***Образец № 3.1***

**ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ**

**за изпълнение на обществена поръчка с предмет:**

 **„ДОСТАВКА НА КОМУНИКАЦИОННА ТЕХНИКА ЗА НУЖДИТЕ НА УЧЕБЕН ЦЕНТЪР ПО КИБЕРОПЕРАЦИИ”**

**за обособена позиция № 1:**

**Доставка на 1 брой Firewall система**

От участник: .......………………………………………......................................................................

................................................................................................................................................................

................................................................................................................................................................

*(посочва се наименованието на участника, ЕИК, представляващо лице и данни за кореспонденция – адрес, телефон, факс, електронна поща; в случай на обединение следва да се посочат наименованието на обединението, представляващият обединението и неговите членове)*

**УВАЖАЕМИ ДАМИ И ГОСПОДА,**

Представям Ви нашето техническо предложение за изпълнение на обявената от Вас обществена поръчка.

**Обособена позиция № 1 –** Доставка на 1 брой Firewall система

|  |  |  |
| --- | --- | --- |
| **ПАРАМЕТРИ** | **ТЕХНИЧЕСКИ ИЗИСКВАНИЯ** | **ПРЕДЛОЖЕНИЕ НА УЧАСТНИКА** |
| **Firewall система със следния състав и параметри на отделните устройства в системата:** |  |
| **Защитна стена от ново поколение (NGFW) – 2 броя** |  |
| Тип на кутията/шасито | За директен монтаж в 19‘‘ комуникационен шкаф |  |
| Захранване | минимум два токозахранващи модула, работещи в режим с пълно резервиране, поддържащи захранване от 220-240v AC, 50Hz |  |
| Работен температурен диапазон | от 0º до +40 ºC |  |
| Интерфейси | * Минимум 12 порта 100/1000BASE-T и 4 SFP+ интерфейса с възможност за разширение чрез допълнителен модул с още поне 8 порта SFP+
* Минимум 1 брой сериен конзолен порт
* Минимум 1 брой USB порт
 |  |
| Производителност | * Минимум 20 Gbps с активирани statefull inspection, firewall
* NGFW (IPS, AVC) – 9 Gbps
* Брой сесии – минимум 3 000 000
* Нови сесии за 1 секунда – минимум 70000
* IPSec производителност – минимум 2 Gbps
* Брой VPN тунели – минимум 8000
* С възможност за VPN load balancing
 |  |
| Методи за управление и наблюдение | * Kонзола, HTTP и HTTPS
* Ping
* DNS
* TFTP
* FTP
* NTP
* SSHv2 и SNMPv3
* Syslog
* Експортиране на трафична информация чрез IPFIX или подобен протокол към външна система за трафичен анализ
* Задаване ниво на достъп до системата за всеки администратор
* Идентификация на администраторите чрез локална база, RADIUS сървър и LDAP
* Ethernet порт за out of band управление и наблюдение на устройството
* Управление и наблюдение чрез външен софтуер, предлагащ корелация на събитията, автоматично активиране на политики и дългосрочно съхраняване на информацията
* Система за корелация между различни видове събития
* Управление на алармите
* Интеграция с външни системи през REST API
 |  |
| Режим на работа | Да поддържа прозрачен режим на работа – Inline |  |
| Маршрутизиране | Да поддържа режим на работа като маршрутизатор |  |
| IPSec тунели | Да поддържа IPSec тунели с IKE/IKEv2 управление на сесиите и следните методи за защита:* Encryption: 3DES, AES-128 и AES-256
* Authentication: preshared key, RSA и ECDSA
* Integrity: SHA, SHA-256, SHA-384, SHA-512
* Да поддържа SCEP протокол за получаване на сертификат
* Да поддържа OCSP за проверка валидността на сертификати
* Да поддържа инспектиране на SSL трафик
* Да поддържа SSL VPN отдалечен достъп
* Да поддържа минимум 1000 802.1Q VLAN
* Да има вградена IPS система с автоматично обновяване на сигнатурите от cloud услуга на производителя
* Да има вградена Anti-Malware система за защита от файлове със зловреден код и обновяване на сигнатурите от cloud услуга на производителя
* Да поддържа ретроспективно уведомяване на администратора при получаване на информация, класифицираща вече свалени файлове като съдържащи зловреден код
* Да има вградена DPI система с класифициране на мрежовия трафик на ниво приложения и категории от приложения с автоматично обновяване сигнатурите на приложенията от cloud услуга на производителя.
* Да има система за URL филтриране по категории с автоматично обновяване сигнатурите на приложенията от cloud услуга на производителя
* Да поддържа филтриране на мрежовия трафик на база приложения и групи/категории от приложения
 |  |
| Протоколи за маршрутизация | * RIP и RIPv2
* OSPFv2 и OSPFv3
* BGPv4
 |  |
| Мултикаст маршрутизиране | Да поддържа минимум IGMPv2 и PIM-SM мултикаст маршрутизиране |  |
| NAT | Да поддържа динамичен и статичен NAT |  |
| PAT | Да поддържа динамичен и статичен PAT |  |
| NAT и PAT услуги | * NAT за IPv4
* NAT 66
* NAT 64/46 транслации
 |  |
| Поддържани протоколи | Да поддържа NAT AGL за SIP, H.323 и FTP протоколи |  |
| DMZ зони | Да позволява обособяване на DMZ зони |  |
| Rate limiting | Да поддържа rate limiting с класифициране на трафика на база минимум следните параметри:* Интерфейс
* IP мрежи
* Приложения и категории от приложения
* URL категория и репутация
* Active Directory потребители и групи от потребители
* Да поддържа интеграция с Microsoft Active Directory за идентификация на потребителите и създаването на Firewall политики на база AD групи и потребителите
* Да поддържа идентификация на потребителите чрез външен RADIUS сървър
 |  |
| Окомплектовка | Окомплектовка за монтаж в 19‘‘ комуникационен шкаф |  |
| Гаранция | 3 години от производителя, доказано със сериен номер видим на официалния сайт на производителя |  |
| **Система за управление и наблюдение на NGFW системи – 1 брой** |  |
| Инсталация | да поддържа виртуализация върху VMWare ESXi платформа |  |
| Капацитет | 2 броя NGFW системи за наблюдение и управление с възможност за разширение |  |
| Основни функции | * Централизирано управление на лицензи, събития и политика
* Да поддържа пълно управление и наблюдение на предложените NGFW системи в т. 25.1.
* Да поддържа корелация на събитията получавани от NGFW
* Да поддържа създаване и прилагане на NGFW политики върху управляваните устройства
* Да поддържа автоматично прилагане на политики при определени събития
* Да поддържа дългосрочно съхранение на NGFW събитията
* Да поддържа автоматично изпълнение на предварително планирани задачи
* Да има възможност да генерира графично представяне на всички устройства, заразени при евентуална атаката
* Да предоставя възможност за лесно създаване на персонализирано правило за спиране напредването на атаката
* Да дава подробен анализ на злонамерения софтуер за безопасното му пренасочване
 |  |
| Управление и наблюдение | * Да има GUI WEB интерфейс
* Да бъде с ролево управление, да може да се задават различни права за достъп на администраторите или група от администратори
* Да бъде с единна политика за множество функции за защита
* Да бъде с отворени APIs за интегриране с решения на трети страни и работни потоци от клиенти, като защитни стени, мрежова инфраструктура, log management, SIEM, trouble ticketing, и patch management
 |  |

1. Запознати сме с проекта на договор, приемаме го и ако бъдем определени за изпълнител ще сключим договор в законоустановения срок.

2. Валидността на нашето предложение ще бъде………………………………............ (минимум 6 месеца) от крайния срок за подаване на оферти и ще остане обвързващо за нас.

3. Заявявам, че имаме възможност да доставим комуникационната техника, съгласно посоченото в документацията за участие в процедурата количество, в срок и с необходимото качество.

4. Заявявам, че ако бъдем избрани за ИЗПЪЛНИТЕЛ, ще изпълним предмета на поръчката в пълно съответствие с техническата спецификация, изискванията на ВЪЗЛОЖИТЕЛЯ, нормативните изисквания, добрите практики в областта, настоящото предложение и ценовото ни предложение.

5. За обезпечаване изпълнението на задълженията си по договора за възлагане на обществената поръчка, преди подписването на договора ще предоставим на ВЪЗЛОЖИТЕЛЯ **парична, или банкова гаранция, или застраховка за обезпечаване отговорността си за изпълнение на задълженията по договора, в размер на 3% (три процента)** от стойността на договора без ДДС, **от които 1% (един процент) за гаранционно поддържане**.

6. Предлагам следните срокове за изпълнение:

6.1. **Срокът за доставка** е: ………. (…………………………..*словом*) календарни дни, считано от датата, следваща датата на получаване на възлагателното писмо.

6.2. **Срокът за реакция при получено уведомление за неизправност** е:

…………. (……………………………..*словом*) часа, считано от получаване на уведомлението за неизправност (но не повече от 24 часа).

6.3. **Гаранционен срок**: ………………………. (……………………………..*словом*) месеца, считано от датата на подписване на приемо-предавателния протокол.

7. Запознати сме, че всяко отклонение от предварително зададените условия на ВЪЗЛОЖИТЕЛЯ могат да доведат до отстраняване на офертата ни в настоящата процедура.

**Забележка**: Представя се и документ за упълномощаване, когато лицето, което подава офертата, не е законният представител на участника.

**ПОДПИС и ПЕЧАТ:**

|  |  |
| --- | --- |
| **Дата**  | \_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_ |
| **Име и фамилия** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Подпис на упълномощеното лице** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Длъжност**  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **Наименование на участника** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |