ОБҐРУНТУВАННЯ
технічних та якісних характеристик предмета закупівлі, розміру бюджетного призначення, очікуваної вартості предмета закупівлі

Предмет закупівлі та її номер: **«Мережеве обладнання» (UA-2021-10-28-009669-a)**

Технічні та якісні характеристики предмета закупівлі

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.

1. **Міжмережевий екран наступного покоління (NGFW) з необхідним набором ліцензій (1 рік) та сервісною технічною підтримкою (24*7, 1 рік) - 1 шт.**

№ з/п	Назва	Вимоги
1.	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; • Якщо відповідно до функціональності пристроїв/систем або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем (кластеризації, маршрутизатори, комутатори) 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;
2.	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.
3.	Мережеві інтерфейси	• Не менше ніж 12 * GE RJ45; • Не менше ніж 4 * GE SFP; • Не менше ніж 1 * USB; • Не менше ніж 1 консольний порт; • Не менше ніж 2 * GE RJ45 порт керування; • Не менше ніж 2 * 10 GE SFP+.
4.	Продуктивність сервісів безпеки	• Пропуска здатність сервісу Stateful Firewall (на пакетах розміром 1518 байт, UDP): не менше ніж 20 Гбіт/с; • Кількість одночасних TCP-сесій: не менше ніж 1 500 000; • Кількість нових TCP-сесій/секунду: не менше ніж 56 000; • Пропуска 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 1 Гбіт/с; • Пропуска здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 1,8 Гбіт/с.
5.	Продуктивність VPN	• Пропуска здатність IPSec VPN: не менше ніж 11,5 Гбіт/с; • Кількість одночасних SSL VPN підключень до шлюзу: не менше ніж 500; • Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 16 000; • Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 2 000.
6.	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.
7.	Висока доступність (high availability)	• Active-Active; • Active-Standby.
8.	L2 функціонал та мережеві служби	• Агрегація портів (802.3ad); • VLAN (802.1Q та Trunking); • Вбудований DHCP, NTP, DNS-сервера;
9.	NAT	• Статичний NAT; • Динамічний NAT; • PAT.
10.	Multicast	• Sparse та dense режим; • Підтримка PIM.
11.	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; • Інспектування/сканування SSL/TLS трафіку на загрози; • Захист від невідомих загроз (0-day); • Запобігання витоку даних (DLP); • Захист від DOS-атак; • IPSec VPN, SSL VPN.
12.	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).
13.	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.
14.	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).
15.	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.
16.	Web 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 whitelists.

17.	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 certificate inspection); • Повноцінне інспектування контенту зашифрованих сесій (full SSL/TLS inspection); • Інспектування SSL/TLS-трафіка має включати наступні інспекції: IPS, AC/AVC, AV/AMP, Web-фильтрацію, DLP.
18.	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 10 000 файлів на день (24 години).
19.	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.
20.	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.
21.	IPSec VPN, SSL VPN	• Алгоритми шифрування: 3DES, AES128, AES192, AES256; • Алгоритми хешування: MD5, SHA256, SHA384, SHA512; • Diffie-Hellman Group: 1, 2, 5, 14; • Підтримка Hub & Spoke топології, Spoke & Spoke (mesh) топології, DMVPN/ADVPN або аналог.
22.	QoS	• Traffic Shaping; • Traffic Policing.
23.	Маршрутизації та SD-WAN	• Статична маршрутизація та маршрутизація по політиках (PBR); • 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 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.
24.	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.
25.	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.

26.	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 в м. Київ (обладнання для заміни доставляється наступного дня після підтвердження заміни сервісом підтримки виробника).

2. **Високопродуктивний мережевий екран наступного покоління (NGFW) з необхідним набором ліцензій (1 рік) та сервісною технічною підтримкою (24*7, 1 рік) - 1 шт.**

№ з/п	**Назва**	**Вимоги**
1.	Архітектура та форм-фактор	• Desktop.
2.	Мережеві інтерфейси	• Не менше, ніж: 2/1x GE RJ45 - WAN/DMZ; • Не менше, ніж: 7x GE RJ45 LAN; • Порт керування: 1x RJ-45 Serial Console Port; • USB порт: 1x; • Wireless Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2.
3.	Загальна продуктивність	• Пропускна здатність IPv4 (1518/512/64 byte UDP) - не менше, ніж: 10/10/6 Gbps; • Кількість одночасних TCP-з’єднань - не менше, ніж: 700 000; • Кількість нових TCP-з’єднань/сек. - не менше, ніж: 35 000; • Максимальна кількість політик - не менше, ніж: 5 000; • Пропускна здатність AppControl - не менше, ніж: 1.8 Gbps; • Пропускна здатність IPS - не менше, ніж: 1.4 Gbps; • Комплексна пропускна здатність (IPS+AppControl+AV) Enterprise Traffic Mix: не менше ніж: 700 Mbps; • Віртуальні домени - не менше, ніж: 10; • Підтримка керування комутаторами – не менше, ніж: 16; • Підтримка керування WiFi-точками доступу (всього/у режимі тунелю) – не менше, ніж: 64/32; • Пропускна спроможність між пристроєм та WiFi-точками доступу (CAPWAP, HTTP 64K) – не менше, ніж: 8 Gbps.
4.	Продуктивність VPN	• Пропускна здатність IPSec VPN (512 byte, AES256-SHA256) - не менше, ніж; 6.5 Gbps; • Кількість IPSec тунелів типу шлюз-шлюз - не менше, ніж: 200;

		• Кількість IPSec тунелів типу клієнт-шлюз - не менше, ніж: 500; • Кількість конкурентних SSL VPN - не менше, ніж: 200; • Пропускна здатність SSL VPN - не менше, ніж: 900 Mbps.
5.	Протоколи канального рівня	• Режими роботи Layer-2 інтерфейсів: aggregated, loopback, VLANs (802.1Q and Trunking), virtual hardware, software, and VLAN switches; • Підтримка VXLAN та interVTEP (VXLAN Tunnel End Point); • Підтримка EMAC-VLAN: додавання декілька MAC-адрес на один фізичний інтерфейс; • Функціонал Virtual Wire Pair: обробка трафіку лише між двома призначеними інтерфейсами в одному мережевому сегменті.
6.	Мережеві служби та технології	• Підтримка протоколів: SCTP, TCP, UDP, ICMP, IP; • Статична маршрутизація та маршрутизація на основі політик; • Протоколи динамічної маршрутизації: RIPv2, OSPF v2/v3, IS-IS, BGP4; • Multicast трафік: режими sparse та dense, підтримка PIM; • Підтримка IPv6: можливість керування системою по протоколу IPv6, маршрутизація IPv6, тунелювання IPv6, мережевий екран та UTM для трафіку IPv6, NAT46, NAT64, IPv6 IPsec VPN. • Об'єкти: підмережі, IP-діапазони, GeoIP, FQDN; • Режими роботи: NAT/маршрутизатор та transparent bridge; • Режими NAT: за політикою/за центральною таблицею NAT; • Підтримка NAT: NAT64, NAT46, статичний/динамічний NAT, PAT, Full Cone NAT, STUN; • Вбудований DHCP-, NTP- та DNS-сервери; • Шейпінг трафіку і QoS: загальна політика шейпінгу, IP шейпінг, максимальна і гарантована пропускна здатність, максимальна кількість одночасних підключень на IP, пріоритезація трафіка, Type of Service (TOS) і Differentiated Services (DiffServ); • Session helpers & ALGs: dcerpc, dns-tcp, dns-udp, ftp, H.245 I, H.245 0, H.323, MGCP, MMS, PMAP, PPTP, RAS, RSH, SIP, TFTP, TNS (Oracle); • Підтримка VoIP трафіку: SIP/H.323 /SCCP NAT traversal, RTP; • Підтримка SD-WAN: балансування навантаження між каналами зв’язку та їх резервування з перевіркою стану з’єднання; • Підтримка USB 3G/4G модемів LTE; • Можливість створення віртуальних серверів, перевірки їх стану та балансування навантаження між ними, використовуючи різні методи (Round Robin, Weighted, Least Session та ін.), а також, підтримка функції мультиплексування HTTP; • Підтримка створення віртуальних повнофункціональних апплайнсів та можливість обміну данних між ними на рівнях L2-L3 (VDOM); • Створення адміністративних доменів для окремих адміністраторів системи із власними правами та налаштуваннями (ADOM);

		• Централізоване налаштування та можливість інспектування трафіку точок доступу WiFi, а також моніторинг їх роботи та трафіку під'єднаних до них користувачів.
7.	Аутентифікація та PKI	• Локальна база даних користувачів; • Підтримка протоколів аутентифікації: LDAP, Radius, TACACS+; • Single-Sign-On: Windows AD, Novell eDirectory; • 2-факторна аутентифікація: інтегрований токен-сервер, підтримка фізичних та програмних токенів; • Ідентифікація пристроїв: розпізнавання пристроїв та операційних систем користувачів, іх автоматична класифікація; • Підтримка налаштування політик доступу пристроїв та користувачів; • PKI і сертифікати: підтримка сертифікатів стандарту X.509, SCEP, CSR, створення та автоматичне оновлення сертифікатів до закінчення їх підтримки, OCSP; • Інспекція SSL трафіку: - Підтримка режимів роботи Full SSL Inspection та Certificate Inspection Only; - Можливість робити виключення для перевірки сертифікатів відомих сервісів; - Гнучкі налаштування поведінки пристрою для сертифікатів, які не проходять перевірку валідації; • Інспекція SSH трафіку.
8.	Параметри VPN	• IPSec VPN: - Підтримка віддалених пірів: IPSec-compliant clients/devices зі статичною IP-адресою та/або динамічним DNS; - Методи аутентифікації пірів: certificate, pre-shared key; - Режими IPSec Phase 1: aggressive та main (ID protection); - Опції допуску пірів: any ID, specific ID, dialup user group ID; - Підтримка IKEv1, IKEv2 (RFC 4306); - Підтримка IKE mode configuration (як сервер або клієнт), DHCP over IPSec; - Протоколи шифрування: DES, 3DES, AES128. AES192, AES256; - Протоколи хешування: MD5, SHA1, SHA256; SHA384, SHA512; - Групи Diffie-Hellman: 1, 2, 5, 14; - Підтримка функції XAuth в режимі сервера або клієнта (PAP, CHAP, Auto), NAT Traversal; - Можливість змінювати параметри: IKE encryption key expiry, NAT traversal keepalive frequency; - Підтримка функцій: Dead peer detection, Replay detection; - Режими роботи IPSec: gateway-to-gateway, hub-and-spoke, full mesh, redundant-tunnel, VPN in transparent mode; - Опції налаштування IPSec VPN: route-based або policy-based. • SSL VPN: - Можливість кастомізації SSL VPN порталів: color themes, layout, bookmarks, connection tools, client download, SSL VPN realms;

		- Надання можливості користувачам самостійно кастомізувати сторінку свого SSL VPN порталу; - Можливість обмеження доступу користувачів до SSL VPN порталу, в разі невідповідності вимогам політик безпеки; - В разі використанння користувачем лише веб-браузера при роботі з SSL VPN-порталом (web mode), повинна підтримуватися робота наступних протоколів: - HTTP/S, FTP, Telnet, SMB/CIFS, SSH, VNC, RDP, SOCKS; - В разі використанння користувачем VPN-клієнта при роботі з SSL VPN-порталом (tunnel mode), повинні підтримуватися наступні операційні системи: MAC OSX, Linux, Windows; - Перевірка MAC-адреси пристрою користувача на порталі; - Очищення кешу перед завершенням сесії SSL VPN; - Детальний моніторинг: IPSec- та SSL VPN-з'єднань; - Підтримка інших протоколів: L2TP клієнт/сервер, L2TP over IPSec, PPTP, GRE на IPSEC.
9.	Контроль додатків	• Категорії додатків: Botnet, Collaboration, Email, File Sharing, Game, General Interest, Network Service, P2P, Proxy, Remote Access, Social Media, Storage Backup, Update, Video/Audio, VoIP, Industrial, Web Applications та інші; • Доступні фільтри додатків: за поведінкою, категоріями, популярністю, технологією, ризиком, постачальником; • Режими роботи: monitor, allow, block, quarantine; Використання ISDB.
10.	Механізми захисту від загроз	• IPS: - Режими роботи: pass, monitor, block, reset або quarantine; - Вибір сигнатур на основі фільтрів: критичність, ціль, OS, додаток та/або протокол; - Опція логування заблокованих пакетів; - Можливість створення кастомних сигнатур; - Підтримка виключень для визначених IPS сигнатур; - Блокування IP-адрес Botnet-серверів використовуючи глобальну репутаційну базу даних (IP-reputation). • Антивірус: - Підтримка інспекції протоколів: HTTP/HTTPS, SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS, MAPI, FTP/SFTP, ICQ, YM, NNTP - Підтримка хмарного сервісу для аналізу поведінки файлів (Sandbox); - Підтримка чорних та білих списків для файлів; - Евристичне сканування; - Можливість отримання динамічних сигнатур для блокування загроз нульового дня, які було зафіксовано окремими службами аналітики; - Можливість видаляти з файлів (PDF, Microsoft Office) зловмисний код або посилання, залишаючи при цьому оригінал файлу незмінним. • DNS-фільтрація: - Статична DNS-фільтрація на основі створених фільтрів та чорних списків;

		- Динамічна DNS-фільтрація з використанням хмарної бази даних в реальному часі. • Веб-фільтрація: - Статична веб-фільтрація на основі URL, веб-контенту та заголовка MIME; - Динамічна веб-фільтрація з використанням хмарної бази даних в реальному часі; - Функція safe search: підтримка Google, Yahoo!, Bing і Yandex; - Інспекція Java Applet, ActiveX та cookie; - Можливість блокування різних HTTP-методів (POST, PUSH); - Підтримка рейтингу зображень по URL; - Блокування HTTP Redirects та HTTP POST; - Можливість обмеження трафіку (квотування) за категоріями; - Веб-фільтрація кастомних категорій та в обхід категорій; - Веб-фільтрація в обхід профілю: дозволяє адміністратору тимчасово призначити різні профілі для користувачів/груп користувачів/IP. • Антиспам: - Підтримка чорних та білих списків за параметрами: IP/Netmask, Email Wildcard, Email Regular Expression; - Підтримка інспектування протоколів: SMTP, POP3, IMAP; - Перевірка відправника пошти за репутаційною базою; - Перевірка URL у повідомленнях: за базою зловмисних та фішингових URL; - Перевірка контрольних сум повідомлень; - Перевірка повідомлень локальних користувачів: HELO DNS Lookup, Return Email DNS Check; - Фільтрація файлів за типом розширення. • DLP: - Підтримка інспектування протоколів: HTTP-POST, SMTP, POP3, IMAP, MAPI, NNTP; - Підтримка інспекції тексту повідомлень та тексту файлів; - Режими роботи: allow, block, quarantine IP/Interface; - Фільтрація об’єктів, що інспектуються за: розміром файлу, типом файлу, змістом, наявністю шифрування; - Інспекція об’єктів по водяних знаках: фільтрування файлів, що містять у собі корпоративний ідентифікатор. • Профіль захисту VOIP: - Можливість лімітувати запити за їх типом (REGISTER, INVITE); - Можливість лімітувати запити SCCP дзвінки. • Web Proxy: - Пітримка режимів роботи Proxy: Explicit та Transparent; - Підтримка інспектування протоколів: HTTP/S, SMTP, POP3, IMAP, MAPI, NNTP, FTP, DNS; - Підтримка кешування веб-контенту; - Підтримка PAC-файлів та протоколу WPAD; - Переадресація веб-проксі сеансів на інші проксі-сервери. • Web Application Firewall: - Можливість запобігання атак, спрямованих на веб-сервери, завдяки базі даних сигнатур;

		- Перевірка HTTP-запитів на відповідність RFC; - Обмеження та контроль параметрів у запитах користувачів. • Захист від DoS/DDoS атак: - IPv4 та IPv6 захист від сканування та DOS/DDoS-атак, таких як: TCP Syn flood, TCP / UDP / SCTP port scan, ICMP sweep, TCP / UDP / SCTP / ICMP flood (source/destination) та ін., шляхом обмежень кількості трафіку відповідних протоколів для кожного окремого користувача. • Підтримка протоколу ICAP в режимах request, response та streaming; • Можливість об'єднання з іншими пристроями інформаційної безпеки у єдину мережу, з метою обміну даними про підозрілу та шкідливу мережеву активність.
11.	Відмовостійкість	• Режими HA: активний-пасивний, активний-активний; • Моніторинг з'єднань та стану портів; • Можливість синхронізування конфігурації пристроїв, таблиці маршрутів, таблиці з'єднань та ін. • Підтримка протоколу VRRP; • Підтримка кластеризації між віртуальними пристроями (VDOM); Підтримка кластеризації на основі геолокації.
12.	Керування, контроль і діагностика	• Підтримка доступу до системи: HTTPS, SSH, Telnet, консоль; • Підтримка централізованого керування окремими спеціалізованими системами; • Підтримка протоколів моніторингу (SNMPv1,2,3) та логування Syslog (CEF), підтримка механізму reliable syslog; • Підтримка протоколів sFlow v5 та Netflow v9.0; • Надсилання повідомлень на електронну пошту користувача в разі відбування подій безпеки, та можливість самостійного визначення критичності відповідних подій; • Категоризація логування за основними категоріями: - Forward Traffic; - System Events; - Security Events (для кожного механізму захисту окремо). • Можливість швидкого впровадження: майстер налаштування, автоматичне налаштування чеерз USB, виконання локальних і зовнішніх сценаріїв; • Панель з динамічними віджетами моніторингу подій безпеки, активністю користувачів, навантаженості системи; • Моніторинг окремих подій за основними категоріями: - Маршрути (статичні та динамічні); - DHCP; - SD-WAN; - Load Balance; - IPSec VPN; - SSL VPN; - User Monitor.
13.	Гарантія та Сервісна підтримка	• Обладнання повинно забезпечуватись гарантією від виробника та сервісною підтримкою строком не менш ніж 12 місяців; • Умови сервісної підтримки повинні включати в себе 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 сервісного випадку сервісом підтримки виробника), оновлення мікрокоду системи і версій встановленого програмного забезпечення.
14.	Складові сервісної підтримки	• Отримання актуальних репутаційних баз, баз ботнетів та всіх необхідних оновлень; • Отримання основних та проміжних релізів програмного забезпечення через сайт, підтримка програмних кодів у актуальному стані відповідно до рекомендацій виробника, в тому числі мікрокодів пристроїв; • Надання консультацій по телефону, електронній пошті та на сайті підтримки виробника по питаннях установки, конфігурування і експлуатації обладнання з понеділка по неділю з 00.00 до 24.00 годин цілодобово; • Постійний (24*7) авторизований доступ до сайту виробника.

3. **Комутатор рівня доступу з необхідним набором ліцензій (1 рік) та сервісною технічною підтримкою (24*7, 1 рік) - 1 шт.**

№ з/п	Назва	Вимоги
1.	Архітектура та форм-фактор	• Зовнішній - для встановлення в стандартну монтажну шафу 19", висота 1U.
2.	Мережеві інтерфейси	• Не менше, ніж 48x GE RJ45; • Не менше, ніж 4x 10GE SFP; • Порти керування: 1x dedicated 100Mbps RJ45; 1x RJ-45 Serial Console Port. • PoE budget не менше, ніж 180W.
3.	Продуктивність	• Комутаційна здатність - не менше, ніж: 176 Gbps; • Кількість пакетів в секунду - не менше, ніж: 262M; • Загальна кількість MAC-адрес - не менше, ніж: 32 000; • Затримка - менше, ніж (µs): 1; • Кількість VLAN - не менше, ніж: 4096; • Кількість портів в LAG групі - не менше, ніж: 8; • DRAM - не менше, ніж: 1 GB; • Flash - не менше, ніж: 256 MB. • Packet Buffer – не менше ніж 2 MB.
4.	Підтримка протоколів та стандартів канального рівня моделі OSI	• Jumbo Frames; • IEEE 802.1D MAC Bridging/STP; • IEEE 802.1w Rapid Spanning Tree Protocol (RSTP); • IEEE 802.1s Multiple Spanning Tree Protocol (MSTP); • Edge Port / Port Fast; • IEEE 802.1Q VLAN Tagging; • Private VLAN; • IEEE 802.3ad Link Aggregation with LACP; • Unicast/Multicast traffic balance over trunking port (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac); • IEEE 802.1AX Link Aggregation; • Spanning Tree Instances (MSTP/CST); • IEEE 802.3x Flow Control and back-pressure; • IEEE 802.3 10Base-T; • IEEE 802.3u 100Base-TX; • IEEE 802.3z 1000Base-SX/LX;

		• IEEE 802.3ab 1000Base-T; • 802.3ae 10 Gigabit Ethernet; • 802.3 CSMA/CD Access Method and Physical Layer Specifications; • Storm Control; • MAC, IP, Ethertype-based VLANs; • Virtual-Wire; • IGMP Snooping (v1/v2/v3).
5.	Підтримка протоколів та стандартів мережевого рівня моделі OSI	• Статична маршрутизація; • DHCP Relay; • Протоколи динамічної маршрутизації RIPv2, OSPFv2, VRRP (можливе додаткове ліцензування).
6.	Безпека	• Port Mirroring; • Admin Authentication Via RFC 2865 RADIUS; • 802.1x authentication with port-based assignment; • 802.1x authentication with mac-based assignment; • sFlow; • ACL Tables; • Підтримка об’єднання пристрою у так звану фабрику безпеки рішеннями того же виробника, для виявлення потенційних вразливостей мережі та можливості їх усунення за допомогою протоколу SNMPv1,v2,v3; • Можливість автоматично ізолювати хости з підозрілою або зловмисною активністю.
7.	Управління	• Telnet / SSH; • HTTP / HTTPS; • SNMP v1/v2c/v3; • SNTP; • LLDP (802.1ab, Link Layer Discovery Protocol) (receive and transmit); • Standard CLI and web GUI interface; • Software download/upload: TFTP/FTP/GUI; • Support for HTTP REST APIs for Configuration and Monitoring; • Можливість використання аппаратних та віртуальних пристроїв, в якості централізованих систем керування.
8.	Трансивери	• В комплекті повинні бути наявні SFP+ LR та SR трансивери від того же виробника.
9.	DAC	• В комплекті повинні бути наявні SFP+ DAC кабелі довжиною 1,3,5 метрів від того же виробника.
10.	Підтримка RFC та MIB	• RFC 2571 Architecture for Describing SNMP Framework; • DHCP Client; • RFC 854 Telnet Server; • RFC 2865 RADIUS; • RFC 1643 Ethernet-like Interface MIB; • RFC 1213 MIB-II; • RFC 1354 IP Forwarding Table MIB; • RFC 2572 SNMP Message Processing and Dispatching; • RFC 1573 SNMP MIB II; • RFC 1157 SNMPv1/v2c; • RFC 2030 SNTP.
11.	Відмовостійкість	• Multi-Chassis Link Aggregation (MCLAG); • VRRP (можливе додаткове ліцензування).

12.	Гарантія та Сервісна підтримка	• Обладнання повинно забезпечуватись гарантією від виробника та сервісною підтримкою строком не менш ніж на 12 місяців • Умови сервісної підтримки повинні підтримувати 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 RMA сервісом підтримки) та оновлення мікрокоду системи і версій встановленого ПЗ.
13.	Складові сервісної підтримки	• Отримання основних та проміжних релізів програмного забезпечення через сайт або на фізичних носіях, підтримка програмних кодів у актуальному стані відповідно до рекомендацій Виробника, в тому числі мікрокодів пристроїв; • Надання консультацій по телефону, електронній пошті та на сайті підтримки виробника по питаннях установки, конфігурування і експлуатації обладнання з понеділка по неділю з 00.00 до 24.00 годин цілодобово; • Організація та виконання міграцій, оновлень в режимі безперервності функціонування системи Замовника; • Постійний (24/7) авторизований доступ до сайту виробника.

Розмір бюджетного призначення, очікувана вартості предмета закупівлі

Найменування	Одиниця виміру	Кількість	Загальна вартість, грн. з ПДВ
Міжмережевий екран тип 1	шт	1	424 000,00
Міжмережевий екран тип 2	шт	1	
Комутатор	шт	1	

Очікувана вартість послуг та розмір бюджетного призначення були визначені відповідно до службової записки Бєляєва О.О. б/н б/д, сформованої з використанням даних відкритих джерел, комерційних пропозицій тощо.

_____