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, то вони усі мають бути у комплекті поставки рішення.

На обладнання не має бути анонсів end-of-sale та end-of-life (EOS/EOL) від виробника.

**Примітка: У разі посилання у викладеній інформації на конкретну торговельну марку чи фірму, патент, конструкцію або тип у найменуваннях за предметом закупівлі, джерело його походження або виробника, - слід вважати в наявності вираз “або еквівалент”**

|  |  |
| --- | --- |
| Технічні характеристики | |
| **Міжмережевий екран (Firewall)** | **Cisco Firepower FPR1150-NGFW-K9 (або еквівалент)** |
| Пропускна здатність: брандмауер (FW) + видимість і контроль програм (AVC) (1024B) | Не менше 5,3 Гбіт/с |
| Пропускна здатність: FW + AVC + система запобігання вторгненням (IPS) (1024B) | Не менше 4,9 Гбіт/с |
| Кількість одночасних сеансів з AVC | Не менше 600 000 |
| Кількість нових підключень за секунду з AVC | Не менше 28 000 |
| Безпека транспортного рівня (TLS) | Не менше 1,4 Гбіт/с |
| Пропускна здатність: NGIPS (1024B) | Не менше 6,1 Гбіт/с |
| Пропускна здатність IPSec VPN (1024B TCP з Fastpath) | Не менше 2,4 Гбіт/с |
| Кількість VPN-пірів | Не менше 800 |
| Диспетчер пристроїв Cisco (локальне керування) | ТАК |
| Централізоване управління | Централізована конфігурація, журналювання, моніторинг і звітування виконуються Threat Defense Manager (FMC) або, як альтернатива, з хмари за допомогою Cisco Defense Orchestrator. |
| AVC | Стандартний, підтримка понад 4000 програм, а також геолокації, користувачів і веб-сайти |
| Cisco Security Intelligence | Стандартний, з аналізом загроз IP, URL і DNS |
| Cisco IPS | Доступний; може пасивно виявляти кінцеві точки та інфраструктуру для кореляції загроз і інтелектуальних індикаторів компрометації (IoC) |
| Захист мереж від шкідливих програм | Доступний; дає змогу виявляти, блокувати, відстежувати, аналізувати та стримувати цільове та стійке зловмисне програмне забезпечення, звертаючись до континууму атак як під час, так і після атак.  Інтегрована кореляція загроз із Cisco AMP для кінцевих точок також доступна додатково |
| Ізольоване програмне середовище Cisco Malware Analytics | В наявності |
| URL фільтрація: кількість категорій | Не менше 80 |
| Фільтрування URL-адрес: кількість URL-адрес, класифікованих за категоріями | Не менше 280 млн |
| Автоматизоване оновлення каналу загроз і сигнатур IPS | Так: провідна система колективної безпеки (CSI) від групи Cisco |
| Форм-фактор | Монтаж в стійку, 1U |
| Мережеві інтерфейси | 8 x RJ-45, 2 x SFP,2 x SFP+ |
| Інтерфейси управління | 1x 1000BASE-T  1x послідовна консоль (RJ-45) |
| Інтерфейси USB | 1 x USB 3.0 Type-A (500 мА) |
| Накопичувач SSD | Не менше 1 х 200 ГБ |
| Встановлені процесори | Не менше 1х Intel |
| ОЗУ | 32 GB DDR4 SDRAM |
| Встановлення та налаштування міжмережевого екрану | ТАК (У вартість міжмережевого екрану має бути включено встановлення та налаштування відповідних модулів безпеки) |
| Гарантійні зобов’язання | |
| Гарантійний термін | Не менше 1 року |

Товар, що поставляється, повинен бути оригінальним та новим, що раніше не використовувався (всі складові частини товару повинні бути новими), із захисними пломбами, стрічками тощо.

Товар обов’язково повинен мати оригінальну упаковку виробника, яка не може бути пошкодженою або заміненою на іншу