрез ACL |  |
|  | Да поддържа напълно автоматизирано първоначално провизиране - plug-and-play, zero touch plug&play и подобни за автоматично откриване и свързване към SD-WAN контролерите |  |
|  | Да поддържа управляеми IPSec топологии – hub-and-spoke, full mesh и комбинации между двете |  |
|  | Да поддържа отделна, виртуална, топология за всеки сегмент |  |
|  | Да поддържа следните протоколи за интеграция с външни мрежи:   * Static route * OSPF * BGP * VRRP |  |
|  | Да поддържа 802.1Q |  |
|  | Да поддържа IGMP v2 и v3 |  |
|  | Да поддържа минимум PIM SSM |  |
|  | Да поддържа PIM rendezvous point |  |
|  | Да поддържа статичен и динамичен NAT и NAT pool |  |
|  | Да поддържа изграждане на SD-WAN през NAT на външно устройство (CPE, Internet Gateway и подобни) – NAT overlay |  |
|  | Да поддържа QoS:   * Минимум 8 пакетни опашки на интерфейс * LLQ опашка * Управление на пакетните опашки с WRР или подобен алгоритъм * Управление 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 |  |
|  | Да поддържа packet duplication – изпращане на един пакет по два отделни маршрута до приемащия SD-WAN маршрутизатор |  |
|  | 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 |  |
|  | 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 |  |
|  | 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. |  |
|  | Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя; |  |
|  | Устройството да е окомплектовано с SDWAN лицензи за минимум 5Gbps WAN трафик |  |
| **Гаранция и поддръжка:** | |  |
|  | Срок на хардуерната гаранция - минимум 5 (пет) години. |  |
|  | Срок на техническа поддържка – минимум 5 (пет) години. |  |
|  | Получаване на нови версии на софтуера - минимум 5 (пет) години. |  |
|  | Срок на абонаментите за използване на софтуерни функции - ~~минимум~~ 5 (пет) години. |  |

* + 1. **Софтуер за управление на софтуерно дефинирана мрежа**

|  |  |  |
| --- | --- | --- |
| **Изискано от Възложителя** | | **Предложено от участника** |
| **А.** | | **Б.** |
| **Обща информация** | | |
|  | Софтуерни контролери за изграждане и управление на SDWAN мрежа с SDWAN маршрутизаторите в това задание. |  |
|  | Инсталация – върху VMWare ESXi на възложителя |  |
|  | Количество – съгласно изискванията на производителя за постигане на висока надеждност и резервиране на SDWAN контролната система |  |
|  | 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. |  |
|  | Управление на маршрутизаторите и техните функции в SDWAN мрежата чрез темплейти |  |
|  | Управление на услугите и виртуалните топологии в SDWAN мрежата чрез политики |  |
|  | Управление на транспортната IPSec топология чрез политики |  |
|  | Динамично управление на различни трафични класове през IPSec транспортната инфраструктура на база параметрите на тунелите – jitter, latency, загуба на пакети |  |
|  | Управление на IPS, application Firewall, URL Filter и Malware защитата в SDWAN машршрутизаторите с такива функции. |  |
|  | Наблюдение на SDWAN маршрутизаторите |  |
|  | Наблюдение на SDWAN IPSec транспортните тунели и техните параметри – минимум up/down, packet loss, jitter и delay |  |
|  | Наблюдение на трафичните параметри от различни класове приложения, които използват SD-WAN мрежата |  |
|  | Визуализация на маршрутите за различните класове трафик през SDWAN мрежата |  |
|  | Изграждане на карта с топологията на SD-WAN мрежата с овърлей върху географска карта на страната. |  |
|  | Визуализация на пътя на трафичните потоци, на ниво приложения, върху транспортните тунели. |  |
|  | Преодставяне на информация за QoS на трафичните потоци от приложенията |  |
|  | Исторически справки за трафичните потоци през SDWAN мрежата |  |
|  | Web GUI интерфейс |  |
|  | Role based access controll |  |
|  | Да поддържа SSO съвместимо с Microsoft ADFS |  |
|  | Да има REST API за интеграция с външни софтуерни системи |  |
| **Гаранция и поддръжка:** | |  |
|  | Срок на хардуерната гаранция - минимум 5 (пет) години. |  |
|  | Срок на техническа поддържка – минимум 5 (пет) години. |  |
|  | Получаване на нови версии на софтуера – минимум 5 (пет) години. |  |
|  | Срок на абонаментите за използване на софтуерни функции - минимум 5 (пет) години. |  |

* + 1. **Съвместимост на компоненти**

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

**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.*

1. **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.

1. **Условия на доставка**
   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.
   2. Приемането и предаването на изпълнението ще се осъществява въз основа на изискванията на договора за обществена поръчка.
2. **Условия на гаранционно обслужване**
   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.
   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.
   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.
3. **Срок на изпълнение** 
   1. Задължаваме се да извършим доставка на оборудването в срок до ……… 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.*

* 1. Срокът на гаранционно обслужване е ……..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.*

1. **Място на изпълнение**
   1. Потвърждаваме, че мястото на извършване на доставката е на територията на гр. София, като сме запознати, че ще бъде посочено в писмената заявка конкретния адрес на извършване на доставката.
   2. Гаранционното обслужване ще се извършва спрямо местонахождението на доставеното и инсталирано оборудване.
2. **Други изисквания** 
   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 …………………………………………………………… (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.*

* 1. 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:** | **………./ ………….. / ……….…..** |
| **Подпис и печат:** | **......................................................** |
| **Име и фамилия** | **......................................................** |
| **Длъжност** | **......................................................** |
| **Наименование на участника** | **......................................................** |

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. [↑](#footnote-ref-1)