|  |
| --- |
| Назва закупівлі: **Мережеве обладнання**Класифікатор та його відповідний код: **ДК 021:2015: 32420000-3: Мережеве обладнання**Процедура закупівлі: **Відкриті торги з особливостями**Очікувана вартість: **5 000 858,47 грн з ПДВ**Дата оприлюднення: **13 серпня 2024 року**Детальна інформація за посиланням: <https://prozorro.gov.ua/tender/UA-2024-08-13-007176-a> |

**ІНФОРМАЦІЯ ПРО ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ**

**ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

Вимоги необхідні до обладнання технічні (якісні), кількісні характеристики

1. Все обладнання повинно бути новим, не бувшим у використанні або відновленим.

2. Запропонований товар не повинен мати статус EOL/EOS (End-of-Life/End-of-Support) або подібного.

3. Пропоновані моделі обладнання повинні бути сучасними, та такими, що мають останні стабільні версії програмного забезпечення.

4. Обладнання, повинно бути виготовлено в країнах, на які не розповсюджуються обмеження в торговельних відносинах по торгових міжнародних договорах уряду України.

5. Учасник у складі своєї пропозиції повинен надати копію (копії) авторизаційного листа від виробника (або виробників) обладнання (або офіційного представництва в Україні) щодо повноважень Учасника на постачання такого обладнання. Лист (листи) повинен бути адресований Замовнику з зазначенням номеру оголошення та назви предмету закупівлі.

Технічні вимоги до предмета закупівлі:

**1. Контролер для керування бездротовою мережею з ліцензіями – 2 комплекти**

| **Найменування** | **Вимоги** |
| --- | --- |
| Загальна характеристика та функціональність | * Контролер для централізованого управління і моніторингу бездротової мережі з можливостями формування відмовостійкого кластеру для балансування навантаження та керування точками доступу;
 |
| Форм-фактор | * Форм-фактор для встановлення в стандартну серверну шафу 19" і мати висоту не більше 1RU;
 |
| Характеристики масштабованості та продуктивності | * Максимальна кількість точок доступу, що можуть керуватися контролером: не менше 64
* Максимальна кількість клієнтів, що можуть одночасно працювати в мережі під управлінням контролеру: не менше 4096
* Максимальна кількість VLAN: не менше 4096
* Пропускна спроможність пристрою в централізованому режимі: не менше 8 Гбіт/с
* Максимальна пропускна спроможність міжмережевого екрану: 8 Гбіт/с
* Максимальна кількість одночасних сесій міжмережевого екрану: не менше 64000;
* В склад пропозиції повинно бути включено компоненти та ліцензії необхідні для формування відмовостійкого кластеру із можливістю балансування навантаження та забезпечення єдиної точки ліцензування управління та моніторингу;
 |
| Вимоги до можливого розширення | * Рішення повинне дозволити подальше масштабування за кількістю точок, клієнтів та пропускною спроможністю на всю інфраструктуру Замовника (розрахунково до 64 точок доступу, до 4096 клієнтів) шляхом подальшого нарощування відмовостійкого кластеру в конфігураціях N+1 або N+N із збереженням єдиної точки ліцензування, управління та моніторингу
 |
| Інтерфейси вводу/виводу | * Не менше 8 (восьми) комбінованих портів 10/100/1000BASE-T/SFP.
* USB 2.0 - 1 порт
* Console – 1 порт mini USB, RJ-45
 |
| Підтримувані режими роботи бездротової мережі | * Централізований, з тунелюванням всього трафіку користувачів бездротової мережі на контролер;
* За встановленими політиками – трафік користувачів бездротової мережі тунелюється на контролер або комутується в мережу безпосередньо точкою доступу в залежності від типу трафіку і встановлених адміністратором політик
 |
| Підтримка функцій та протоколів моніторингу та управління | * Веб-інтерфейс управління (HTTP/HTTPS)
* CLI інтерфейс управління
* SSH
* Протокол SNMP v2с, v3;
* Системний журнал та передача записів системного журналу за протоколом Syslog відповідно до встановлених адміністратором правил;
* Централізована система управління, що забезпечує додаткові можливості візуалізації та моніторингу бездротової мережі, зокрема відображення на плані поверху місцезнаходження бездротових клієнтів, потенційно зловмисних бездротових пристроїв, візуалізацію покриття бездротової мережі (heatmap).
 |
| Протоколи та функції управління радіочастотним ресурсом | * Автоматичний вибір оптимальних радіочастотних каналів та рівнів потужності випромінювання між точками під управлінням контролера;
* Підтримка управління радіочастотними параметрами для мереж 802.11n (HT20, HT40) та 802.11ac (VHT20, VHT40, VHT80, VHT160)
* Автоматичне переведення клієнтських пристроїв, що підтримують роботу в двох діапазонах 2,4 та 5 ГГц в менш завантажений частотний діапазон (band steering);
* Автоматичне динамічне регулювання потужності випромінювання та радіочастотних каналів точок кластеру в разі відмови однієї з точок кластеру або змін в оточенні для усунення зон із поганим покриттям;
* Оптимальне розділення ефірного часу між клієнтами, що підтримують різні стандарти 802.11 з можливістю рівного розділення часу між клієнтами, або пріоритетного доступу для клієнтів що підтримують найбільш нову версію стандарту 802.11 (airtime fairness)
* Можливість встановлення доступності мережі за розкладом з відключенням радіо точок в неробочій час;
* Можливість відстеження бездротовою мережею місцезнаходження та переміщення підключеного клієнтського пристрою в реальному часі з відображенням його місцезнаходження на плані поверху в системі управління (не включено в пропозицію) або експорту в зовнішні додатки через API.
 |
| Протоколи та функції безпеки | * Підтримка автентифікації IEEE 802.1X (як мінімум повинні підтримуватись методи EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-GTC, EAP-TLV, EAP-MD5).
* RFC 2548 Microsoft vendor-specific RADIUS attributes
* RFC 2716 PPP EAP-TLS
* RFC 2865 RADIUS authentication
* RFC 3579 RADIUS support for EAP
* RFC 3580 IEEE 802.1X RADIUS guidelines
* RFC 3748 extensible authentication protocol
* MAC address authentication
* Можливість автентифікації гостей з вбудованого веб-порталу (captive portal), або перенаправлення на зовнішній веб-портал
* Підтримка серверів автентифікації:
* Внутрішня база (локальна автентифікація)
* LDAP/SSL secure LDAP сервер
* RADIUS сервер
* TACACS+ сервер
* Підтримка протоколів IPsec з методами автентифікації X.509 PKI, IKEv2, IKE PSK, IKE aggressive для встановлення захищених тунелів між контролером та віддаленими точками доступу, що підключаються через незахищені мережі зовнішніх операторів зв’язку та ін
* Наявність міжмережевого екрану з контролем стану з’єднання та розпізнаванням програмних додатків (шляхом використання функціональності глибокого аналізу пакетів (DPI) для трафіку бездротових користувачів з можливістю створення політик, що враховують додаток або категорію додатків, тип клієнтського пристрою та класи користувачів.
* Можливість визначення типу та ОС клієнтського пристрою за непрямими ознаками (OS Fingerprinting);
* Бездротова система запобігання вторгненням (wIPS);
* Підтримка отримання значення ролі від ClearPass для встановлення необхідних обмежень для клієнтського пристрою;
* Підтримка профайлінгу за допомогою функціоналу IF-MAP;
 |
| Протоколи та функції якості обслуговування | * Балансування клієнтів/навантаження між всіма радіо та каналами точок бездротової мережі під управлінням контролеру;
* Динамічний вибір та асоціація клієнта з оптимальної для нього точкой доступу;
* Можливість призначення політик якості обслуговування для SSID або групи користувачів
* Можливість створення політик якості обслуговування, що враховують додаток або категорію додатків тип клієнтського пристрою та класи користувачів, в тому числі обмеження пропускної здатності для не бізнес-критичних категорій додатків (соціальні мережі, пірінгові мережі)
 |
| Протоколи та функції мобільності та роумінгу | * Підтримка безшовного роумінгу клієнтів між точками під управлінням контролеру;
* Підтримка безшовного роумінгу клієнтів між точками під управлінням різних контролерів в кластері;
* Підтримка можливості роумінгу між підмережами та VLAN
 |
| Протоколи та функції L2 | * Віртуальні локальні мережі VLAN (IEEE 802.1Q)
* Протокол IEEE 802.1ab (LLDP);
* Протокол агрегації з’єднань IEEE 802.3ad (LACP)
* Протокол Spanning Tree (стандарти IEEE 802.1D STP, IEEE 802.1w (RSTP))
 |
| Протоколи та функції L3 | * Статичні маршрути;
* Протоколи динамічної маршрутизації: OSPFv2
* Протокол резервування віртуальных маршрутизаторів IPv4 (VRRP);
 |
| Функції відмовостійкості та високої доступності | * Можливість створення кластерів високої доступності з синхронізацією стану пристроїв. Підтримуються режими:
* 1+1 Активний/Резервний
* 1+1 Активний/Активний
* N+1
 |
| Додатковий функціонал для моніторингу та управління | * Система підтримує управління і моніторинг всього мережевого обладнання, що включені до даної пропозиції, а також має як мінімум базові можливості моніторингу мережевим обладнанням третіх виробників (моніторинг мультивендорною мережею);
* Система повинна мати можливість відмовостійкого впровадження;

Крім цього, система повинна виконувати:* Побудову та графічне відображення топології мережі на різних рівнях;
* Моніторинг продуктивності мережі в режимі реального часу, швидка ідентифікація найбільш завантажених ділянок та пристроїв мережі;
* Інвентаризацію пристроїв, управління версіями конфігурацій та ОС пристроїв, засоби порівняння конфігурацій, резервне копіювання, відновлення і відкат;
* Збір, фільтрацію та аналіз подій системних журналів пристроїв;
* Генерацію звітів, з використанням системних та створених користувачем шаблонів, можливість запуску за розкладом та автоматичного відправлення звітів по електронній пошті;
* Виявлення збоїв та критичних проблем продуктивності в мережі, генерування аварійних сигналів, повідомлення адміністратора;
* Можливість масового конфігурування пристроїв (внесення пакетних змін до конфігурації групи пристроїв);
* Підтримку багатокористувацького управління на основі розподілу ролей.
* Підтримку карт для розміщення точок доступу на об’єктах, моделювання карт покриття та визначення місцеположення клієнтського пристрою;
* Підтримку аналізу поведінки несанкціонованих точок доступу та клієнтів, які можуть вплинути на роботу бездротової мережі Замовника (wIPS);
* Функціонал контролера повинен підтримувати управління мінімум 30 бездротовими пристроями
 |
| Гарантія та Сервісна підтримка | * Обладнання повинно забезпечуватись гарантією та сервісною підтримкою від учасника строком не менше ніж на 12 місяців з дати поставки обладнання.
* Умови сервісної підтримки обладнання повинні включати в себе можливість реєстрації сервісних випадків в режимі 24 год х 7 днів на тиждень, протягом гарантійного строку, доставку і заміну неякісного обладнання протягом 4-х годин з моменту отримання звернення від Замовника.
* Можливість скачування та оновлення програмного забезпечення та мікрокодів.
 |

**2. Комутатор – 10 шт.**

| **Найменування** | **Вимоги** |
| --- | --- |
| Форм-фактор та архітектура: | * Комутатор фіксованої конфігурації
 |
| Характеристики продуктивності комутатора: | * Максимальна продуктивність комутації/маршрутизації на систему: 41,7 млн. пакетів / с
* Максимальна пропускна спроможність переадресації на систему: 56 Гбіт / с
 |
| Наявність інтерфейсів наступних типів: | * 24 інтерфейсів 10/100/1000 Base-T з підтримкою РОЕ+
* 4 інтерфейси 1G SFP
 |
| Характеристики масштабованості: | * Максимальна кількість записів MAC-адрес: 32 000
* Максимальна кількість IPv4/IPv6 маршрутів: 2 000 / 1 000
 |
| Підтримка протоколів та функцій рівня 2:  | * Віртуальні локальні мережі VLAN (IEEE 802.1Q) - 4,094 ID, 2048 активних;
* Протокол Spanning Tree (стандарти IEEE 802.1D STP, IEEE 802.1w (RSTP), IEEE 802.1s (MSTP));
* Протокол Multiple VLAN Registration Protocol (MVRP);
* Функції відслідковування повідомлень протоколів управління багатоадресними групами та оптимізації багатоадресного трафіку (IGMP snooping та MLD snooping);
* Протокол агрегації з’єднань IEEE 802.3ad (LACP)
* Протокол IEEE 802.3x, управління потоком даних;
* Протокол IEEE 802.1AB (LLDP) та розширення LLDP-MED ;
* Підтримка надвеликих (Jumbo) фреймів розміром 9К
 |
| Підтримка протоколів та функцій рівня 3: | * Статичні маршрути для IPv4/IPv6;
* Протоколи маршрутизації IPv4: RIP, OSPF (для використання комутатору в режимі L3 доступу);
* Протоколи маршрутизації IPv6: RIPng, OSPFv3 (для використання комутатору в режимі L3 доступу);
* Протокол резервування віртуальных маршрутизаторів IPv4/IPv6 (VRRP/VRRPv3);
* Балансування трафіку за маршрутами з однаковою метрикою (ECMP);
* Маршрутизація за призначеними політиками (PBR);
* Протокол реєстрації багатоадресних груп (IGMP), з підтримкою версій IGMP v1, v2, v3;
* Протокол багатоадресної маршрутизації PIM для IPv4 та IPv6, включаючи PIM-DM, PIM-SM;
* Сервер DHCP;
* Підтримка віртуалізації Virtual Extensible LAN (VXLAN) - VXLAN L2 шлюз
 |
| Підтримка протоколів та функцій безпеки: | * Списки контролю доступу для вхідного та вихідного трафіку, що дозволяють використовувати поля заголовків рівня 3 та 4;
* Функцій захисту від атак на протокол STP: Root guard, BPDU port protection
* Функцій захисту від атак на протоколу ARP: захист від атак типу ARP poisoning
* Функцій Port security: обмеження кількості МАС адрес на порту, прив’язка МАС до порту, блокування неавторизованих МАС адрес;
* Функцій захисту протоколу DHCP: блокування DHCP пакетів від неавторизованих DHCP серверів
* Протоколи автентифікації, авторизації та обліку (ААА): RADIUS, TACACS+;
* VLAN з ізоляцією користувачів (Private VLAN);
* Підтримка методів автентифікації користувачів: 802.1X, WEB автентифікації, та MAC автентифікації;
* Керування доступом на основі визначених ролей;
* Системний журнал;
* Захищений протокол віддаленого керування SSHv2 для доступу в режимі CLI, та HTTPS для доступу до графічного інтерфейсу керування
* Функції захисту Control Plane комутатора від атак типу «відмова в обслуговуванні» (Control Plane Policing)
 |
| Підтримка протоколів та функцій якості обслуговування: | * Підтримка приорітезації IEEE 802.1p,
* Підтримка класифікації трафіка за критеріями: значення полів IEEE 802.1p, IP precedence, Type of Service (ToS), DSCP, IP адреса, протокол L3, порт-джерело трафіку, номери портів TCP/ UDP;
* Дії для трафіку, що відповідають умовам класифікатору: обмеження швидкості, ремаркування;
* Можливість встановлення обмеження швидкості на порту для всього або певних видів трафіку, в тому числі: широкомовний трафік, багатоадресний трафік, ICMP трафік, одноадресний трафік до адреси призначення, що відсутня в таблиці комутації (unknown unicast);
* Дисципліни якості обслуговування: Strict Priority Queuing (SPQ), Priority Queuing (PQ) із можливістю встановлення гарантованих мінімумів пропускної здатності доступних кожній черзі;
 |
| Підтримка віртуалізації комутаторів: | * N:1 віртуалізація: можливість об’єднання декількох комутаторів в один віртуальний пристрій (стек), що має єдине управління, виглядає як один вузол для мережевих протоколів L2/L3, в тому числі можливість крос-шасі LACP агрегації з’єднань до іншого активного обладнання;
* Повинна підтримуватись можливість об’єднання в стек не менше 8 комутаторів.
 |
| Підтримка функцій та протоколів моніторингу та управління: | * Інтерфейс командного рядку (CLI)
* Протокол SNMP v1, v2, v3;
* Протокол sFlow (RFC 3176);
* Протокол Remote monitoring (RMON);
* Протокол синхронізації часу Network Time Protocol (NTP);
* Системний журнал та передача записів системного журналу за протоколом Syslog відповідно до встановлених адміністратором правил;
* Наявність засобів автоматизації конфігурування пристрою з системи централізованого управління без початкового настроювання адміністратором (zero-touch provisioning);
* Дзеркалювання трафіку (створення копії трафіку що відповідає визначеним умовам (інтерфейс, MAC-адреса, VLAN, поля L3 заголовку) та передача його на локальний або віддалений порт моніторингу);
* Протокол OpenFlow версії не нижче 1.3.
* Підтримка управління з хмарного сервісу виробника
 |
| Простір, який займається у серверній шафі: | * 1 U
 |
| Гарантія / сервісна підтримка у складі пропозиції: | * Обмежена пожиттєва гарантія;
* Включає заміну компонент, що вийшли з ладу, доступ до оновлень ПЗ, віддалену діагностику та підтримку з боку центру технічної підтримки виробника в режимі 8 х 5
 |

**3****. Пристрій мережевої безпеки (брандмауер) – 1 шт.**

| **Найменування** | **Вимоги** |
| --- | --- |
| **Загальні вимоги** | * Якщо відповідно до функціональності пристроїв/систем або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем (кластеризації) або ліцензій, то все це має бути закладено в комплект поставки з урахуванням вимог до строку та функціональності технічної підтримки
* 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 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 рішення
 |
| **Мережеві інтерфейси** | * Не менше ніж 16х GE RJ45
* Не менше ніж 8х GE SFP інтерфейсів та не менше ніж 2хSFP SX 1 GE модуля до них
* Не менше ніж 8х 10 GE SFP+
* Не менше ніж 2х GE RJ45 WAN
* Не менше ніж 2х GE RJ45 Management/HA
* Не менше ніж 1х USB Port
* Консольний порт 1x RJ45
 |
| **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 здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 8 Гбіт/c
 |
| **Продуктивність VPN** | * Пропускна здатність IPSec VPN: не менше ніж 55 Гбіт/c
* Пропускна здатність SSL VPN: не менше ніж 3,6 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 2000
 |
| **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
 |
| **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, DNS та Video-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
 |
| * **Web, DNS та Video-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)
* Інспектування Video контенту Youtube та можливість блокування його на основі відношення до певної категорії або каналу (Video-фільтрація)
* Виявлення та блокування доступу до Botnet мереж
* Блокування певних небезпечних елементів web-сайтів (Java Applet, ActiveX scripts, тощо)
* Статичні blacklists та whitelists
 |
| **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)**  | * Відправка файлів з користувацького трафіку на аналіз у cloud sandbox для виявлення невідомих загроз класу "0-day"
* Ліцензування має дозволяти аналізувати у cloud sandbox не менше ніж 14 000 файлів на день (24 години)
 |
| **Запобігання витоку даних (Data Loss Prevention)** | * Запобігання витоку конфіденційних даних шляхом перевірки трафіку (за назвою файлів, типом файлів, розміром файлів, регулярними виразами)
* Запобігання витоку конфіденційних даних шляхов перевірки трафіка за допомогою бази даних заздалегідь визначеної інформації такої як: тип даних, словники та сенсори (credit card numbers, SIN numbers, тощо) (за умови додаткового ліцензування)
* 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: 5, 14, 19, 27, 32
* Підтримка Hub & Spoke топології, Spoke & Spoke (mesh) топології
* Агрегація IPSec тунелів
* DMVPN/ADVPN або аналог
 |
| **QoS** | * Traffic Shaping
* Traffic Policing
 |
| **Маршрутизації та SD-WAN** | * Статична маршрутизація та маршрутизація по політиках
* Динамічні протоколи маршрутизації: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4
* 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 з 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
 |
| **Автентифікація, авторизація та облік (AAA)** | * Локальна база даних користувачів
* Підтримка протоколів LDAP, RADIUS, TACACS+
* Підтримка 2-факторної автентифікації (two-factor authentication)
* 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
* 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
* Підтримка інтеграції з системами типу SIEM
 |
| **Технічна сервісна підтримка** | * Обладнання повинно забезпечуватись технічною сервісною підтримкою строком не менше ніж 36 місяців
* 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 веб-додатків 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)
 |