|  |
| --- |
| Назва закупівлі: **Пристрій мережевої безпеки (міжмережевий екран)**Класифікатор та його відповідний код: **ДК 021:2015: 32420000-3: Мережеве обладнання**Процедура закупівлі: **Відкриті торги з особливостями**Очікувана вартість: **1 600 000,00 грн з ПДВ**Дата оприлюднення: **21 липня 2023 року**Детальна інформація за посиланням: <https://prozorro.gov.ua/tender/UA-2023-07-21-004822-a> |

ІНФОРМАЦІЯ ПРО НЕОБХІДНІ ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ

Для забезпечення надання гарантованого та безпечного доступу до мережі Інтернет Державного підприємства «Державний експертний центр Міністерства охорони здоров’я України», необхідно на серверних технічних майданчиках провести модернізацію існуючого обладнання мережевої безпеки Fortinet Fortigate.

Обладнання Fortinet повинно забезпечувати:

• контентну фільтрацію трафіку користувачам (Web Filtering);

• функціональну систему запобігання вторгненням (IPS);

• захист електронної поштової системи від небажаної кореспонденції (Antispam Services);

• функціональний міжмережевий екран;

• захист від шкідливого програмного забезпечення (Antivirus software);

• бути спроможним, сумісним та придатним до об’єднання в єдину інфраструктуру з існуючим у Замовника обладнанням мережевої безпеки Fortinet Fortigate, що находиться в експлуатації у Замовника.

Всі посилання на конкретну торгівельну марку чи фірму, патент, конструкцію або тип предмета закупівлі, джерело його походження або виробника, слід читати з виразом «або еквівалент».

Учасники процедури закупівлі повинні надати в складі тендерних пропозицій інформацію та документи, які підтверджують відповідність тендерної пропозиції Учасника технічним, якісним, кількісним та іншим вимогам до предмета закупівлі, наведеним у цьому додатку тендерної документації.

Невідповідність пропозиції Учасника торгів вимогам цього додатку тендерної документації призводить до її відхилення. Неповні пропозиції відхиляються та участі у конкурсній процедурі не беруть.

Відповідність технічних, якісних та кількості характеристик запропонованих товарів вимогам замовника повинна бути підтверджена учасником шляхом надання у складі тендерної пропозиції довідки, яка має містити порівняльну таблицю технічних, якісних та кількісних характеристик товару, що пропонується учасником, які мають бути не гіршими за наведені в вимогах до технічних, якісних та кількості характеристик до предмету закупівлі, що викладені у цьому додатку тендерної документації, із обов’язковим зазначенням типу, марки, моделі, назви товару, що пропонується Учасником.

Декларація (декларації) про відповідність вимогам Технічних регламентів: - з електромагнітної сумісності обладнання (у відповідності до постанови КМУ від 16.12. 2015 №1077); - низьковольтного електричного обладнання (у відповідності до постанови КМУ від 16.12.2015 №1067) дійсна (дійсні) на момент подачі пропозиції;

Експертний висновок зареєстрований в Адміністрації Державної служби спеціального зв’язку та захисту інформації України про відповідність пристрїв мережевої безпеки (міжмережевих екранів) вимогам нормативних документів із технічного захисту інформації з рівнем гарантій Г-2, дійсний на момент подачі пропозиції;

 Довідка у довільній формі щодо наявності інформації про товар, що пропонується у «Переліку засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту у якої встановлена законом» у відповідності до п. 17 Положення «Про технічний захист інформації в Україні», затвердженого Указом Президента України від 27.09.1999 №1229 із зазначенням номеру запису про товар у вказаному переліку (з врахуванням останіх змін на момент подачі пропозиції).

Учасники процедури закупівлі повинні надати в складі тендерних пропозицій документ/копію документу від виробника товару/офіційного представника виробника товару (сертифікат/авторизаційний лист/ інший документ) про надання учаснику процедури закупівлі відповідного статусу (дилер/партнер/інший статус) та підтвердження зобов’язань здійснення підтримки на товар, що пропонується із зазначенням номеру закупівлі у системі Prozorro та найменування Замовника.

Доставка до сервісного центру товару, який вийшов з ладу, виконується Учасником за власний рахунок (включаючи повернення до Замовника відремонтованого товару). Учасники процедури закупівлі повинні надати в складі тендерних пропозицій гарантійних лист щодо таких зобов’язань.

ТЕХНІЧНІ, якісні та кількісні ВИМОГИ (характеристики) ДО ПРЕДМЕТУ ЗАКУПІВЛІ

| № п/п | Назва | Вимоги | Кіл-ть |
| --- | --- | --- | --- |
|  | Пристрій мережевої безпеки (міжмережевий екран) FortiGate-60F Hardware plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)(FG-60F-BDL-950-12) | Загальні вимоги- Пристрій мережевої 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 виробникаАрхітектура 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 - Не менше ніж 1 USB- Не менше ніж 1 консольний портПродуктивність 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/cПродуктивність 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 200Віртуалізація- Віртуальні FW, (Virtual Systems/Security contexts/Virtual Domains) що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами, тощо: не менше ніж 10Контролер керування комутаторами та точками доступу- Керування не менше ніж: 24 комутаторів- Керування не менше ніж: 64 точок доступуДвух факторна автентифікація- OTP токени не менше 500Висока доступність (high availability)- Active-Active - Active-StandbyL2 функціонал та мережеві служби- Агрегація портів (802.3ad)- VLAN (802.1Q та Trunking)- Вбудований DHCP, NTP, DNS-сервераNAT- Cтатичний NAT- Динамічний NAT- PATMulticast- Sparse та dense режим- Підтримка PIMСервіси 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 VPNStateful 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 додатківЗахист 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 пристроївWeb та DNS-фільтрація- Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фильтрація)- Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація)- Виявлення та блокування доступу до Botnet мереж- Блокування певних небезпечних елементів web-сайтів (Java Applet, ActiveX scripts, тощо)- Статичні blacklists та whitelistsSSL/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, DLPЗахист 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, NNTPЗахист від DOS-атак- Можливість розпізнавання та блокування DoS атак: TCP Syn flood2) TCP/UDP/SCTP port scan 3) ICMP sweep 4) TCP/UDP/SCTP/ICMP session floodingIPSec 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-шлюзQoS- Traffic Shaping - Traffic PolicingМаршрутизації 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 рішенняАвтентифікація, 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 OCSPКерування, звітність, інтеграція- Графічний веб-інтерфейс (Web GUI)- Інтерфейс командного рядка (CLI)- Підтримка централізованої системи керування - 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, syslogТехнічна сервісна підтримка- Пристрій мережевої безпеки (міжмережевий екран) повинен 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 в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника) | 1 |
|  | Пристрій мережевої безпеки (міжмережевий екран) FortiGate-100F Hardware plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)(FG-100F-BDL-950-12) | Загальні вимоги- Пристрій мережевої 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 виробникаАрхітектура та форм-фактор- NGFW повинні являти собою програмно-апаратний комплекс (ПАК) для встановлення в стандартну монтажну шафу 19", висота не більше ніж 1 RU- Не менше ніж 2 блоки живлення (100-240V AC, 50-60 Hz)- Якщо таких пристроїв, для виконання вимог ТЗ, повинно бути декілька (кластеризація, додаткові модулі безпеки, маршрутизатори, тощо) вони усі мають бути у комплекті поставки рішенняМережеві інтерфейси- Не менше ніж 12х GE RJ45- Не менше ніж 4х GE SFP- Не менше ніж 4х GE RJ45/SFP Shared Media Pairs- Не менше ніж 2х 10 GE SFP+- Не менше ніж 2х GE RJ45 WAN- Не менше ніж 1х GE RJ45 Management- Не менше ніж 1х GE RJ45 DMZ- Не менше ніж 1x USB- Консольний порт 1x RJ45Продуктивність сервісів безпеки- Пропускна здатність сервісу Stateful Firewall (на пакетах розміром 1518 байт, UDP): не менше ніж 20 Гбіт/c- Кількість одночасних TCP-сесій: не менше ніж 1 500 000- Кількість нових TCP-сесій/секунду: не менше ніж 56 000- Пропускна здатність на середніх пакетах розміром 450 байт або Enterprise Testing Conditions / Enterprise traffic mix (FW+App Control+IPS+Malware Protection): не менше ніж 1 Гбіт/c- Пропускна здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 1 Гбіт/cПродуктивність VPN- Пропускна здатність IPSec VPN: не менше ніж 11,5 Гбіт/c- Кількість одночасних SSL VPN підключень до шлюзу: не менше ніж 500 - Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 16000 - Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 2000Віртуалізація- Віртуальні FW, (Virtual Systems/Security contexts/Virtual Domains) що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами, тощо: не менше ніж 10Контролер керування комутаторами та точками доступу- Контролер керування комутаторами та точками доступуДвух факторна автентифікація- OTP токени не менше 5000Висока доступність (high availability)- Active-Active - Active-StandbyL2 функціонал та мережеві служби- Агрегація портів (802.3ad)- VLAN (802.1Q та Trunking)- Вбудований DHCP, NTP, DNS-сервераNAT- Cтатичний NAT- Динамічний NAT- PATMulticast- Sparse та dense режим- Підтримка PIMСервіси 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 VPNStateful Firewall- Режими роботи: NAT/маршрутизаторпрозорий 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 додатківЗахист 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 пристроївWeb та DNS-фільтрація- Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фильтрація)- Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація)- Виявлення та блокування доступу до Botnet мереж- Блокування певних небезпечних елементів web-сайтів (Java Applet, ActiveX scripts, тощо)- Статичні blacklists та whitelistsSSL/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, DLPЗахист 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, NNTPЗахист від DOS-атак- Можливість розпізнавання та блокування DoS атак: TCP Syn floodTCP/UDP/SCTP port scan ICMP sweep TCP/UDP/SCTP/ICMP session floodingIPSec 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-шлюзQoS- Traffic Shaping - Traffic PolicingМаршрутизації 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 рішенняАвтентифікація, 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 OCSPКерування, звітність, інтеграція- Графічний веб-інтерфейс (Web GUI)- Інтерфейс командного рядка (CLI)- Підтримка централізованої системи керування - 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, syslogТехнічна сервісна підтримка- Пристрій мережевої безпеки (міжмережевий екран) повинен 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 в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника) | 1 |
|  | Пристрій мережевої безпеки (міжмережевий екран) FortiGate-400F Hardware plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)(FG-400F-BDL-950-12) | Загальні вимоги- Пристрій мережевої 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 виробникаАрхітектура та форм-фактор- NGFW повинні являти собою програмно-апаратний комплекс (ПАК) для встановлення в стандартну монтажну шафу 19", висота не більше ніж 1 RU- Не менше ніж 2 блоки живлення (100-240V AC, 50-60 Hz)- Якщо таких пристроїв, для виконання вимог ТЗ, повинно бути декілька (кластеризація, додаткові модулі безпеки, маршрутизатори, тощо) вони усі мають бути у комплекті поставки рішенняМережеві інтерфейси- Не менше ніж 16х GE RJ45;- Не менше ніж 8х 1GE SFP;- Не менше ніж 4 x 1GE/10GE SFP+ Slots;- Не менше ніж 4 x 10GE SFP+ Ultra Low Latency Slots- Не менше ніж 2х GE RJ45 Management;Продуктивність сервісів безпеки- Пропускна здатність сервісу Stateful Firewall (на пакетах розміром 1518 байт, UDP): не менше ніж 79,5 Гбіт/c- Кількість одночасних TCP-сесій: не менше ніж 7 800 000- Кількість нових TCP-сесій/секунду: не менше ніж 500 000- Пропускна здатність на середніх пакетах розміром 450 байт або Enterprise Testing Conditions / Enterprise traffic mix (FW+App Control+IPS+Malware Protection): не менше ніж 9 Гбіт/c- Пропускна пуска здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 8 Гбіт/cПродуктивність VPN- Пропускна здатність IPSec VPN: не менше ніж 55 Гбіт/c- Кількість одночасних SSL VPN підключень до шлюзу: не менше ніж 5000 - Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 50000 - Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 2000Віртуалізація- Віртуальні FW, (Virtual Systems/Security contexts/Virtual Domains) що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами, тощо: не менше ніж 10Контролер керування комутаторами та точками доступу- Керування не менше ніж: 72 комутаторів- Керування не менше ніж: 512 точок доступуДвух факторна автентифікація- OTP токени не менше 5000Висока доступність (high availability)- Active-Active - Active-StandbyL2 функціонал та мережеві служби- Агрегація портів (802.3ad)- VLAN (802.1Q та Trunking)- Вбудований DHCP, NTP, DNS-сервераNAT- Cтатичний NAT- Динамічний NAT- PATMulticast- Sparse та dense режим- Підтримка PIMСервіси 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 VPNStateful Firewall- Режими роботи: 1) NAT/маршрутизатор2) 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 додатківЗахист 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 пристроївWeb та DNS-фільтрація- Інспектування URL-запитів та можливість блокування їх на основі відношення до певної категорії (Web-фильтрація)- Інспектування запитів DNS та можливість блокування їх на основі відношення до певної категорії (DNS-фільтрація)- Виявлення та блокування доступу до Botnet мереж- Блокування певних небезпечних елементів web-сайтів (Java Applet, ActiveX scripts, тощо)- Статичні blacklists та whitelistsSSL/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, DLPЗахист 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, NNTPЗахист від DOS-атак- Можливість розпізнавання та блокування DoS атак:  1) TCP Syn flood 2) TCP/UDP/SCTP port scan  3) ICMP sweep  4) TCP/UDP/SCTP/ICMP session floodingIPSec 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 аналогМожливість підключення не менше 400 користувачів IPSec VPN клієнт-шлюзQoS- Traffic Shaping - Traffic PolicingМаршрутизації 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 рішенняАвтентифікація, 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 OCSPКерування, звітність, інтеграція- Графічний веб-інтерфейс (Web GUI)- Інтерфейс командного рядка (CLI)- Підтримка централізованої системи керування - 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, syslogТехнічна сервісна підтримка- Пристрій мережевої безпеки (міжмережевий екран) повинен 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 в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника) | 1 |

Учасник повинен гарантувати дотримання норм чинного законодавства із захисту довкілля, основних вимог державної політики України в галузі захисту довкілля та вимог чинного природоохоронного законодавства України під час постачання товару, що є предметом закупівлі (надати довідку в довільній формі).