ЗАЯВКА

по рамков договор № РД-06-12 от 10.01.2024 г.
(вх. № ПО-16-309/10.01.2024 г. на „Информационно обслужване“ АД)

Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*16*
Описание на дейност/проект съгласно ПГ:	*Доставка и инсталация на защитни стени за нуждите на МЗ и РЗИ*	
CPV код	*32420000-3 Мрежово оборудване*	
Изискване за достъп до класифицирана информация ДА/НЕ	НЕ	
Стойност: (*стойността следва да съответства на заложената в План-графика*) **без ДДС**	*323 840,00 лв., от които:* *315 440,00 лв. – за доставка на защитни стени* *8 400,00 лв. – за дейности по инсталация*	
Начин на плащане:(*еднократно, на части, периодично или др.*)	*На части:* • *След подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка и издадена фактура.* • *След подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по инсталация и издадена фактура.*	
Плащане с акредитив ДА/НЕ	*Не е приложимо*	
Документи за плащане с акредитив	*Не е приложимо*	
Срок на изпълнение: (*от дата - до дата или в месеци, ако не е обвързан с конкретна дата*)	• *Срок за начало на изпълнение на заявката - до 3 месеца от датата на приемане на заявката. Изпълнителят информира Възложителя за датата на начало на изпълнението.* • *Срок за доставка – до 30 дни след началото на изпълнение.* • *Срок за изпълнение на дейностите по инсталация – до 15 работни дни след доставка.*	
Гаранционен срок:	*съгласно Техническите параметри*	
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 извършената доставка.* • *С подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършените дейности по инсталация.*	
Приложения: (*напр.: технически параметри, образци на отчетни документи*)	*Технически параметри*	
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		

Координатор по заявката:		*Подпис:*
Ръководител на проект/дейност по заявката *(напр.: представител на дирекцията - Заявител):*		*Подпис:*
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		*Подпис:*
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		
Координатор от „Информационно обслужване“ АД по заявката		*Подпис:*
Ръководител на проект/дейност по заявката		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно		*Подпис:*

обслужване“ АД		

ТЕХНИЧЕСКИ ПАРАМЕТРИ
ЗА ДОСТАВКА И ИНСТАЛАЦИЯ НА ЗАЩИТНИ СТЕНИ ЗА НУЖДИТЕ НА МЗ И РЗИ

1. ЦЕЛ

С оглед изграждане на централизиран защитен интернет възел за нуждите на МЗ и РЗИ е необходима доставка на защитни стени от ново поколение, както следва:

Обща информация	
REQ.1.	Количество – 2 броя.
Спецификация – минимални изисквания	
REQ.2.	Минимална пропускателна способност с активирана функция за идентификация на приложенията - 13 Gbps
REQ.3.	Минимална пропускателна способност с активирани всички функционалности за защита: IPS/ AntiVirus/AntiMalware/URL/Firewall/Application Control – 7 Gbps
REQ.4.	Минимална производителност за IPsec VPN – 6.5 Gbps
REQ.5.	Минимален брой сесии - 1 400 000
REQ.6.	Минимален брой нови сесии в секунда - 145 000
REQ.7.	Разпознати и поддържани приложения (минимум) - 3 650 броя
REQ.8.	Минимален брой мрежови интерфейси: - Да разполага 12x1/2.5/5/10G Base-T ports - Да разполага с 10x1/10G SFP/SFP+ интерфейса - Да има възможност за допълнителни минимум 4x25G SFP28
REQ.9.	Режими на работа на интерфейсите: - L2 - L3 - Tap - Transparent - едновременно/микс да се използват върху едно устройство.
REQ.10.	Маршрутизиращи протоколи: - OSPFv2/v3 - BGP with graceful restart - RIP - Static routing - Policy-based forwarding - Point-to-Point Protocol over Ethernet (PPPoE) - Bidirectional Forwarding Detection (BFD)
REQ.11.	Минимални изисквания към IPSec имплементация: - Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) - Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
REQ.12.	Минимален брой конкурентни SSL VPN потребителя включени в системата (постоянни лицензи) - 1000 SSL VPN потребителя.
REQ.13.	Минимален брой IPSec Site-to-Site VPN - 2000 отдалечени точки.

REQ.14.	Устройството да поддържа виртуални таблици за маршрутизация минимум 11 броя.
REQ.15.	Устройството да има възможност да поддържа виртуализация (виртуални контексти) – 11 броя.
REQ.16.	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
REQ.17.	Системата следва да декриптира и инспектира SSL като поддържа: TLS v1.1, TLS v1.2, TLS v1.3
REQ.18.	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API, извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
REQ.19.	Режим на надеждност: - Active-Passive - Active/Active - Клъстер до 6 устройства разпределени в отдалечени центрове за данни.
REQ.20.	Минимален брой делегирани интерфейси за управление (в допълнение на мрежовите интерфейси): - 1 x 10/100/1000 out-of-band management port - 2 x 100/1000Mbps, 1 x 10Gbps SFP+ интерфейси за отказоустойчивост - 1 x RJ-45 конзолен порт
REQ.21.	Предназначена за вграждане в 19‘‘ шкаф с максимален размер 1U
REQ.22.	Резервирано захранване, 100-240VAC (50-60Hz)
Функционални изисквания към системата	
REQ.23.	Изграждане на сектори с различна степен на доверие, които да разделят мрежата на отделни сегменти и прилагане на политики на база потребителски имена от Активната Директория;
REQ.24.	Системата да анализира съдържанието за наличие на зловреден код като включва минимум AntiVirus, AntiSpyware, IPS;
REQ.25.	Системата да прави анализ на непознати заплахи (Zero Day зловреден код) в защитена среда като създава и дистрибутира сигнатури в реално време;
REQ.26.	Системата за анализ на Zero Day зловреден код трябва да използва минимум следните методи за анализ: Static Analysis, Machine Learning, Dynamic Analysis, Bare metal analysis
REQ.27.	Предлаганата защитна стена трябва да може да изпраща минимум 2000 файла на час към системата за анализ на Zero Day;
REQ.28.	Системата да анализира PE и PowerShell скриптове в защитната стена и предоставя защита в реално време;
REQ.29.	Системата следва да инспектира за заплахи HTTPS протокола чрез декриптиране;
REQ.30.	Системата следва да инспектира за заплахи HTTP 1.1 и HTTP 2.0 протоколи;

REQ.31.	NGFW възможностите и прилежащите бази данни като Antivirus, Sandboxing трябва да използват сигнатури и съдържание на производителя на защитната стена – Не се приема OEM или интеграция с трети страни;
REQ.32.	Управлението на устройството трябва да се реализира че физически отделени процесор и памет отделени от ресурсите използвани за управление на трафика;
REQ.33.	Решението да използва вътрешните ресурси на защитната стена за да анализира и открива зловреден JavaScript с цел кражба на корпоративни потребителски имена и пароли чрез Phishing;
REQ.34.	Наличие на DLP (Data Loss Prevention) функционалност, за ограничаване на движението на конфиденциални файлове към и извън организацията;
REQ.35.	Решението да притежава възможност да ограничава достъпа на потребителите до Web сървъри, които не поддържа минимални изисквания за валиден публичен сертификат и съответно високо ниво на сигурност (TLSv 1.1, TLSv1.2, TLSv1.3);
REQ.36.	Препращане на подозрителните DNS заявки към устройството с цел ограничаване на достъпа и регистриране на заразени машини в мрежата;
REQ.37.	Предложението решение трябва може да изгражда отдалечен VPN достъп чрез агент инсталиран на крайно клиентската машина;
REQ.38.	Агента за VPN достъп трябва да поддържа (да може да бъде инсталиран) минимум следните операционни системи: Windows, Linux, macOS, Android, iOS, Raspbian, Ubunto
REQ.39.	Възможност за QoS трафика според типа приложение потребител и/или URL категория;
REQ.40.	Прозрачна идентификация на потребителите от Активната директория без изискване на крайната машина да се инсталира агент, настройки в browser или отваряне на Web Portal;
REQ.41.	Решението да може да изпраща декриптирани потоци от данни към трети страни за допълнителен анализ след което отново да криптира трафика.
REQ.42.	Да предоставя възможност за карантина на заразени устройства независимо от техните IP адреси, локация и потребител.
REQ.43.	Да предоставя възможност за съставяне на политика за сигурност базирана на устройство независимо от неговия IP Address, локация и потребител.
REQ.44.	Решението да може да чете данните в X-Forwarded-For (XFF) за идентифициране на реалния източник на данни (IP Address), когато той се намира зад други мрежови устройства.
REQ.45.	Защита на корпоративните потребителски имена и пароли, посредством блокиране или ограничаване на тяхното използване в външни за организацията системи и публично достъпни доставчици (Dropbox, Google, Facebook, LinkedIn).
REQ.46.	Решението да включва функционалност позволяваща служебния достъп до публични облачни услуги като Office 365, Google, Dropbox и YouTube, и ограничаваща достъпа до лични потребителски акаунти за същите приложения.

REQ.47.	Анализът на логовете и репортинг да се извършва от самото устройство с през неговия графичен интерфейс, без да необходима инсталация на допълнителен софтуер.
REQ.48.	Решението да притежава Уеб базиран интерфейс с различни статистики на база време, приложение, категории, потребители, заплахи и други;
REQ.49.	Генерираните отчети и логове следва да са обогатени с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и други);
REQ.50.	Решението да може автоматично да тегли IP, Domain или URL листи от Web Server собственост на клиента или външна организация с цел ограничаване / позволяване на достъпа до гореспоменатите.
REQ.51.	Решението да може автоматично да открива какви приложения работят в организацията и да предлага лист от такива, които да бъдат добавени към нови или вече съществуващи правила за сигурност.
REQ.52.	Решението да предоставя механизъм за откриване и превенция на DNS Tunneling канали за комуникация, включително възможност да следи и ограничаване достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA));
REQ.53.	Системата да предоставя филтриране на уеб сайтовете по категории и ограничаване на достъпа до опасно съдържание в Интернет, включително мулти категоризация на URL съгласно тип на съдържанието и риск. Да има възможност да анализира URL и тяхното съдържание в реално време. Всяка заявка за достъп да бъде анализирана чрез Machine Learning на база на HTTP Request, включително да може да идентифицира новорегистрирани домейни и ограничава достъпа до тях;
REQ.54.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, чрез който да осъществява отдалечен защитен достъп от телефони и таблети (с операционни системи iOS, Android) и инспекция (compliance check) на крайно клиентската машина, който се извършва по време на изграждането на защитена връзка;
REQ.55.	Системата да има възможност за надграждане с допълнителен лиценз инсталиран на защитната стена, с който да открива и управлява IoT (Internet of Things) устройства като предоставя възможност за автоматично генериране на препоръчани правила за достъп и контрол.
REQ.56.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя.
Гаранция и поддръжка:	
REQ.57.	Хардуерна гаранция за срок от минимум 3 (три) години.
REQ.58.	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.59.	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.

2. ДЕЙНОСТИ ПО ИНСТАЛАЦИЯ НА ЗАЩИТНИ СТЕНИ

2.1 Инсталиране на защитни стени от ново поколение в шкаф, определен от Възложителя.

2.2 Конфигуриране на защитни механизми на защитни стени за инспекция, обследване и при необходимост блокиране на интернет трафик от потребители.

2.3 Интеграция с активна директория.

3. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО

Заявки за обслужване (тикети) за доставеното оборудване 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.

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.

Изпълнителят следва да осигури изпълнението на доставката от лице, надлежно оторизирано от производителя или от официален негов представител с права за извършване на продажба и извършване на гаранционна сервизна дейност на територията на Република България.

4. ГАРАНЦИЯ И ПОДДРЪЖКА. УСЛОВИЯ НА ГАРАНЦИОННО ОБСЛУЖВАНЕ

1. В съответствие с режима на гаранционно обслужване ангажираните от Изпълнителя лица, отстраняват 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 и изискванията на заявката. 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.
2. Времето за реакция е до 8 часа от уведомяването му.

* *Време за реакция е времето от момента на уведомяване от страна на Възложителя за възникнал проблем до обратна реакция (обаждане или пристигане на място) от ангажираните от Изпълнителя лица.*

3. Ангажираните от Изпълнителя лица са длъжни да осигурят преглед на място в срок не по-късно от следващия работен ден.
4. Ангажираните от Изпълнителя лица се задължават да отстранят настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местонахождение на оборудването до 72 часа от установяването.

В случай, че повредата и/или несъответствието прави устройството негодно за използване по предназначението му, ангажираните от Изпълнителя лица са длъжни да го заменят с ново, с параметри, гарантиращи същата или по-добра функционалност и производителност.

5. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

Мястото на извършване на доставката е сградата на „Информационно обслужване“ АД, намираща се в гр. София, ул. „Лъчезар Станчев“ № 11.

Гаранционното обслужване ще се извършва спрямо местонахождението на инсталираното оборудване.