**Обґрунтування**

**технічних та якісних характеристик предмета закупівлі
Код ДК 021:2015 32420000-3 Мережеве обладнання (Мережеве обладнання)**

**(номер / ідентифікатор закупівлі UA-2023-11-23-016400-a)**

Технічні та якісні характеристики предмета закупівлі та їх обґрунтування щодо позиції/позицій предмета закупівлі:

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Технічні (якісні) характеристики предмета закупівлі | Параметри технічних (якісних) характеристик предмета закупівлі | Обґрунтування технічних та якісних характеристик предмета закупівлі |
| 1 | 2 | 3 | 4 |
|  | **Міжмережевий екран** | **Міжмережевий екран** наступного покоління (NGFW) з необхідним набором ліцензій (1 рік) та сервісною технічною підтримкою (24\*7, 1 рік).Загальні вимоги:• Мережевий пристрій безпеки що пропонується, повинен являти собою міжмережевий екран наступного покоління (NGFW) та здійснювати інспекцію мережевого трафіку та захист інфраструктури відповідно до нижченаведених вимог• Якщо відповідно до функціональності пристроїв/систем або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то вони усі мають бути у комплекті поставки рішення 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• Обладнання повинне мати можливість керування наявною у замовника централізованою системою керування мережевими пристроями FortiManager. • Запропоноване обладнання повинне мати чинні експертні висновки Державної служби спеціального зв'язку та захисту інформації України на відповідність вимогам законодавства в галузі захисту інформації. Архітектура та форм-фактор:• Мережевий пристрій безпеки повинен являти собою програмно-апаратний комплекс (ПАК), висотою не більше ніж 1 RU.Інтерфейси:• Не менше ніж 10 \* 1 GE RJ45• Не менше ніж 1 \* USB• Не менше ніж 1 консольний портЖивлення:• 1 блок живлення (100-240V AC, 50-60 Hz)• Можливість підключення резервного блоку живленняПродуктивність сервісів безпеки:• Кількість одночасних TCP-сесій: не менше ніж 700 000• Кількість нових TCP-сесій/секунду: не менше ніж 35 000• Пропускна здатність для шаблону трафіку Enterprise traffic mix (з включеними сервісами FW+App Control+IPS+Malware Protection): не менше ніж 700 Мбіт/c• Пропускна здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 600 Мбіт/cПродуктивність VPN:• Пропускна здатність IPSec VPN: не менше ніж 6 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 10Висока 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)• 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 хмарною системою захисту від атак нульового дня (cloud sandbox) шляхом відправки об'єктів (файли, URL) для аналізу та отримання результатів інспектування• Ліцензія, що має дозволяти інспектувати у cloud sandbox не менше ніж 5 000 об'єктів на день (24 години), має бути у комплекті поставкиЗахист від DOS-атак:• Можливість розпізнавання та блокування DoS атак:  TCP Syn flood TCP/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• Підтримка Hub & Spoke топології, Spoke & Spoke (mesh) топології, DMVPN/ADVPN або еквівалентQoS:• Traffic Shaping • Traffic PolicingМаршрутизація та SD-WAN:• Статична маршрутизація та маршрутизація по політиках (PBR)• Динамічні протоколи маршрутизації: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4• 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 або пасивними методами• 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• Динамічне виправлення втрати пакетів або відновлювання пакетів з помилками, що викликані несприятливими умовами WAN-каналів під час роботи через VPN (Forward Error Correction)• Дуплікація пакетів через декілька каналів зв’язку з метою покращення роботи сервісів, що можуть бути викликані несприятливими умовами WAN-каналів під час роботи через VPN• Балансування пакетів однієї сесії через декілька IPSec VPN тунелівАвтентифікація, 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) у комплекті поставки• 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• 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 • 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) | Граничний пристрій безпеки. Для забезпечення контролю інформаційних потоків (трафіку) в мережі у віддалених підрозділах ДНДЕКЦ МВС. |
|  | **Міжмережевий екран** | **Міжмережевий екран** наступного покоління (NGFW) з необхідним набором ліцензій (1 рік) та сервісною технічною підтримкою (24\*7, 1 рік):**Загальні вимоги:*** Мережевий пристрій безпеки що пропонується, повинен являти собою міжмережевий екран наступного покоління (NGFW) та здійснювати інспекцію мережевого трафіку та захист інфраструктури відповідно до нижченаведених вимог
* Якщо відповідно до функціональності пристроїв/систем або згідно архітектурного підходу реалізація технічних вимог потребує додаткових пристроїв/систем або ліцензій, то вони усі мають бути у комплекті поставки рішення 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
* Обладнання повинне мати можливість керування наявною у замовника централізованою системою керування мережевими пристроями FortiManager.
* Запропоноване обладнання повинне мати чинні експертні висновки Державної служби спеціального зв'язку та захисту інформації України на відповідність вимогам законодавства в галузі захисту інформації.

**Архітектура та форм-фактор:****•** Мережевий пристрій безпеки повинен являти собою програмно-апаратний комплекс (ПАК), висотою не більше ніж 1 RU**Інтерфейси:*** Не менше ніж 8 \* 1 GE RJ45
* Не менше ніж 2 \* 1 GE SFP
* Не менше ніж 1 \* USB
* Не менше ніж 1 консольний порт

**Живлення:****•** 1 блок живлення (100-240V AC, 50-60 Hz)• Можливість підключення резервного блоку живлення**Продуктивність сервісів безпеки:*** Кількість одночасних TCP-сесій: не менше ніж 1 500 000
* Кількість нових TCP-сесій/секунду: не менше ніж 40 000
* Пропускна здатність для шаблону трафіку Enterprise traffic mix (з включеними сервісами FW+App Control+IPS+Malware Protection): не менше ніж 900 Мбіт/c
* Пропускна здатність під час інспекції SSL/TLS трафіку з використанням IPS: не менше ніж 700 Мбіт/c

**Продуктивність VPN*** Пропускна здатність IPSec VPN: не менше ніж 6 Гбіт/c
* Кількість одночасних SSL VPN підключень до шлюзу: не менше ніж 200
* Кількість одночасних клієнт-шлюз IPSec VPN підключень: не менше ніж 2 500
* Кількість одночасних шлюз-шлюз IPSec VPN підключень: не менше ніж 200

**Віртуалізація:**• Віртуальні FW, (Virtual Systems/Security contexts/Virtual Domains) що являють собою незалежні пристрої із власними політиками безпеки, інтерфейсами, адміністраторами, тощо: не менше ніж 10**Висока доступність (high availability):*** Active-Active
* Active-Standby

**L2 функціонал та мережеві служби:*** Агрегація портів (802.3ad)
* VLAN (802.1Q та Trunking)
* Вбудований DHCP, NTP, DNS-сервера

**NAT:*** Cтатичний NAT
* Динамічний NAT
* PAT

**Multicast:**• Sparse та dense режим• Підтримка PIM**Сервіси безпеки:*** Stateful Firewall
* Ідентифікація та контроль застосувань (AC/AVC)
* Захист від загроз на основі сигнатурного аналізу (IPS)
* Захист від malware (Antivirus/AMP)
* Web та DNS-фільтрація
* Iнспектування/сканування SSL/TLS трафіку на загрози
* Захист від невідомих загроз (0-day)
* 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 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

**SSL/TLS-інспекція*** Перехоплення, розшифрування та інспекція HTTPS, IMAPS, POP3S, SMTPS, FTPS-сесій
* Конфігурація виключень з SSL/TLS-інспекції певних IP-адрес, URL, тощо (exemption/override)
* Інспектування SSL/TLS-сертифікату на відповідність певному web-ресурсу до якого здійснюється підключення та строку дійсності (SSL/TLS сertificate іnspection)
* Повноцінне інспектування контенту зашифрованих сесій (full SSL/TLS іnspection)
* Інспектування SSL/TLS-трафіка має включати наступні інспекції: IPS, AC/AVC, AV/AMP, Web-фильтрацію, DLP

**Захист від невідомих загроз (0-day)** * Інтеграція з хмарною системою захисту від атак нульового дня (cloud sandbox) шляхом відправки об'єктів (файли, URL) для аналізу та отримання результатів інспектування
* Ліцензія, що має дозволяти інспектувати у cloud sandbox не менше ніж 5 000 об'єктів на день (24 години), має бути у комплекті поставки

**Захист від DOS-атак*** Можливість розпізнавання та блокування DoS атак:
* TCP Syn flood
* TCP/UDP/SCTP port scan
* ICMP sweep
* TCP/UDP/SCTP/ICMP session flooding

**IPSec VPN, SSL VPN:*** Алгоритми шифрування: 3DES, AES128, AES192, AES256
* Алгоритми хешування: MD5, SHA256, SHA384, SHA512
* Diffie-Hellman Group: 1, 2, 5, 14
* Підтримка Hub & Spoke топології, Spoke & Spoke (mesh) топології, DMVPN/ADVPN або аналог

**QoS:*** Traffic Shaping
* Traffic Policing

**Маршрутизація та SD-WAN:*** Статична маршрутизація та маршрутизація по політиках (PBR)
* Динамічні протоколи маршрутизації: RIP v1/v2, OSPF v2/v3, IS-IS, BGP4
* 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 або пасивними методами
* 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
* Динамічне виправлення втрати пакетів або відновлювання пакетів з помилками, що викликані несприятливими умовами WAN-каналів під час роботи через VPN (Forward Error Correction)
* Дуплікація пакетів через декілька каналів зв’язку з метою покращення роботи сервісів, що можуть бути викликані несприятливими умовами WAN-каналів під час роботи через VPN
* Балансування пакетів однієї сесії через декілька IPSec VPN тунелів

**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) у комплекті поставки
* 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

**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

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) | Граничний пристрій безпеки. Для забезпечення контролю інформаційних потоків (трафіку) в мережі у віддалених підрозділах ДНДЕКЦ МВС. |
|  | **Мережевий комутатор** | **Мережевий комутатор** доступу (L2, PoE) з необхідним набором ліцензій.**Загальні вимоги*** Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем 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
* Обладнання має підтримувати інтеграцію з Міжмережевими екранами наступного покоління, що є предметом данної закупівлі, технічні вимоги до яких приведені в п.1 та п.2
* Обладнання повинне мати можливість керування наявною у замовника централізованою системою керування мережевими пристроями FortiManager, що має бути підтверджене посиланнями на на відкриті веб-ресурси виробника

**Архітектура та форм-фактор**• Мережевий комутатор (L2) для встановлення в стандартну монтажну шафу 19”**Живлення:**• 1 блок живлення (100-240V AC, 50-60 Hz) або більше**Інтерфейси:*** Не менше ніж 24 \* GE RJ45
* Не менше ніж 4 \* 1GE SFP
* Не менше ніж 1 \* RJ45 консольний порт

**Живлення PoE:*** Кількість портів з PoE стандарту IEEE 802.3af/at – не менше 12
* PoE бюджет - не менше ніж 185 W

**Продуктивність:*** Комутаційна здатність: не менше ніж 128 Gbps
* Кількість пакетів в секунду: не менше ніж 190 Mpps
* Максимальна кількість МАС-адрес: не менше ніж 32 000
* Затримка (μs): не більше ніж 1
* Максимальна кількість VLAN: не менше ніж 4000
* Кількість портів в LAG групі: не менше ніж 8

**Підтримка протоколів та стандартів канального рівня моделі OSI:*** Jumbo Frames
* IEEE 802.1D MAC Bridging/STP (will interoperate)
* IEEE 802.1w Rapid Spanning Tree Protocol (RSTP, will interoperate)
* IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
* Edge Port / Port Fast
* IEEE 802.1Q VLAN Tagging
* IEEE 802.3ad Link Aggregation with LACP
* 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
* IGMP Snooping (v1/v2/v3)

**Безпека:*** Port Mirroring
* 802.1x authentication with port-based assignment
* 802.1x authentication with mac-based assignment
* sFlow
* ACL Tables

**Керування:*** 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

**QoS:**IEEE 802.1p Based Priority Queuing | Для організації мережі та системи відеоспостереження у віддалених підрозділах ДНДЕКЦ МВС. |
|  | **Мережевий комутатор** | **Мережевий комутатор** доступу (L2/L3, PoE).**Загальні вимоги:*** Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем 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
* Обладнання має підтримувати інтеграцію з Міжмережевими екранами наступного покоління, що є предметом данної закупівлі, технічні вимоги до яких приведені в п.1 та п.2
* Обладнання повинне мати можливість керування наявною у замовника централізованою системою керування мережевими пристроями FortiManager.

**Архітектура та форм-фактор:**• Мережевий комутатор (L2) для встановлення в стандартну монтажну шафу 19”**Живлення:*** 1 блок живлення (100-240V AC, 50-60 Hz)
* Можливість підключення резервного блоку живлення

**Інтерфейси:*** Не менше ніж 48 \* GE RJ45
* Не менше ніж 4 \* 10GE SFP+
* Не менше ніж 1 \* RJ45 консольний порт

**Живлення PoE:*** Кількість портів з PoE стандарту IEEE 802.3af/at – не менше 48
* PoE бюджет - не менше ніж 420 W

**Продуктивність:*** Комутаційна здатність: не менше ніж 170 Gbps
* Кількість пакетів в секунду: не менше ніж 260 Mpps
* Максимальна кількість МАС-адрес: не менше ніж 32 000
* Затримка (μs): не більше ніж 1
* Максимальна кількість VLAN: не менше ніж 4000
* Кількість портів в LAG групі: не менше ніж 8

**Підтримка протоколів та стандартів канального рівня моделі OSI:*** Jumbo Frames
* IEEE 802.1D MAC Bridging/STP (will interoperate)
* IEEE 802.1w Rapid Spanning Tree Protocol (RSTP, will interoperate)
* IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
* Edge Port / Port Fast
* IEEE 802.1Q VLAN Tagging
* IEEE 802.3ad Link Aggregation with LACP
* 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
* IGMP Snooping (v1/v2/v3)

**Layer 3 OSI функції:*** IPv4 маршрутних записів: не менше ніж 16 000
* Статична маршрутизація

**Безпека:*** Port Mirroring
* 802.1x authentication with port-based assignment
* 802.1x authentication with mac-based assignment
* sFlow
* ACL Tables

**Керування:*** 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

**QoS:**• IEEE 802.1p Based Priority Queuing | Формування резерву мережевого обладнання для ЦОД ДНДЕКЦ МВС та організації мережі та системи відеоспостереження у віддалених підрозділах ДНДЕКЦ МВС. |
|  | **Мережевий комутатор** | **Мережевий комутатор** доступу (L2/L3).**Загальні вимоги:*** Якщо відповідно до функціональності системи або згідно архітектурного підходу реалізація технічних вимог потребує додаткових систем 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
* Обладнання має підтримувати інтеграцію з Міжмережевими екранами наступного покоління, що є предметом данної закупівлі, технічні вимоги до яких приведені в п.1 та п.2
* Обладнання повинне мати можливість керування наявною у замовника централізованою системою керування мережевими пристроями FortiManager.

**Архітектура та форм-фактор:*** Мережевий комутатор (L2) для встановлення в стандартну монтажну шафу 19”

**Живлення:*** 1 блок живлення (100-240V AC, 50-60 Hz)
* Можливість підключення резервного блоку живлення

**Інтерфейси:*** Не менше ніж 48 \* GE RJ45
* Не менше ніж 4 \* 10GE SFP+
* Не менше ніж 1 \* RJ45 консольний порт

**Продуктивність:*** Комутаційна здатність: не менше ніж 170 Gbps
* Кількість пакетів в секунду: не менше ніж 260 Mpps
* Максимальна кількість МАС-адрес: не менше ніж 32 000
* Затримка (μs): не більше ніж 1
* Максимальна кількість VLAN: не менше ніж 4000
* Кількість портів в LAG групі: не менше ніж 8

**Підтримка протоколів та стандартів канального рівня моделі OSI:*** Jumbo Frames
* IEEE 802.1D MAC Bridging/STP (will interoperate)
* IEEE 802.1w Rapid Spanning Tree Protocol (RSTP, will interoperate)
* IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
* Edge Port / Port Fast
* IEEE 802.1Q VLAN Tagging
* IEEE 802.3ad Link Aggregation with LACP
* 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
* IGMP Snooping (v1/v2/v3)

**Layer 3 OSI функції:*** IPv4 маршрутних записів: не менше ніж 16 000
* Статична маршрутизація

**Безпека:*** Port Mirroring
* 802.1x authentication with port-based assignment
* 802.1x authentication with mac-based assignment
* sFlow
* ACL Tables

**Керування:*** 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

**QoS:**IEEE 802.1p Based Priority Queuing | Для організації мережі та системи відеоспостереження у віддалених підрозділах ДНДЕКЦ МВС. |
|  | **Кабель мережевий** | F/UTP Cat.6 4/23AWG solid, LSZH, WR 500m. | Для організації комп’ютерної мережі. |
| 3.1. | **Гарантійний термін на запропонований учасником товар має становити не менше 12 місяців.** |

**Обґрунтування**

**розміру бюджетного призначення та очікуваної вартості**

**предмета закупівлі**

**Код ДК 021:2015 32420000-3 Мережеве обладнання (Мережеве обладнання)**

**(номер / ідентифікатор закупівлі UA-2023-11-23-016400-a)**

864 012,00 грн.

(загальна очікувана вартість предмета закупівлі)

|  |  |  |  |
| --- | --- | --- | --- |
| №п/п | Розмір бюджетного призначення | Очікувана вартість предмета закупівлі | Обґрунтування розміру очікуваної вартості |
| 1 | 2 | 3 | 4 |
| 1. | 864 012,00 грн. | 864 012,00 грн. | Розрахунок очікуваної вартості проводився шляхом аналізу цінових пропозицій трьох комерційних пропозицій:- пропозиція 1 становить798 972,00 грн;- пропозиція 2 становить857 832,00 грн;- пропозиція 3 становить935 232,00 грн.Очікувана вартість становить 864 012,00 грн.  |