# **Додаток 2**

 до тендерної документації

# **Технічні вимоги до предмета закупівлі**

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ

**Міжмережеві екрани ДК 021:2015:** 32420000-3 Мережеве обладнання

|  |  |
| --- | --- |
| **Найменування та опис** | **Кількість (од.)** |
| Міжмережевий екран наступного покоління з функціональністю уніфікованого захисту від загроз (NGFW) FortiGate-60F з ліцензійним програмним забезпеченням (1 рік) та сервісною технічною підтримкою (24\*7, 1 рік) **або еквівалент** | 6 |

|  |  |
| --- | --- |
| **Найменування** | **Технічні вимоги** |
| **Загальні вимоги** | * Мережевий пристрій безпеки що пропонується, повинен являти собою міжмережевий екран наступного покоління (NGFW) та здійснювати інспекцію мережевого трафіку та захист корпоративної інфраструктури відповідно до нижченаведених вимог
* Всі необхідні ліцензії для забезпечення зазначеного в цих вимогах функціоналу та кількісних показників продуктивності мають бути у комплекті запропонованого рішення
* На обладнання не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника.
* NGFW повинен мати чинні експертні висновки Державної служби спеціального зв'язку та захисту інформації України на відповідність вимогам законодавства в галузі захисту інформації або проходити відповідну державну експертизу на момент подання Учасником пропозиції конкурсних торгів
 |
| **Архітектура та форм-фактор** | * NGFW повинні являти собою програмно-апаратний комплекс (ПАК), для встановлення на поличку в стандартну монтажну шафу 19", висота не більше ніж 1 RU
* 1 блок живлення (100-240V AC, 50-60 Hz)
 |
| **Мережеві інтерфейси** | * Не менше ніж 10 GE RJ45 (7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port)
* Не менше ніж 1 USB
* Не менше ніж 1 консольний порт
 |
| **Продуктивність сервісів безпеки** | * Пропускна здатність сервісу Stateful Firewall (на пакетах розміром 1518 байт, UDP): не менше ніж 10 Гбіт/c
* Кількість одночасних TCP-сесій: не менше ніж 700 000
* Кількість нових TCP-сесій/секунду: не менше ніж 35 000
* Пропускна здатність на пакетах розміром 450 байт або Enterprise Testing Conditions / Enterprise traffic mix / APPMIX (з включеними сервісами FW+App Control+IPS+Malware Protection): не менше ніж 700 Mбіт/c
* Пропускна здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 1.4 Гбіт/c
 |
| **Продуктивність VPN** | * Пропускна здатність IPSec VPN: не менше ніж 6.5 Гбіт/c
* Кількість одночасних SSL VPN підключень до шлюзу: не менше ніж 200
* Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 500
* Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 200
 |
| **Віртуалізація** | * Віртуальні FW, (Virtual Systems/Security contexts/Virtual Domains) що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами, тощо: не менше ніж 10
 |
| **Двух факторна автентифікація** | * OTP токени не менше 500
 |
| **Висока доступність (high availability)** | * Active-Active
* Active-Standby
 |
| **L2 функціонал та мережеві служби** | * Агрегація портів (802.3ad)
* VLAN (802.1Q та Trunking)
* Вбудований DHCP, NTP, DNS-сервера
 |
| **NAT** | * Cтатичний NAT
* Динамічний NAT
* PAT
 |
| **Multicast** | * Sparse та dense режим
* Підтримка PIM
 |
| **Сервіси безпеки** | * Stateful Firewall
* Ідентифікація та контроль застосувань (AC/AVC)
* Захист від загроз на основі сигнатурного аналізу (IPS)
* Захист від malware (Antivirus/AMP)
* Web та DNS-фільтрація
* Iнспектування/сканування SSL/TLS трафіку на загрози
* Захист від невідомих загроз (0-day)
* Запобігання витоку даних (DLP)
* Захист від DOS-атак
* IPSec VPN, SSL VPN
 |
| **Stateful Firewall** | * Режими роботи:
* NAT/маршрутизатор
* прозорий режим (міст)
* Підтримка VoIP трафіку: глибока інспекція та захист від атак на протокол SIP
* Виконання ролі проксі для аналізу, інспектування та забезпечення коректної роботи сесій різних протоколів (session helpers, application layer gateway)
 |
| **Ідентифікація та контроль застосувань (AC/ AVC)** | * Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та певної категорії додатків (application control/application visibility control)
* Конфігурація відповідних до користувацького оточення AC/AVC-сенсорів з необхідним набором сигнатур
* Конфігурація виключень у діях з певними додатками (exemption/override)
* Створення користувацьких сигнатур додатків
 |
| **Захист від загроз на основі сигнатурного аналізу (IPS)** | * Інспектування та застосування дій до мережевого трафіку на основі сигнатурного аналізу та виявлення відомих атак (intrusion prevention system)
* Конфігурація відповідних до користувацького оточення IPS-сенсорів з необхідним набором сигнатур
* Конфігурація виключень у діях з певними сигнатурами (exemption/override)
 |
| **Захист від malware (Antivirus/AMP)** | * Anti-Virus / Anti-malware захист
* Виявлення та блокування небажаних програми або файлів (grayware)
* Виявлення та блокування файлів на основі налаштованих порогових значень їх розміру для різних протоколів
* Захист від зловмисних програм для мобільних пристроїв
 |
| **SSL/TLS-інспекція** | * Перехоплення, розшифрування та інспекція HTTPS, IMAPS, POP3S, SMTPS, FTPS-сесій
* Конфігурація виключень з SSL/TLS-інспекції певних IP-адрес, URL, тощо (exemption/override)
* Інспектування SSL/TLS-сертифікату на відповідність певному web-ресурсу до якого здійснюється підключення та строку дійсності (SSL/TLS сertificate іnspection)
* Повноцінне інспектування контенту зашифрованих сесій (full SSL/TLS іnspection)
* Інспектування SSL/TLS-трафіка має включати наступні інспекції: IPS, AC/AVC, AV/AMP, Web-фильтрацію, DLP
 |
| **Захист від невідомих загроз (0-day)**  | * Інтеграція з системою захисту від складних атак нульового дня (у вигляді хмарного сервісу – cloud sandbox)
* Відправка файлів з користувацького трафіку на аналіз у cloud sandbox для виявлення невідомих загроз класу "0-day"
* Ліцензування має дозволяти інспектувати у cloud sandbox не менше ніж 5 000 файлів на день (24 години)
 |
| **Запобігання витоку даних (Data Loss Prevention)** | * Запобігання витоку конфіденційних даних шляхов перевірки трафіку (за назвою файлів, типом файлів, розміром файлів, регулярними виразами)
* Запобігання витоку конфіденційних даних шляхов перевірки трафіка за допомогою заздалегідь визначеної інформації (credit card numbers, SIN numbers, тощо)
* Функціонал DLP має запобігати витоку через наступні протоколи: HTTP-POST, HTTP-GET, SMTP, POP3, IMAP, MAPI, FTP, NNTP
 |
| **Захист від DOS-атак** | * Можливість розпізнавання та блокування DoS атак:
* TCP Syn flood
* TCP/UDP/SCTP port scan
* ICMP sweep
* TCP/UDP/SCTP/ICMP session flooding
 |
| **IPSec VPN, SSL VPN** | * Алгоритми шифрування: 3DES, AES128, AES192, AES256
* Алгоритми хешування: MD5, SHA256, SHA384, SHA512
* Diffie-Hellman Group: 1, 2, 5, 14-20, 21, 27-32
* Підтримка Hub & Spoke топології, Spoke & Spoke (mesh) топології, DMVPN/ADVPN або аналог
* Можливість підключення не менше 400 користувачів IPSec VPN клієнт-шлюз
 |
| **QoS** | * Traffic Shaping
* Traffic Policing
 |
| **Маршрутизації та SD-WAN** | * Статична маршрутизація та маршрутизація по політиках (PBR)
* Динамічні протоколи маршрутизації: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4
* Архітектурна реалізація SD-WAN: вбудований в операційну систему NGFW
* Формування логічного SD-WAN інтерфейсу шляхом об’єднання фізичних та логічних інтерфейсів з різнотипними підключеннями (MPLS, broadband Internet, LTE, тощо)
* Оцінка якості каналів зв'язку SD-WAN шляхом відправлення пакетів чи запитів до певних вузлів у мережі
* Контроль характеристики каналів зв'язку в режимі реального часу (packet loss, jitter, latancy) та іх графічне відображення (gui real-time monitor)
* Визначення SLA для користувацьких додатків (applications) з використанням характеристик каналів зв'язку (packet loss, jitter, latancy)
* Визначення різнопланових стратегій вибору каналів зв'язку для маршрутизації трафіку додатків та сервісів виходячи з критеріїв відповідності SLA, кращих значень характеристик каналів зв'язку, тощо
* Визначення правил маршрутизації трафіку додатків та сервісів через канали SD-WAN у урахуванням стратегій та SLA
* Автоматичне балансування навантаження, переключення і резервування каналів зв’язку для користувацьких додатків та сервісів при зміні храктеристик мережевих з’єднань (loss, jitter, latancy) в реальному часі
* Динамічно виправляти втрати пакетів або відновлювати пакети з помилками викликані несприятливими умовами WAN-каналів під час роботи через VPN (Forward Error Correction)
* Балансування пакетів однієї сесії через два IPSec VPN тунеля на основі "per packet" балансування
* Всі необхідні ліцензії для забезпечення зазначеного вище функціонала мають бути у комплекті запропонованого рішення
 |
| **Автентифікація, авторизація та облік (AAA)** | * Локальна база даних користувачів
* Підтримка протоколів LDAP, RADIUS, TACACS+
* Підтримка 2-факторної автентифікації (two-factor authentication) на основі програмних токенів
* Не менше ніж 2 програмні токени для встановлення на мобільні пристрої (смартфони)
* Single Sign-On: інтеграція с Windows AD
* PKI та сертифікати: X.509, SCEP support, створення Certificate Signing Request (CSR), автоматичне поновлення сертифікатів до закінчення терміну дії, підтримка OCSP
 |
| **Керування, звітність, інтеграція** | * Графічний веб-інтерфейс (Web GUI)
* Інтерфейс командного рядка (CLI)
* Підтримка централізованої системи керування FortiManager Ролевий доступ адміністраторів (RBAC)
* Підтримка REST API
* Централізоване ведення журналів та звітності (logging and reporting)
* Функціонал запису пакетів з мережевих інтерфейсів для подальшого їх аналізу (packet capture)
* Функціонал резервного копіювання та відновлення файлів конфігурації
* SNMP v1, v2, v3
* sFlow v5/Netflow v9, syslog
 |
| **Ліцензійне програмне забезпечення** | * Примірник програмної продукції FortiGate-60F 1 Year Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium)
 |
| **Технічна сервісна підтримка** | * Обладнання повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 12 місяців з рівнем сервісу 24\*7
* Постійний доступ до центру технічної підтримки виробника через сайт, електронною поштою або за телефоном 24\*7
* Постійний авторизований доступ до сайту виробника 24\*7
* Отримання актуальних репутаційних баз, сигнатур захисту та всіх необхідних оновлень для сервісів безпеки
* Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника
* Можливість реєстрації сервісних випадків в режимі 24\*7\*365, доставку і заміну запасних частин у режимі Next Business Day (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника)
 |

*Якщо в технічній специфікації міститься посилання на конкретні марку чи виробника або на конкретний процес, що характеризує продукт чи послугу певного суб’єкта господарювання, чи на торгові марки, патенти, типи або конкретне місце походження чи спосіб виробництва, то слід розуміти у значені «або еквівалент».*

Все обладнання має бути новим, не повинно бути попередньо вживаним або відновленим. Моделі обладнання, що будуть запропоновані, мають бути сучасними та містити останні стабільні версії програмного забезпечення, яке розміщено на офіційних ресурсах виробника на момент подання пропозиції.

Учасник повинен надати детальну технічну специфікацію обладнання на відповідність технічним вимогам та посилання на офіційний сайт виробника, українською чи англійською мовами, де вказано характеристики запропонованої моделі товару для можливості перевірки достовірності наданої учасником пропозиції.

В складі пропозиції Учасник повинен надати документальне підтвердження повноважень щодо здійснення постачання обладнання, запропонованого у даних торгах, у вигляді листа авторизації від виробника або офіційного представництва виробника чи дистриб'ютора в Україні.