Приложение № 2
към рамков договор МС-117/09.10.2024 г.

ЗАЯВКА по Рамков договор № МС-117 от 09.10.2024 г. (ПО-16-3093/09.10.2024 г. на ИО АД)		☒
ЗАЯВКА по Рамков договор № МС-117 от 09.10.2024 г. (ПО-16-3093/09.10.2024 г. на ИО АД) (актуализирана)		☐ [1]
Позиция от ПГ-2025 г.:	*№ по ред от ПГ*	*4*
Описание на проект съгласно ПГ:	*Надграждане на информационната и комуникационна инфраструктура*	
CPV код	*30233141-1* *32420000-0* *48600000-4* *48700000-5* *48730000-4*	
Рег. номер на писмо от МЕУ за утвърждаване на проекта /становище по проекта	МЕУ-17121/17.11.2025 г.	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**, *в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*		*1 630 940.00 лв. без ДДС*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*		*На части, след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка и издадена фактура за съответната доставка*
Плащане с акредитив или авансово ДА/НЕ		*ДА* *При невъзможност до края на бюджетната година дейността да бъде изпълнена цялостно или частично, Бенефициерът ще открие сметка за разплащане на дължимите суми*

[1] Отбелязва се в случай че заявката е актуализирана

	(неотменяем акредитив), която ще покрива срока за извършване на услугата
Документи за плащане с акредитив или авансово	*Документи за банката за усвояване на средствата – фактура, издадена от Изпълнителя, подписана от оторизираните представители на Администрацията на Министерския съвет и подписан приемно-предавателен протокол по чл.6 от договора за приемане на съответния етап*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*До 4 месеца от подписване на заявката*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**	*Неприложимо*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*	*На части, с подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на всяка извършена доставка и издадена фактура за съответната доставка*
Приложения: (*напр: технически параметри, образци на отчетни документи***)**	*Техническа спецификация*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.	
ЗАЯВКАТА е ИЗГОТВЕНА ОТ:	
Ръководител на проект по заявката от страна на БЕНЕФИЦИЕРА (напр: представител на дирекцията – Заявител):	*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:	
Координатор на договора от страна на ВЪЗЛОЖИТЕЛЯ:	*Подпис:*
Ръководител на договора от страна на БЕНЕФИЦИЕРА:	*Подпис:*

ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Ръководител на проект по заявката		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		*Подпис:*

Забележка: *С една заявка могат да се възлагат повече от един проект по ПГ, само когато те са еднотипни и управлението им (възлагане, изпълнение, отчитане) може да се извършва съгласно описаните в таблицата от заглавната страница на заявката параметри и лица. В този случай в таблицата се добавят необходимия брой редове, за описване на съответните проекти. Когато проектите не са еднотипни, те се възлагат с отделни заявки.*

Приложение №1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

За

Надграждане информационната и комуникационна инфраструктура на АМС

Гр.София, 2025 г.

I. ЦЕЛ

Целта на настоящия документ е да опише изискванията към изпълнението на проект със заявка по ред 4 от ПГ2025 Актуализация 3.

II. ОБХВАТ

В обхвата на заявката е включена доставката на следното оборудване за нуждите на АМС:

1. **Комутатор тип 1 – 4 броя**

Минимални технически изисквания	
REQ.1.	Токозахранване – вградено, 100-240VAC.
REQ.2.	Безшумна работа.
REQ.3.	Слот за SD карта.
REQ.4.	12 порта 100/1000BASE-T, два ъплинк порта 1000BASE-T и два ъплинк порта SFP+ (10GE).
REQ.5.	802.3af и 802.3at PoE с обща мощност 240W.
REQ.6.	Осигуряване на PoE захранване без прекъсване при рестарт на комутатора.
REQ.7.	USB порт.
REQ.8.	Конзолен порт.
REQ.9.	Хардуерно IP forwarding и комутиране със следните параметри: - Производителност – минимум 68Gbps. - Forwarding – минимум 50Mpps. - MAC адреси – 32000. - IPv4 маршрути – 4000. - IPv6 маршрути – 2000. - Мултикаст маршрути – 1000. - SVI интерфейси – 512. - Пакетни буфери – 6MB.
REQ.10.	DRAM - 4GB.
REQ.11.	802.1AE с 128 битово криптиране.
REQ.12.	Jumbo frames - 9198 байта.
REQ.13.	Експортиране на трафична информация за 16000 трафични потока чрез един от следните протоколи - IPFIX, NetFlow, JFlow, sFlow или еквивалентен протокол.
REQ.14.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.15.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.16.	Класифициране на мрежовите потоци на ниво приложение.
REQ.17.	Рутинг протоколи: - RIPv2 и RIPng. - OSPF и OSPFv3 до 1000 маршрута - VRRP. - Рутиране на база политики.
REQ.18.	IEEE 802.3ad LACP протокол.

Минимални технически изисквания	
REQ.19.	IEEE 802.1AB (LLDP) или LLDP-MED.
REQ.20.	QoS със следните функции: - HQoS. - 8 изходящи пакетни опашки на всеки порт. - Групиране на трафика в трафични класове на база Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка. - Traffic policing. - Traffic shaping. - Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. - Поддръжка на две приоритетни опашки (PQ) на порт. - Поддръжка на Weighted Tail Drop (WTD) или еквивалентен алгоритъм за управление на задръствания. - Поддръжка на Weighted Random Early Detection (WRED) или еквивалентен алгоритъм за предотвратяване на задръствания. - DSCP и 802.1p маркиране на трафика на база трафични политики.
REQ.21.	Изолиране на потребителите от един и същ VLAN.
REQ.22.	Идентификация и оторизация на достъпа: • 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL. • MAC authentication bypass. • Идентификация чрез вграден Web портал. • 802.1x идентификация на повече от едно устройство на комутаторен порт. • 802.1x Multi-Domain идентификация.
REQ.23.	Хардуерно реализирани листи за филтриране на трафика, на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове.
REQ.24.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.25.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.26.	DHCP Snooping или еквивалентен метод.
REQ.27.	DHCP опция 82.
REQ.28.	Dynamic ARP inspection или еквивалентен метод.
REQ.29.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.30.	Автоматично запаметяване на използвания от първото клиентското у-во MAC адрес и блокиране на мрежовия достъп за други устройства, които се свързват към същия порт.
REQ.31.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.32.	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
REQ.33.	Протоколи и функции за управление и наблюдение: - Web GUI. - CLI. - DNS. - TFTP. - FTP.

Минимални технически изисквания	
	- NTP. - SSHv2 и SNMPv3. - Вграден DHCP сървър. - Traffic policing за контролиране на трафика до контролната система на комутатора. - Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. - API интерфейс с поддръжка на RESTCONF и NETCONF. - YANG дейта модели.
Гаранция, поддръжка и лицензи:	
REQ.34.	Хардуерна гаранция за срок от 5 (пет) години.
REQ.35.	Техническа поддръжка за срок от 5 (пет) години.
REQ.36.	Получаване на нови версии на софтуера за срок от 5 (пет) години.

2. Комутатор тип 3 – 1 брой

Минимални технически изисквания	
REQ.1	Монтаж - в 19“ шкаф.
REQ.2	Токозахранване – модулно, с два токозахранващи модула, AC.
REQ.3	Вентилатори – модулни.
REQ.4	24 порта 100/1000BASE-T и осем порта SFP+ за 1GE и 10GE SFP и SFP+ модули.
REQ.5	Вграден хардуерен порт за стеково свързване с производителност 480Gbps.
REQ.6	Да поддържа изграждане на стек от 8 комутатора.
REQ.7	Обща захранваща шина за споделяне на захранването между 4 комутатора.
REQ.8	Брой USB портове – 1.
REQ.9	Сериен конзолен порт – 1.
REQ.10	Изолиране на потребителите от един и същ VLAN.
REQ.11	Идентификация и оторизация на достъпа: • 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL. • MAC authentication bypass . • Идентификация чрез вграден Web портал. • Комбиниране на методите за идентификация на един порт – 802.1x, MAC адрес, WEB идентификация. • RADIUS CoA. • 802.1x идентификация на повече от едно устройство на комутаторен порт. • 802.1x Multi-Domain идентификация.
REQ.12	Хардуерно реализирани листи за филтриране на трафика, на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове.
REQ.13	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ.14	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ.15	802.1AE с 256 битово криптиране
REQ.16	DHCP Snooping или еквивалентен метод.
REQ.17	DHCP опция 82.
REQ.18	Dynamic ARP inspection или еквивалентен метод.
REQ.19	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ.20	Автоматично запаметяване на използвания от първото клиентското у-во MAC адрес и блокиране на мрежовия достъп за други устройства, които се свързват към същия порт.

REQ.21	Spanning Tree защити - BPDU Guard и Root Guard.
REQ.22	Хардуерен модул за удостоверяване автентичността на хардуера и софтуера чрез използване на криптографски методи.
REQ.23	Хардуерен IP forwarding и комутиране със следните параметри: • Производителност – минимум 200Gbps. • Forwarding – минимум 150Mpps. • MAC адреси – 32000. • IPv4 маршрути – 32000. • IPv6 маршрути – 16000. • Multicast маршрути – 8000. • 1000 активни VLAN. • SVI интерфейси – 1000. • Пакетни буфери – 16MB.
REQ.24	DRAM - 8GB.
REQ.25	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: • Рутиране. • STP. • 802.3ad.
REQ.26	Непрекъснато комутиране при извършване на SSO.
REQ.27	Jumbo frames - 9198 байта.
REQ.28	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ.29	Функция Private VLAN.
REQ.30	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ.31	Рутинг протоколи: • RIP, RIP-NG. • OSPFv2 и OSPFv3. • BGP. • IS-IS. • IGMPv2 и IGMPv3 snooping. • Мултикаст рутиране с PIM-SM и PIM-SSM. • Рутиране на база политики. • Виртуализация на рутинг таблици и протоколи VRF lite или еквивалент. • VRRP.
REQ.32	IEEE 802.3ad LACP протокол.
REQ.33	IEEE 802.3ad групи с портове от различни комутатори в един стек.
REQ.34	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ.35	Класифициране на трафичните потоци на ниво приложения.
REQ.36	QoS със следните функции, като минимум: • HQoS. • 8 изходящи пакетни опашки на всеки порт. • Групиране на трафика в трафични класове на база Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка. • Traffic policing. • Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR, PIR и burst параметри. • Traffic shaping.

	• Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. • Поддръжка на две приоритетни опашки (PQ) на порт. • Поддръжка на Weighted Tail Drop (WTD) или еквивалентен алгоритъм за управление на задръствания. • Поддръжка на Weighted Random Early Detection (WRED) или еквивалентен алгоритъм за предотвратяване на задръствания. • DSCP и 802.1p маркиране на трафика на база трафични политики.
REQ.37	MPLS с поддръжка на L3 VPN и VPLS.
REQ.38	BGP EVPN с VXLAN или еквиваленти функции и протоколи за изграждане на SDN фабрика.
REQ.39	Протоколи и функции за управление и наблюдение: • Web GUI. • CLI. • RMON. • IPv4/v6 ping. • DNS. • TFTP. • FTP. • NTP клиент и сървър. • SSHv2 и SNMPv3. • Експортиране на трафична информация за 60000 трафични потока чрез IPFIX, NetFlow, JFlow или еквивалентен протокол към външна система за трафичен анализ. • Вграден DHCP сървър. • Конфигурация в отделен конфигурационен файл. • Задаване ниво на достъп до системата за всеки администратор. • Работа с външна система за съхраняване на изпълнените от всеки администратор команди. • Traffic policing за контролиране на трафика до контролната система на комутатора. • Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. • Отделен Ethernet порт за out of band управление и наблюдение. • API интерфейс с поддръжка на gNMI, RESTCONF и NETCONF. • YANG дейта модели. • Възможност за инсталиране на софтуерни контейнери.
REQ.40	Комплект планки за монтаж в 19“ шкаф, стеков кабел, кабел за изграждане на захранваща шина, захранващи кабели.
REQ.41	Устройството е окомплектовано със съответните лицензи и права за използване според условията на производителя.
REQ.42Гаранция и поддръжка:	
REQ.43	Хардуерна гаранция за срок от 5 (пет) години.
REQ.44	Техническа поддръжка за срок от 5 (пет) години.
REQ.45	Получаване на нови версии на софтуера за срок от 5 (пет) години.

3. Комутатор тип 4 – 1 брой

Минимални технически изисквания	
REQ.1	Тип на кутията/шасито - за монтаж в 19“ шкаф
REQ.2	Захранване – модулно, с минимум два токозахранващи модула за резервиране, 220-240v AC, 50Hz
REQ.3	Минимум 48 порта поддържащи 100M / 1G Base-T (RJ45) интерфейса
REQ.4	Да притежава минимум 4 порта поддържащи 10G SFP+ порта
REQ.5	Брой USB портове - минимум 1
REQ.6	Да поддържа изолиране на потребителите от един и същ VLAN
REQ.7	Да поддържа 802.1X на всички портове за потребители
REQ.8	Да поддържа 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL.
REQ.9	Да поддържа идентификация на база MAC адреси
REQ.10	Да поддържа идентификация чрез вграден Web портал
REQ.11	Да поддържа комбиниране на методите идентификация на един порт – 802.1x, MAC адрес, WEB идентификация.
REQ.12	Да поддържа RADIUS CoA
REQ.13	Да поддържа хардуерно реализирани листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове
REQ.14	Да поддържа 802.1AE 128 битово криптиране на всички портове
REQ.15	Да поддържа автоматично инспектиране на DHCP трафика със следните функции: • блокиране на DHCP заявки с разлика в MAC адреса на Ethernet фрейма и MAC адреса в DHCP заявката. • блокиране на DHCP пакети за освобождаване на адрес или отказ, които идват от порт различен от този, през който е получен IP адреса. • Защита от IP Spoofing
REQ.16	Да поддържа автоматично запаметяване на използвания от клиентското у-во MAC адрес и да блокира мрежовия достъп за други устройства свързвани към същия порт
REQ.17	Да поддържа игнориране на BPDU пакети получавани от клиентски портове
REQ.18	Да подържа възможност за игнориране на STP root bridge информация през неоторизирани портове
REQ.19	Да поддържа криптографски метод за проверка на автентичността на използвания софтуер
REQ.20	Хардуерно маршуритизиране за IPv4 и IPv6 със следните параметри, като минимум: • Производителност – минимум 170Gbps • Forwarding – минимум 130Mpps • Брой IPv4 и IPv6 маршрута – общо 4500 • Multicast маршрути - 1000 • SVI интерфейси - 500 • Пакетни буфери – 6MB
REQ.21	DRAM - минимум 2GB DRAM
REQ.22	Да има възможност да поддържа стекове свързване между минимум осем устройства чрез използване на стак портове с капацитет от 80Gbit
REQ.23	Да поддържа Statefull Switch Over (SSO) между комутатори в един стек
REQ.24	MAC адреси – минимум 16000
REQ.25	Да поддържа Jumbo frames от поне 9198 байта
REQ.26	Да поддържа енкапсулация на трафика във VXLAN чрез допълнителен лиценз
REQ.27	Spanning Tree – IEEE 802.1d, 802.1w и 802.1w
REQ.28	Да поддържа следните протоколи за маршрутизация: • Статично маршрутизиране за IPv4 и IPv6 • OSPFv2 и OSPFv3 до 1000 маршрута

	• Мултикас маршрутизиране с PIM-SM и PIM-SSM • Маршрутизиране на база политики • VRRP
REQ.29	Да поддържа IEEE 802.3ad LACP протокол
REQ.30	Да поддържа IEEE 802.3ad групи с портове от различни комутатори в един стек
REQ.31	Да поддържа LLDP или подобен
REQ.32	Да поддържа класифициране на трафичните потоци на ниво апликациите посредством вградена DPI система чрез допълнителен лиценз
REQ.33	Да поддържа QoS със следните функции, като минимум: • Минимум 8 изходящи пакетни опашки на всеки порт. • Групиране на трафика в трафични класове на база произволни комбинации от Layer2, Layer 3, Layer 4 и Layer 7 трафични параметри, 802.1p и DCSP маркировка • Traffic policing на база трафични класове • Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и Commited Burst параметри. • Traffic shaping на база трафични класове • Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всяка опашка, като процент от пропускателната способност на интерфейса • Управление на пакетните опашки чрез задаване на минимално гарантирана скорост за всяка опашка. • Поддръжка на приоритетна опашка (PQ) • Поддръжка на Weighted Tail Drop (WTD) алгоритъм за предотвратяване на задръствания • DSCP и 802.1p маркиране и премаркиране на трафика на база трафични политики
REQ.34	Да поддържа изграждането на софтуерно управлявани виртуални мрежи чрез допълнителен лиценз
REQ.35	Да поддържа динамична сегментация на потребителите на база минимум MAC адреси, профилиране на потребителското устройства и 802.1x удостоверяване на идентичност
REQ.36	Да поддържа минимум следните методи за управление и наблюдение: • Управление чрез конзола и GUI • RMON. • IPv4/v6 ping • DNS • TFTP • FTP • NTP клиент и сървър • SSHv2 и SNMPv3 • Експортиране на трафична информация за минимум 16000 трафични потока чрез IPFIX, Netflow, JFlow или подобен протокол към външна система за трафичен анализ • Конфигурация в отделен конфигурационен файл, който позволява бързо и лесно преместване на конфигурацията върху ново у-во • Задаване ниво на достъп до системата за всеки администратор.

	• Работа с външна система за съхраняване на изпълнените от всеки администратор команди • Traffic policing за контролиране на трафика до контролната система на комутатора • Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. • Отделен Ethernet порт за out of band управление и наблюдение на устройството • Да поддържа NETCONF/YANG интерфейс
REQ.37	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя
REQ.38	Устройството да е окомплектовано с необходимите планки за монтаж в 19“ шкаф и кабели.
Гаранция и поддръжка:	
REQ.39	Срок на хардуерната гаранция - минимум 5 (пет) години.
REQ.40	Срок на техническа поддържка – минимум 5 (пет) години.
REQ.41	Получаване на нови версии на софтуера - минимум 5 (пет) години.

4. Система за защита на DNS трафик

Минимални технически изисквания	
REQ.1	DDI Системата (DNS, DHCP & IP Address Management) трябва да бъде доставена като готов за използване OVA образ с възможност за интегриране във VMware среда, която АМС вече притежава.
REQ.2	Системата трябва да предоставя услуга за управление на IP адреси – IPAM (IP Address Management)
REQ.3	Системата трябва да разполага с механизми за контрол на въвежданите данни (коректност на IP адреси, маски и др.)
REQ.4	Системата трябва да позволява добавяне на описания и атрибути за мрежови обекти, IP адреси, домейни. Тези атрибути трябва да имат възможност за дефиниране на типа и размера им
REQ.5	Системата трябва да поддържа механизъм за сканиране на мрежи и хостове/IP адреси (т.нар. network discovery)
REQ.6	Системата трябва да поддържа функции като „намери 10 неизползвани адреса от мрежа X“ и „намери 10 неизползвани подмрежи с размер напр. /24 в подмрежа напр. abcd/16“. Функцията трябва да бъде налична за IPv4 и IPv6
REQ.7	Системата трябва да позволява импортиране на данни в CSV формат директно от графичния интерфейс и да разполага с подробна документация за формата на импортираните данни
REQ.8	Капацитетът на DNS/DHCP/IP базата данни трябва да бъде за минимум 100000 записа.
REQ.9	Системата трябва да позволява интеграция с VMware vCenter и OpenStack услуги, за да извършва процес на откриване на виртуални машини, работещи във VMware/OpenStack инфраструктура, и автоматично да създава DNS записи за тези машини
REQ.10	Системата трябва да поддържа внедряване на DHCP услуги за IPv4 и IPv6 с минимална производителност от 200 DHCP leases в секунда
REQ.11	Системата трябва да поддържа актуализиране на DDNS данни чрез DHCP услугата
REQ.12	Системата трябва да поддържа актуална информация за разпределените IP адреси и устройствата, на които е присвоен даден адрес (MAC адрес, време и дата на присвояване на адреса, IP)
REQ.13	Системата трябва да поддържа функционалност DHCP Failover с възможност за повторно договаряне на наличните адресни пространства
REQ.14	Трябва да бъде възможно проверката за наличност на IP адрес преди

	неговото разпределяне чрез ICMP
REQ.15	Системата трябва да разпознава типа на устройството/системата на станции, мобилни устройства и др. въз основа на анализа на DHCP заявката. Трябва да поддържа отчет за типа на устройството в историята на DHCP наемите и да предоставя възможност за филтриране/блокиране на разпределението на адреси за избрани типове устройства (напр. разпределяне на адрес за Windows станция, но не и за таблет или смартфон)
REQ.16	Системата трябва да предоставя авторитетни и рекурсивни услуги за разрешаване на домейн имена (DNS - Domain Name System)
REQ.17	Производителността на авторитетния DNS трябва да бъде поне 10 000 DNS заявки в секунда
REQ.18	Системата трябва да изпълнява автоматични DNS актуализации в съответствие с RFC 2136
REQ.19	Системата трябва да разполага с вграден механизъм за уведомяване при промени в зоните, в съответствие с RFC 1996
REQ.20	Системата трябва да поддържа DNS протоколи както за IPv4, така и за IPv6
REQ.21	Системата трябва да поддържа DNS Anycast услуга за IPv4 и IPv6 (използвайки BGP и OSPF протоколи)
REQ.22	Системата трябва да поддържа DNSSEC услуга с автоматично обновяване на подписите при промени в DNS зоните
REQ.23	Системата трябва да поддържа DDNS услуга
REQ.24	Системата трябва да поддържа защитено обновяване на DNS записи с поддръжка на GSS-TSIG протокол
REQ.25	Системата трябва да поддържа MultiMaster DNS функционалност
REQ.26	Системата трябва да поддържа механизъм за IDN (Internationalized Domain Names) и да разполага с вграден конвертор за punycode (поддръжка на кирилица)
REQ.27	Системата трябва да поддържа IDN за DNSKEY записи, DS записи, NSEC записи, NSEC3PARAM записи и RRSIG записи
REQ.28	Системата трябва да поддържа EDNS0 разширения съгласно стандарта RFC 6891
REQ.29	Системата трябва да поддържа следните алгоритми за публични ключове, използвани с DNSSEC: DSA, RSA/MD5, RSA/SHA1, RSA/SHA-256, RSA/SHA-512, ECDSAP/SHA-256, ECDSAP/SHA-384
REQ.30	Подписаните с DNSSEC зони трябва да поддържат динамични DNS актуализации
REQ.31	Системата трябва да поддържа автоматично подписване на DNS записи след промени
REQ.32	Системата трябва да функционира като платформа за разпространение на файлове чрез протоколите TFTP, FTP, HTTP и да предлага услуги за синхронизация на времето чрез NTP (Network Time Protocol)
REQ.33	Системата трябва да работи под контрола на специализирана операционна система. Използването на операционни системи с общо предназначение не е разрешено. Тя не трябва да зависи от или да изисква конкретни версии на операционни системи с общо предназначение или програмни библиотеки
REQ.34	Управлението на системата трябва да се осъществява чрез уеб браузър, без да е необходимо инсталирането на допълнителен софтуер като агент, клиент и др
REQ.35	Възможност за управление от няколко системни администратори, вписани едновременно
REQ.36	Системата трябва да предоставя възможност за управление на IPv4 и IPv6 адреси, позволявайки графичен, конзолен, и API интерфейси

REQ.37	Системата трябва да поддържа удостоверяване на потребители чрез: - Локална потребителска база - RADIUS протокол - TACACS+ протокол - LDAP - Microsoft Active Directory
REQ.38	Системата трябва да има вградена база данни за съхранение на DDI информация. Базата данни не трябва да изисква поддръжка, свързана с нейната конфигурация и управление
REQ.39	Системата трябва да може да бъде наблюдавана чрез SNMP (Simple Network Management Protocol)
REQ.40	Системата трябва да позволява планирани резервни копия (backups) към външен сървър, за да улесни възстановяването в случай на бедствие (чрез TFTP, FTP, SCP)
REQ.41	Системата трябва да поддържа интеграция с инструменти за управление на конфигурацията като Ansible, Puppet и Chef
REQ.42	Системата трябва да поддържа възможност за импортиране и експортиране на данни в различни формати, включително CSV и JSON
REQ.43	Устройството трябва да разполага с функционалност за разпознаване и блокиране на DNS тунелиране чрез аналитичен механизъм, базиран на машинно обучение, който разпознава неизвестни модели на тунелиране и извличане на данни чрез DNS. Системата трябва да анализира поне 10 атрибута на всяка DNS заявка, включително: ентропия на символите във FQDN, популярност на дву- и трибуквени комбинации, съотношение на гласни в FQDN, съотношение на цифри, размер на заявката, честота и промяна на честотата на DNS заявките
REQ.44	Системата трябва да разполага с функционалност за откриване на прониквания през DNS, по-специално трябва да разпознава техниката, използвана от зловредния софтуер Powersource/DNS Messenger, и да блокира опити за пренос на данни, кодирани в DNS отговори чрез TXT записи
REQ.45	Системата трябва да разполага с функционалност Response Policy Zones (RPZ) за работа като DNS защитна стена въз основа на списъци с опасни домейни
REQ.46	Системата трябва да регистрира и предоставя информация за всички промени, направени от администратори (кой, кога, какво е променил)
REQ.47	Системата трябва да може да изпраща логове към централен хранилищен сървър чрез Syslog механизъм (TCP и UDP)
REQ.48	Системата трябва да позволява администраторите да имат права, базирани на групи и роли, които ограничават достъпа им само до необходимите ресурси. Подробните разрешения трябва да позволяват конфигуриране на права за отделни обекти, като мрежи, DNS зони и конкретни DNS записи.
REQ.49	Системата трябва да поддържа криптирана комуникация между компонентите си чрез TLS (Transport Layer Security)
REQ.50	Достъпът до административния интерфейс трябва да бъде защитен чрез двуфакторна автентикация (2FA)
REQ.51	Системата трябва да предоставя механизъм за защита срещу неоторизиран достъп чрез прилагане на списъци за контрол на достъпа (ACL)
REQ.52	Системата трябва да поддържа защита от атаки тип DDoS срещу DNS и DHCP услуги
REQ.53	Системата трябва да поддържа механизъм за мониторинг и алармиране при откриване на аномалии в мрежовия трафик, свързан с конфигурираните услуги
REQ.54	Системата трябва да има възможност за запис и анализ на потребителските сесии в административния интерфейс за целите на одит и сигурност
REQ.55	Системата трябва да поддържа криптиране на чувствителни данни в

	конфигурационните файлове и базата данни
REQ.56	Системата трябва да позволява дефиниране на политики за автоматично деактивиране на потребителски акаунти при откриване на подозрителна активност
REQ.57	Услугата трябва да има възможност да предприема действия по DNS заявки и отговори въз основа на дефинирани от клиента правила за защита - Възможните действия трябва да включват: разрешаване на заявка без регистриране, разрешаване на заявка с логиране, блокиране на заявка с NXDomain отговор (няма такъв домейн), пренасочване (отговор с дефиниран IP адрес). Пренасочването трябва да е възможно към уеб страница, предоставена от доставчика. Системата трябва също така да позволява пренасочване към всеки IP адрес. - Системата трябва да предприеме действия въз основа на името на домейна в заявката и въз основа на IP адреса в отговора. Действието върху името на домейн трябва да работи за всеки тип заявка – системата не трябва да позволява заобикаляне на блокирането чрез изпращане на специфични типове заявки като SOA или NS. Системата не трябва да позволява заобикаляне на блокирането на злонамерен домейн чрез изпращане на запитвания с главни или смесени FQDN (DNS протоколът е нечувствителен към малки и големи букви, а сигурната DNS система също трябва да е нечувствителна към малки и големи букви - Системата трябва да позволява да се дефинира персонализиран списък с домейни/IP адреси, по които да се действа, и също така трябва да предоставя списък с домейни и IP адреси под формата на емисии за заплахи, дефинирани по-долу. За персонализирани списъци системата трябва да има възможност да дефинира нивото на заплаха и увереността на заплахата за всеки списък. Системата трябва да позволява създаване и редактиране на персонализирани списъци от клиентския портал, както и чрез API, за да позволи лесно импортиране на персонализирани данни за заплахи. - Системата трябва да предоставя възможност за заобикаляне на блокове със специфични кодове, предоставени на избрани потребители
REQ.58	Трябва да е възможно изпращането на DNS заявки към услуга предоставяща функции за категоризирането и филтрирането им - от персонализирано дефинирана IP мрежа - от DMZ DNS сървъри, сървърите трябва да добавят вътрешен IP адрес на клиента вътре в заявките и да ги изпращат в криптирана форма към услугата - От роуминг агент, предоставен от доставчика. Роуминг агентът трябва да бъде предоставен за Windows, Mac OS, Android и iOS Данните за заплахите, предоставени от доставчика, трябва да включват - списък на интернет домейни, свързани с APT атаки - списък с домейни и IP адреси, свързани със злонамерен софтуер - Списък с домейни, свързани с рансъмуер - списък с IP адреси, свързани с ботнет мрежи - списък на домейните, свързани със злонамерен софтуер, с помощта на алгоритми за генериране на домейни (DGA) - списък с IP адреси на изходните възли на TOR мрежата - списък с домейни, свързани с фишинг - списък на домейните, свързани с неоторизирано копаене на криптовалута - списък на домейните, регистрирани през последните три дни. Данните за новите регистрации трябва да идват от най-малко 500 различни домейна от първо ниво (домейни от първо ниво). - Списък на домейни, които споделят подозрителни характеристики като примерни домейни, са регистрирани по едно и също време от същия регистрант, който в миналото е регистрирал домейни, за които е доказано, че са свързани със злонамерена дейност

REQ.59	Всички горепосочени списъци за заплахи трябва да бъдат налични за конфигуриране в политиката за защитени DNS услуги, както и във формат RPZ, за да бъдат изтеглени на DNS сървърите
REQ.60	Списъците за заплахи от доставчика трябва да бъдат достъпни чрез API във формати CSV, STIX, XML, JSON и CEF за използване в други системи за сигурност като SIEM, защитни стени или защитени уеб шлюзове
REQ.61	Разузнаването на заплахите трябва да може да предоставя контекстуална информация за домейн/IP, поне трябва да включва данни, ако заплахата е свързана с ексфилтрация на данни, влияе ли върху наличността на системите, необходимо ли е взаимодействие с потребителя за активиране на заплахата, какви техники са включени
REQ.62	Защитената DNS услуга трябва да има функционалността за откриване и блокиране на DNS тунелиране с помощта на аналитичен алгоритъм, базиран на машинно обучение и позволяващ откриване на неизвестни модели на тунелиране и ексфилтрация на данни през DNS. Системата трябва да анализира поне 10 атрибута на всяка DNS заявка и това трябва да включва: ентропия на знаците в FQDN, оценяване на всеки набор от 2 и 3 знака за популярност в естествените езици, изчисляване на съотношението на гласните в FQDN, изчисляване на съотношението на цифрите в FQDN, анализиране на размера на заявката, анализиране на честотата на DNS заявките (стойност на честотата и промяна на честотата). Защитената DNS услуга трябва да открива DNS тунелиране, независимо от категорията на съдържанието на домейна, използван в DNS заявката
REQ.63	Защитената DNS услуга трябва да има функционалност за откриване на непознати DGA и DGA домейни в DNS заявки
REQ.64	Защитената DNS услуга трябва да има информация за категорията съдържание за домейни и трябва да може да действа по нея, например трябва да предоставя възможност за предприемане на действия за домейни, хостващи съдържание като порнография, опасност, социални мрежи, анонимайзери и др.
REQ.65	Системата трябва да поддържа механизми за висока наличност (High Availability - HA) за всички основни услуги, включително DNS, DHCP и IPAM
REQ.66	Системата трябва да поддържа клъстеризация на компонентите си с цел осигуряване на надеждност и отказоустойчивост
REQ.67	Системата трябва да позволява автоматично превключване (failover) при отпадане на даден сървър или услуга
REQ.68	Системата трябва да поддържа географски разпределено внедряване с възможност за репликация на данни между различни локации
REQ.69	Системата трябва да има механизъм за автоматично балансиране на натоварването (load balancing) между DNS и DHCP сървърите
REQ.70	Системата трябва да осигурява непрекъсната работа при актуализации (Rolling Updates), без да се нарушава функционирането на критичните услуги
REQ.71	Системата трябва да позволява възстановяване след срив (Disaster Recovery) чрез механизъм за архивиране и репликация на данни
REQ.72	Системата трябва да поддържа синхронизация на конфигурацията и данните между главните и резервните инстанции в реално време
REQ.73	Бързо възстановяване на услугите в случай на срив, като времето за възстановяване не трябва да надвишава 10 минути.
REQ.74	Системата трябва да предоставя централизирана отчетност за всички DNS, DHCP и IPAM събития
REQ.75	Системата трябва да поддържа механизъм за събиране и анализ на логове, включително възможност за интеграция с SIEM (Security Information and Event Management) решения
REQ.76	Системата трябва да позволява генериране на персонализирани отчети за използването на IP адреси, DHCP лизинги и DNS заявки

REQ.77	Системата трябва да осигурява механизъм за известяване на администраторите чрез имейл, SNMP трап (trap) или уеб интерфейс при откриване на критични събития
REQ.78	Системата трябва да предоставя детайлни статистики за производителността на DNS и DHCP услугите, включително натоварване, време за отговор и брой заявки
REQ.79	Системата трябва да позволява интеграция със системи за мрежов мониторинг чрез SNMP (v2c и v3)
REQ.80	Системата трябва да предоставя исторически данни за заетостта на IP адресите и тенденциите на използване
REQ.81	Системата трябва да поддържа механизъм за автоматично архивиране на логове и отчети за последващ анализ
REQ.82	Системата трябва да позволява конфигуриране на политики за съхранение и изтриване на исторически данни
REQ.83	Системата трябва да може да визуализира информацията чрез графики и диаграми в уеб интерфейса
REQ.84	Порталът за защитени DNS услуги трябва да предоставя възможности за отчитане. Докладите трябва да включват: - Отчети за дейността, показващи DNS заявки, изпратени до услугата - Отчети за защитата, показващи DNS заявки, които засягат правилата за сигурност - Трябва да има възможност за изпращане на изходни данни (заявки, събития за защита) до локална SIEM система под формата на съобщения в системен дневник или директна интеграция
REQ.85	Достъпът до клиентския портал трябва да се основава на потребителски данни за вход със специфични роли за достъп, като например достъп само за четене или административен достъп. Промените в конфигурацията на DNS услугата трябва да бъдат регистрирани в регистрационния файл за проверка.
REQ.86	Висока производителност с минимално време за отговор на DNS заявки (не по-високо от 50 милисекунди) при натоварване до 5 хиляди заявки на секунда.
REQ.87	Поддържка на DHCP услуги с производителност минимум 200 заявки на секунда.
REQ.88	Надеждност при обработка на големи обеми данни и да не претоварва мрежовата инфраструктура при високи натоварвания.
REQ.89	Възможност за работа с разширени DNS записи и поддържа функционалности като DNSSEC и Anycast без да се нарушава производителността.
REQ.90	Възможност за обработка на натоварвания, които включват обработка на над 30 милиона DNS заявки и DHCP лизинги месечно.
REQ.91	Възможност за динамично регулиране на ресурсите според натоварването, включително за работа в облачни среди и виртуализирани инфраструктури.
REQ.92	Възможност за интелигентно управление на натоварването и оптимизация на ресурсите чрез използване на технологии като load balancing и autoscaling.
REQ.93	Да бъде в състояние да обслужва нуждите на организацията при неограничено нарастващ обем от мрежови услуги и данни, като остава стабилна и ефективна.
Поддръжка и лицензи	
REQ.94	Системата трябва да е лицензирана за минимум 500 потребителя.
REQ.95	DDI Системата трябва да е оразмерена и лицензиране за безпроблемна работа на поне 1000 IP адреса.
REQ.96	Поддръжка от производителя, включително получаване на нови версии на софтуера и 24/7 техническа помощ чрез телефон, имейл и портал за заявки за срок от минимум 60 (шестдесет) месеца.
REQ.97	Механизъм за известяване на администраторите за наличието на нови актуализации и критични поправки.

5. Система за защита на ниво приложение

Минимални технически изисквания	
REQ. 1.	Предложеното решение трябва да включва 2 броя лицензи за софтуер за мониториране и защита на мрежови приложения (WAF) за трафик от 1Gbps с валидност и включена поддръжка минимум за срок от 60 месеца.
REQ. 2.	Решението да позволява използването на минимално 8 виртуални устройства, като част от лиценза, които да могат да се поставят минимално на следните хипервайзори: VMware ESX и ESXi, KVM, Hyper-V.
REQ. 3.	Решението трябва да предоставя гъвкава пропускателна способност от минимално 10Mbps до 1Gbps, използвайки vSwitch функцията на даден хипервайзор, без да се налага използването на SR-IOV технология.
REQ. 4.	Решението трябва да поддържа възможности за ускорение на уеб приложения, минимално кеширане, компресия и модифициране на хедър (header).
REQ. 5.	Решението трябва да поддържа функция за мониториране на състоянието (Health Monitoring) на уеб трафика. Минимално да се поддържат следните протоколи за мониториране: ICMP, TCP и UDP, HTTP и HTPPS (като решението да може да маркира недостъпни в даден момент точки), LDAP и LDAPS, FTP, SNMP, DNS, IMAP4, NNTP, на ниво физически портове, POP3, RADIUS, RTSP, SMTP, чрез SSL Hello, на ниво UDP порт, SIP UDP/SIP TCP, OCSP.
REQ. 6.	Решението трябва да поддържа функция за бърза TCP проверка на състоянието (Health Check) на уеб трафика.
REQ. 7.	Решението трябва да поддържа проверки на състоянието на уеб трафика, базирани на L2 (ARP), L3 (PING) и L4 (TCP/UDP проверки на портове).
REQ. 8.	Решението трябва да предоставя предефинирани L7 проверки на състоянието на ниво приложение (HTTP, HTTPS, LDAP, SMTP и др.) и персонализиране на проверки за всякакви бинарни и текстово базирани протоколи.
REQ. 9.	Решението трябва да може да засича статуса на сървъри, на база събрани и обработени данни от проверки на състоянието.
REQ. 10.	Решението трябва да може да засича статуса на сървъри, на база зададени логически изрази при сравнение на данни от множество проверки на състоянието.
REQ. 11.	Решението трябва да може да засича претоварване на сървъри, чрез проверки на състоянието .
REQ. 12.	Решението трябва да позволява да се определя интервала на събиране на данни за мониториране.
REQ. 13.	Решението трябва да позволява да се определя максимално допустимо време без отговор при събиране на данни за мониториране (timeout interval).
REQ. 14.	Решението трябва да поддържа проверяване на състоянието на сървъри чрез външни скриптове, минимално Python-базирани.
REQ. 15.	Решението трябва да може да балансира трафика от уеб приложения на слоеве 4 до 7 от OSI модела, минимално на база използван протокол (TCP, UDP), IP адреси на източник/дестинация, съдържание на приложения (минимално URL адреси, бисквитки, хедъри, текст, HTML тагове, XML тагове, DNS домейн, тип заявка).
REQ. 16.	Решението трябва да може да балансира трафика минимално на база най-бърза връзка, количество входящ и изходящ трафик, брой едновременно свързани потребители, тежест, точки с най-малко свързвания.
REQ. 17.	Решението трябва да може да показва страница с информация за грешка при недостъпност на даден ресурс/application сървър. Страницата с информацията за грешката трябва да подлежи на конфигурация, включително относно графичните елементи в нея.
REQ. 18.	Решението трябва да разполага с функция за осигуряване на постоянна свързаност на мрежови сесии, минимално на база IP адрес на източник, бисквитки, ID на SSL сесия, IP хеширане.

REQ. 19.	Решението трябва да поддържа следните протоколи за рутиране, минимално: OSPF, OSPFv3, RIP 1 /RIP 2 и BGP-4.
REQ. 20.	Решението трябва да поддържа минимално следните функционалности: SSL offload, възможност да управлява SSL трафика на клиента, като прекъсва входящи SSL връзки и да изпраща заявки към сървъра в чист текст.
REQ. 21.	Решението трябва да поддържа възможност за пропускане на IP адреси на клиента до крайния сървър през SSL (възможност за работа на решението като прозрачно прокси).
REQ. 22.	Решението трябва да поддържа SHA2 (Secure Hashing Algorithm).
REQ. 23.	Решението трябва да поддържа управление на сървърни сертификати на ниво виртуална услуга (Virtual Service Level).
REQ. 24.	Решението трябва да поддържа използването на TLS версии 1.2 и 1.3.
REQ. 25.	Решението трябва да поддържа функции за TCP и HTTP мултиплексиране.
REQ. 26.	Решението трябва да поддържа HTTP компресиране.
REQ. 27.	Решението трябва да позволява селективно HTTP компресиране, за да избегне познати проблеми с компресирането в често използвани браузъри.
REQ. 28.	Решението трябва да поддържа функция за уеб кеширане в съответствие с RFC 2616 на HTTP 1.1.
REQ. 29.	Решението трябва да поддържа функция за оптимизиране на кешираните данни в клиентски браузър минимално чрез пренаписване на атрибути или чрез промяна на хедърите на обекти.
REQ. 30.	Решението трябва да позволява автоматично девалидиране на кеширани данни, базирано на дадено взаимодействие на потребителите с дадено уеб приложение.
REQ. 31.	Решението трябва да поддържа TCP оптимизиране.
REQ. 32.	Решението трябва да поддържа функция за ускоряване на доставянето на услуги в клетъчни и безжични среди.
REQ. 33.	Решението трябва да може да използва услуги за сигурност от облака на производителя, дори когато е разположено локално, минимално WAF защита, API откриване на активи, API защита, BOT управление и информация за активни атаки.
REQ. 34.	Решението трябва да поддържа OOP защита на приложения без пренасочване на трафик и без споделяне на SSL сертификати.
REQ. 35.	Решението трябва да поддържа възможност за използване на изолирана от Интернет WAAP технология при необходимост.
REQ. 36.	Решението трябва да поддържа защита от ботове, включително поддръжка на използване на Captcha механизъм.
REQ. 37.	Решението трябва да поддържа информация за активни хакери, под формата на списък, който се актуализира в реално време, позволявайки на решението да блокира хакери, преди те да предприемат злонамерени действия.
REQ. 38.	Решението трябва да поддържа използването на ACL списъци.
REQ. 39.	Решението трябва да поддържа функция за филтриране на мрежови пакети за контрол на достъпа.
REQ. 40.	Решението трябва да разполага с конзола за централизирано управление на всички негови компоненти и устройства. Конзолата да може да е достъпна през уеб-браузър.
REQ. 41.	Решението трябва да поддържа използването на SNMP версии 1,2 и 3.
REQ. 42.	Решението трябва да разполага с добре документиран API интерфейс за интегриране с персонализирани приложения.
REQ. 43.	Решението трябва да позволява изпращането на логове към сървър чрез Syslog. Минимално да се поддържат следните формати: BSD syslog-RFC3164 и IETF syslog-RFC5424.
REQ. 44.	Решението трябва да поддържа ролево-базирано управление. Минимално да могат да се лимитират правата на потребителите на решението да управляват: няколко устройства, конфигурацията на едно устройство, специфичен обект и неговата конфигурация или конкретен сървър.

REQ. 45.	Решението трябва да поддържа AAA модел на автентикация на отдалечени потребители, да се поддържат минимално RADIUS, TACACS+ и LDAP.
REQ. 46.	Решението трябва да поддържа използването на резервни методи за автентикация (например използване на локален акаунт), които автоматично да се активират, ако сървърът за отдалечената автентикация е временно недостъпен.
REQ. 47.	Решението трябва да поддържа функция за мониторирането на устройствата му и техните състояния в реално време.
REQ. 48.	Решението трябва да може да съхранява две инстанции на операционната си система, с възможност за активиране/деактивиране на която и да е от тях при необходимост.
REQ. 49.	Решението трябва да позволява вписването на множество администратори едновременно към конзолата за централизирано управление (минимално 5 администратора едновременно).
REQ. 50.	Решението трябва да поддържа инструмент за съветване при актуализации (upgrade на софтуера на решението), който автоматично да анализира конфигурацията на решението и да индикира необходимите стъпки, които трябва да се предприемат, преди актуализацията да се извърши.
REQ. 51.	Решението трябва да предоставя вградени инструменти за събиране на мрежови пакети (подобно на TCPdump).
REQ. 52.	Решението трябва да може да криптира всички пароли в конфигурационните му файлове.
REQ. 53.	Решението трябва да може да предоставя отчет/анализ на състоянието на уеб приложенията и статистика за всички управлявани устройства.
REQ. 54.	Решението трябва да може да предоставя анализи за производителността на уеб приложенията и управляваните устройства, като трябва да може да съхранява информация за минимум 3 месеца назад.
REQ. 55.	Решението трябва да може да предоставя информация за всяко приложение за внесено забавяне (latency) на ниво мрежа и на ниво приложение.
REQ. 56.	Решението трябва да позволява извличането на отчети в различни формати, минимално HTML и PDF.
REQ. 57.	Решението трябва да може да предоставя изглед (dashboard), показващ информация за транзакциите на до 150 уеб приложения.
REQ. 58.	Решението трябва да предоставя изглед (dashboard) с информация за транзакциите на всяко от уеб приложенията, минимално информация за GEO локация и използван браузър.
REQ. 59.	Решението трябва да може да идентифицира минимално аномалии в трафика, причини за проблеми с SSL и HTTP сесии, възникване на бавни отговори и причината за забавянето, както и да може да различава нормални транзакции от такива, свързани с атаки.
REQ. 60.	Решението трябва да поддържа „Топ 5“ класации за уеб приложения базирани на информацията от транзакции с тях. Минимално топ 5 имена на хостове, използвани методи, път за свързване, използвани браузъри, IP адреси на източници.
REQ. 61.	Решението трябва да може да балансира входящия и изходящ трафик измежду няколко ISP канала за комуникация.
REQ. 62.	Решението трябва да поддържа делегирането на поддомейн, който да служи за обработването на всички DNS заявки и multi-homed услуги.
REQ. 63.	Решението трябва да поддържа функция за групиране на няколко DNS сървъра.
REQ. 64.	Решението трябва да се предоставя чрез единен глобален лиценз, който да предоставя всички необходими функционалности и услуги.

REQ. 65.	Решението трябва да поддържа използването на локален лицензионен сървър, който да може да работи в online и в offline режим, като част от същия лиценз, елиминиращ необходимостта всяко устройство да трябва има достъп до Интернет при необходимост.
REQ. 66.	Решението трябва да предоставя опция за управление чрез глобален лицензионен сървър при необходимост, разположен в облака на производителя, без да се налага инсталирането на локален лицензионен сървър.
REQ. 67.	Решението трябва да предоставя възможност за разделяне на капацитета за трафик на глобалния общ лиценз измежду няколко локални такива, с възможност динамично да се променя капацитета на всяка инстанция.
Гаранция и поддръжка:	
REQ. 68.	Период на поддръжка: минимум 60 месеца
REQ. 69.	Тип поддръжка: 24x7x365
REQ. 70.	Възможност за обновление на софтуера в периода на поддръжката до последна актуална версия на производителя.

6. Система за одитиране на промени

Минимални технически изисквания	
REQ.1	Тип решение: софтуерно решение за класификация на данни в ИКТ за средите база данни, exchange, файлов сървър и SharePoint.
REQ.2	Тип лиценз: **абонамент, с включена поддръжка на решението за 60 месеца**
REQ.3	Брой лицензи: **за 450 потребителски акаунти/пощенски кутии**
REQ.4	Решението трябва да работи без да използва агенти, така че да не влияе негативно на производителността на системите и да не спира работния процес.
REQ.5	Решението трябва да събира информация от локални и от облачни приложения и да ги съхранява в защитен, централизиран архив, което да позволява използването на общи известия, търсене, отчитане и анализ.
REQ.6	Решението трябва да позволява на отговорните лица за риска и сигурността на данните и съответствието със стандарти и регламенти на организацията да предотвратят лични данни, медицинска информация, банкова информация и данни, съдържащи интелектуална собственост, да се съхраняват извън отредените за това места.
REQ.7	Решението трябва да предоставя предварително зададени правила за идентифициране на кои данни попадат под регламентите на GDPR, PCI DSS, HIPAA и GLBA, както и на PII, PHI, запис на данни, които са забранени по GDPR и запис на общи финансови данни.
REQ.8	Решението трябва да идентифицира дисковите дялове с най-висока концентрация на чувствителни данни и да открива всички данни тип лични идентифициращи данни, медицинска информация, банкова информация и данни съдържащи интелектуална собственост, които се намират извън защитените локации, така че да предоставя възможност да се реагира подобаващо.
REQ.9	Решението трябва да позволява на потребителите да модифицират предварително зададените правила за класифициране и да създават свои собствени такива.
REQ.10	Решението трябва да позволява на потребителите бързо да открият всички индексирани файлове, които съдържат зададени от потребителите ключови думи.
REQ.11	Решението трябва да се използва за статистически анализ от концепции с множество думи, за да се изградят сложни правила за класификация на данните, както предварително зададени, така и с възможност за изграждане на собствени такива правила.
REQ.12	Решението трябва да събира и да натрупва сложни метаданни, които не са базирани на фрази, приблизителност, ключови думи или предварително зададена таксономия, като по този начин се елиминира необходимостта да се ре-индексира цялото хранилище на данни, когато някое правило за класифициране е добавено или променено.
REQ.13	Решението трябва автоматично да засича, класифицира и индексира нови файлове и промени по настоящи файлове, без необходимост да трябва да се събират наново всички данни от хранилището.

REQ.14	Решението трябва да може да проверява, дали правата за достъп до чувствителни данни са в съответствие с корпоративните политики и наложените регулации и да спомага да се определи, кой ще може да ги достъпи.
REQ.15	Решението трябва да може да се управлява централизирано и да позволява централизирано създаване и управление на категории от данни и правила.
REQ.16	Решението трябва да поддържа разпознаване и класификация на данни в графични файлови формати като .pdf документи и изображения.
REQ.17	Решението трябва да поддържа класификация на мета данни.
REQ.18	Решението трябва да поддържа класификация на данни на бази от данни, минимално да се поддържат Microsoft SQL Server, MySQL, Oracle.
REQ.19	Решението трябва да поддържа класификация на данни на Microsoft Exchange сървър.
REQ.20	Решението трябва да поддържа класификация на данни на Windows файлов сървър.
REQ.21	Решението трябва да поддържа класификация на данни на SharePoint сървър.
REQ.22	Решението трябва да предоставя функция за поставяне на маркировка (тагове) на откритите файлове с класифицирани данни (директно в метаданните на файловете), така че да се улесни интеграцията с други решения, като например с решения за защита от изтичане на данни, които могат да използват таговете за създаване на политики за сигурност с по-голяма точност.
REQ.23	Решението трябва да предоставя функция за автоматично редактиране на класифицираните данни в откритите файлове с класифицирани данни, като данните да могат да се заменят с предварително дефиниран термин.
REQ.24	Решението трябва да има управление на системни отчети, които предоставят информация за състоянието на събирането и класифицирането на данни.
REQ.25	Решението трябва да има Dashboard за здравето на системата, като лесно да може да се достигне до конкретната детайлна информация, която е необходима, за да се отстранят проблемите.
REQ.26	Решението трябва да дава цялостен изглед над средата, като всички функционалности да са част от единна платформа, премахвайки необходимостта от използването на множество отделни решения.
REQ.27	Правата за достъп трябва да са ролево базирани. Платформата трябва да позволява фино разделяне на различните потребители, така че всеки от тях да има достъп само до необходимите му настройки.
REQ.28	Решението трябва да може да се интегрира с други решения, минимално с решение за одит на промени.
REQ.29	При интеграция с решение за одит на промени, да може да предоставя предварително зададени отчети, които предоставят детайлна информация за това, къде се намират чувствителните данни, какво е съдържанието им, кой може да ги достъпи и кой реално ги използва, както и до кои чувствителни файлове има излишни права за достъп от потребители. Възможност за абонамент към автоматични отчети, които периодично да се изпращат към посочени email адреси или споделени директории.
REQ.30	При интеграция с решение за одит на промени, да може да предоставя целия контекст покрай действията, свързани със защитената информация и да подсигурява, че потребителските действия, които застрашават целостта на тези данни, като например непозволени промени в правата за достъп, са засечени и докладвани.
REQ.31	При интеграция с решение за одит на промени, трябва да може да анализира какво количество данни са били достъпени от зловредно лице и кои точно части от тези данни са били реално видяни, модифицирани или изтрити, така че да могат да се известят всички засегнати страни.
REQ.32	При интеграция с решение за одит на промени, да показва точното местонахождение на защитените данни и да предоставя доказателства, че само оторизирани служители могат да четат, модифицират, споделят и изтриват файлове от критична важност.

7. Система за централизирано автентикиране – 2 броя

Минимални технически изисквания	
REQ.1	Инсталация - виртуална машина с поддръжка на VMWare ESXi, Linux KVM и Microsoft Hyper-V.
REQ.2	AAA услуги за потребители и устройства.
REQ.3	Вградени WEB/Captive портали за идентификация на потребителите.
REQ.4	API интерфейс за интеграция с външни системи за отчетност и мрежови политики.
REQ.5	Интеграция с външни сървъри за идентификация - Microsoft Active Directory, LDAP, RADIUS, RSA системи за идентификация с еднократна парола.
REQ.6	Удостоверяване чрез потребителско име и парола, с X.509 сертификат и по MAC адрес.
REQ.7	Профилиране на крайните устройства.
REQ.8	BYOD функции.
REQ.9	Прилагане на различни политики за удостоверяване и оторизация на база: • Час и дата на идентификацията • Тип на връзката – 802.1x wired, 802.1x wireless, достъп през VPN , достъп през WEB портал за идентификация • Използван EAP тип • Потребителско име • RADIUS атрибути • Атрибути на X509 потребителските сертификати • Вид/модел/OS на устройството
REQ.10	Управление на мрежовия достъп: • Динамично зареждане на филтриращи листи (ACL) в мрежовите устройства на база политиките за управление на достъпа. • Динамично назначаване на VLAN мрежи към потребителите на база политиките за управление на достъпа. • URL пренасочвания на потребителите към вградени или външни WEB/Captive портали.
REQ.11	Поддръжка на RADIUS и Radius CoA.
REQ.12	Функция на RADIUS proxy.
REQ.13	Възможност за TACACS+ за идентификация и управление нивото на достъп на администраторите към мрежови устройства.
REQ.14	Възможност за проверка на състоянието (posture assessment) на крайните потребители.
REQ.15	Вграден Certificate Authority.
REQ.16	Web GUI HTTP и HTTPS Ping DNS TFTP FTP NTP SSHv2 Интеграция с LDAP Автоматичен backup на базата данни върху външни FTP и SFTP сървъри
REQ.17	Да бъдат предложени лицензи за удостоверяване и оторизация на 500 крайни устройства едновременно.
Гаранция и поддръжка:	
REQ.18	Техническа поддръжка за срок от минимум 5 (пет) години.
REQ.19	Получаване на нови версии на софтуера за срок от минимум 5 (пет) години.

8. Специализиран дисков масив за архиви – 1 брой

Спецификация – минимални изисквания	
REQ.1.	Тип на шасито – за вграждане в 19-инчов шкаф.
REQ.2.	Капацитет – минимум 145TB използваем капацитет преди компресия и дедупликация, с възможност за бъдещи разширения до 250TB.
REQ.3.	Устройството трябва да разполага с мин. 4 порта със скорост 10/25 Gb/s със съответните SFP модули.
REQ.4.	Основни функционални изисквания: - Данните да могат да се изпращат по LAN, като се използват CIFS, NFS, NDMP протоколи. - Да поддържа изпращане на данните през SAN/FC (Storage Area Network/Fibre Channel) - Всички гореизброени методи за комуникация да могат да работят едновременно. - Устройството/системата трябва да поддържа Inline дедупликация на данните. - Устройството/системата трябва да поддържа употребата на софтуерни приставки (plug-ins) на backup сървъра/медия сървъра/storage устройството/backup клиента, които да позволяват дедупликация на данните преди изпращането им към backup устройството. - Устройството трябва да поддържа криптиране при репликация. - Устройството трябва да поддържа репликация на дедуплицираните данни към същия или подобен тип устройство. - Устройството трябва да поддържа архивиране (backup) на данните с възможност за заключване на архивираните файлове (retention lock) включително с възможност за допълнително активиране на функционалността съобразно нуждите на АМС - Устройството трябва да поддържа моментни копия/snapshots. - Устройството да поддържа виртуална лентова библиотека. - Устройството да поддържа глобална дедупликация на всички пространства (CIFS/NFS shares, VTL, различни директории и др.).
REQ.5.	Решението трябва да позволява репликация със съществуващи Dell PowerProtect DD 6300 със сериен номер CKM00195102318, без необходимост от използване на допълнителен хардуер (освен този за мрежова свързаност) и външни лицензи.
REQ.6.	Гаранционен период: минимум 60 месеца

9. Спомагателни комуникационни елементи – 40 броя

Спецификация	
REQ.1	10GBASE-SR SFP+ модул.
REQ.2	Конектор – дуплексен LC.
REQ.3	Модулът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

10. Лиценз за функционалност „отдалечен достъп - VPN“

Минимални изисквания	
REQ.1	Да поддържа до 300 едновременни (конкуренти) потребителя
REQ.2	Валидност: минимум 60 месеца
REQ.3	Да бъде съвместим с наличните в момента защитни стени Cisco FTD 3100

III. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

- Изпълнителят следва да осигури изпълнението от лице, надлежно оторизирано от производителя или официален негов представител за право на

разпространение на предлаганите продукти на територията на Република България;

- Оборудването трябва да съответства или да надвишава в техническо отношение посочените минимални изисквания в настоящите Технически параметри;
- Оборудването, предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя и да не е спряно от производство;
- Хардуерните компоненти на оборудването следва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа;
- Хардуерът следва да бъде доставен в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, където се изискват, както и с необходимата техническа документация (на електронен носител или чрез линкове, от които може да бъде свалена);
- В рамките на срока на гаранционно обслужване 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. 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;
- Заявки за обслужване (тикети) за доставения хардуер се подават чрез осигурена от Изпълнителя онлайн система за управление на заявки (СУЗ). Всички заявки, получени чрез електронна поща или телефон следва да бъдат регистрирани в СУЗ;
- 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. Времето за реакция е до следващия работен ден от уведомяването;
  Време за реакция е времето от момента на уведомяване от страна на Бенефициера за възникнал проблем до обратна реакция (обаждане или пристигане на място) от ангажирани с изпълнението лица;
- Ангажираните с изпълнението лица са длъжни да осигурят преглед на място в срок не по-късно от следващия работен ден от 9.00 ч. до 17.30 ч.;
- Лицето, ангажирано с изпълнението, следва да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местонахождението на оборудването;
- За всяка извършена дейност, свързана с гаранционното обслужване, се изготвя и предоставя протокол за извършена дейност по гаранционно обслужване, който съдържа описание на извършеното, включително вид и количество. Протоколът се подписва от ангажирано от Изпълнителя лице и оторизираното лице по място на инсталация;
- В случай, че повредата и/ или несъответствието прави устройството негодно за използване по предназначението му, ангажираното с изпълнението лице е длъжно да го замени с ново, с параметри, гарантиращи същата или по-добра функционалност и производителност.

IV. СРОК НА ИЗПЪЛНЕНИЕ

Доставката на оборудването се извършва в срок до 4 месеца от подписване на настоящата заявка.

Срокът на гаранционно обслужване е считано от датата на приемо-предавателния протокол за доставка на оборудването или от датата на регистрация в портала на производителя, което обстоятелство настъпи първо.

V. МЯСТО НА ДОСТАВКА

Място на извършване на доставката е сградата на Администрацията на Министерския съвет, гр. София, бул. „Княз Ал. Дондуков“№ 1 и ул. „Сердика" № 6.

Гаранционното обслужване ще се извършва спрямо местонахождението на инсталираното оборудване