**Додаток 4** до тендерної документації

**ТЕХНІЧНІ ВИМОГИ**

**ІНФОРМАЦІЯ ПРО ТЕХНІЧНІ, ЯКІСНІ ТА КІЛЬКІСНІ ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

**Апаратно-програмний комплекс захищеного доступу до мережі Інтернет Secure Web Gateway (SWG)) за кодом**

**ДК 021:2015 – 32420000-3 Мережеве обладнання**

**1. Призначення апаратно-програмного комплексу захищеного доступу до мережі Інтернет Secure Web Gateway (SWG)**

Відповідно до вимог кібербезпеки при організації роботи користувачів в мережі Інтернет на периметрі доступу необхідно забезпечувати мережевий захист із вирішенням наступних завдань:

* захист від атак “нульового дня” (вразливості програмного забезпечення, які ще невідомі користувачам чи розробникам програмного забезпечення та проти яких ще не розроблені механізми захисту), виявлення зловмисного коду та шкідливого програмного забезпечення;
* фільтрація трафіку та розмежування доступу між мережею об’єкта критичної інфраструктури та зовнішніми мережами за критеріями дозволених та заборонених служб, протоколів, портів, мережевих адрес, мережевих з’єднань, небажаних веб-сайтів тощо. Блокування трафіку та з’єднань, які не відповідають визначеним критеріям;
* фільтрація та аналіз трафіку за визначеними відповідно до політики інформаційної безпеки критеріями;
* моніторинг трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення та за іншими визначеними відповідно до політики інформаційної безпеки критеріями;
* виявлення та запобігання атакам та вторгненням, спрямованим на програмні та апаратні компоненти та інформацію об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури;
* захист від атак типу “відмова в обслуговуванні”;
* захист від несанкціонованого доступу через Інтернет;
* балансування навантаження;
* маскування структури і мережевих адрес мережі;
* завершення з’єднання з вузлом у разі атаки;
* здійснення реєстрації подій, що мають відношення до безпеки.

Для захисту об’єкта критичної інформаційної інфраструктури об’єкта критичної інфраструктури повинні використовуватися програмно-апаратні засоби, потужність яких визначається виходячи із об’єму трафіку, який передбачається в мережі, з урахуванням його потенційного збільшення.

**2. Мета і завдання впровадження апаратно-програмного комплексу захищеного доступу до мережі Інтернет Secure Web Gateway (SWG)**

Метою закупівлі апаратно-програмного комплексу захищеного доступу до мережі Інтернет Secure Web Gateway (SWG) є забезпечення безпечної роботи користувачів Держмитслужби в мережі Інтернет шляхом захисту від загроз вхідного та вихідного трафіку.

Впровадження апаратно-програмного комплексу захищеного доступу до мережі Інтернет Secure Web Gateway (SWG) забезпечить:

* протоколювання дій користувачів;
* фільтрацію, моніторингу та аналізу трафіку на наявність зловмисного коду, вірусів зловмисного програмного забезпечення в реальному часі;
* аналіз контенту сайтів;
* виявлення зловмисних програм «нульового дня».

**3. Вимоги чинного законодавства**

1. Конституція України;

2. Закон України «Про електронну ідентифікацію та електронні довірчі послуги»;

3. Закон України «Про інформацію»;

4. Закон України «Про електронні документи та електронний документообіг»;

5. Закон України «Про доступ до публічної інформації»;

6. Закон України «Про захист персональних даних»;

7. Закон України «Про захист інформації в інформаційно-комунікаційних системах»;

8. Митний кодекс України;

9. Постанова Кабінету Міністрів України від 12 березня 2022 року № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану»;

10. Постанова Кабінету Міністрів України від 08 вересня 2016 року
№ 606 «Деякі питання електронної взаємодії електронних інформаційних ресурсів»;

11. Постанова Кабінету Міністрів України від 02 лютого 2024 року
№ 119 «Деякі питання Національної програми інформатизації»;

12. Постанова Кабінету Міністрів України від 4 лютого 1998 року № 121 «Про затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації засобів інформатизації»

13. Розпорядження КМУ «Деякі питання реалізації концептуальних напрямів реформування системи органів, що реалізують державну митну політику» від 13 травня 2020 р. № 569-р;

14. Довгостроковий національний стратегічний план цифрового розвитку, цифрових трансформацій і цифровізації Державної митної служби України та її територіальних підрозділів на основі Багаторічного стратегічного плану електронної митниці ЄС (Multi-annual strategic plan for electronic customs, MASP-C), затвердженого наказом Міністерства фінансів України від 09.02.2024 № 63 «Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами».

## 4. Загальні вимоги до обладнання

* 1. Все обладнання має випускатися серійно.
	2. Все обладнання має бути новим, що не використовувалося раніше. На момент поставки обладнання, щодо нього не повинні діяти терміни End-of-Life, End-of-Sale та End-of-Support.
	3. Все обладнання має відповідати українським стандартам електроживлення та комплектуватися відповідними кабелями підключення електроживлення.
	4. Все обладнання повинно бути від одного виробника та постачатися зі строком гарантійного та технічного (сервісного) обслуговування терміном не менше 36 місяців.
	5. Все обладнання повинно поставлятися (включати) в комплекті зі всіма необхідними ліцензіями та підписками, які забезпечують роботу всього функціоналу не менше 36 місяців.
	6. Все обладнання повинно мати паспорт-формуляр.
	7. Все обладнання повинно мати дійсний на момент подачі пропозиції експертний висновок, зареєстрований в Адміністрації Державної служби спеціального зв'язку за захисту інформації України, про відповідність запропонованого мережевого обладнання безпеки вимогам нормативних документів системи технічного захисту інформації в Україні з рівнем гарантій Г-2 згідно з НД ТЗІ 2.5-004-99, або знаходитись на експертизі, що підтверджується листом від вендора.
	8. Гарантійна та технічна підтримка обладнання має відповідати таким вимогам:

4.8.1. Надання консультацій телефоном та електронною поштою з питань налаштування і експлуатації обладнання в робочі дні з 9.00 до 18.00 годин;

* + 1. Приймання запитів на обслуговування протягом 24 годин на добу, 7 днів на тиждень, включаючи вихідні та святкові дні, за телефоном, факсом, електронною поштою або через веб-сайт;
		2. Реагування на запити на обслуговування протягом 1 години з моменту отримання запиту на обслуговування за телефоном, факсом, електронною поштою в робочі години;
		3. Виконання обслуговування через веб-сайт цілодобово у робочі, вихідні та святкові дні;
		4. Діагностика несправності апаратної частини обладнання дистанційно (по телефону, електронної поштою, WebEx чи інший вид конференції, або віддалене підключення, надане Замовником);
		5. Заміна несправного обладнання, або його складових частин протягом наступного дня з моменту встановлення несправності та необхідності заміни обладнання (у випадку виникнення критичної несправності, яка може у будь-який момент спричинити зупинку усього технологічного процесу Замовника);
		6. Доступ до закритої частини сайту виробника ([за](http://www.cisco.com) наявності) і онлайн бази знань виробника з великою кількістю технічної інформації та корисними інструментами;
		7. Постійний (протягом 24 годин на добу, 7 днів на тиждень) доступ до Центру Технічної Підтримки виробника, електронною поштою або по телефону;
		8. Надання Замовнику основних та перехідних версій програмного забезпечення виробника за допомогою веб-сайту виробника.

4.9. Термін надання послуг з гарантійної та технічної підтримки обладнання повинен складати не менше ніж 36 місяців.

**СПЕЦИФІКАЦІЯ ТоваРУ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Найменування** | **Короткий опис** | **Кількість** | **Примітки** |
| 1. | Апаратно-програмний комплекс захищеного доступу до мережі Інтернет Secure Web Gateway (SWG)  | Апаратно-програмний комплекс захищеного доступу до мережі Інтернет Secure Web Gateway (SWG) для забезпечення безпечної роботи користувачів Держмитслужби в мережі Інтернет шляхом забезпечення захисту від загроз вхідного та вихідного трафіку та проксування трафіку для проставлення мітки часу. | 2комплекти | Детальний опис наведено у таблиці 1 |

*\* Будь-яке посилання на торгову марку або виробника слід читати зі словами «або еквівалент».*

*\*\* - Еквівалентом вважається ліцензія на програмне забезпечення/технічну підтримку , яка за функціоналом та характеристиками відповідає загальним вимогам до післягарантійної технічної підтримки, технічним вимогам та повністю сумісне з обладнанням, яке встановлено у Замовника.*

## таблиця 1

## Технічні вимоги до комплекту обладнання Апаратно-програмного комплексу захищеного доступу до мережі Інтернет Secure Web Gateway (SWG) (2 комплекти)

|  |
| --- |
| Повна назва запропонованого учасником обладнання\*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Код обладнання\*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **№ з/п** | **Найменування та опис технічних вимог товарів, що вимагаються замовником**(У цьому стовпчику зазначено найменування та технічні характеристики товарів, що вимагаються Замовником) | **Найменування та опис технічних вимог товарів, що пропонуються учасником**(У цьому стовпчику необхідно зазначити найменування та технічні характеристики товарів, що пропонуються Учасником) | **Відповідність,****так/ні**(У разі, якщо технічні характеристики товару, що пропонуються Учасником відповідають або перевищують необхідні характеристики, пишеться -"так", якщо не відповідає – "ні") |
| **1** | **Технічні та архітектурні вимоги до системи** |
| 1.1 | Рішення має впроваджуватися в інфраструктуру Покупця у вигляді апаратно-програмно комплексу (далі – АПК) |   |  |
| 1.2 | АПК повинен складатися з двох апаратних шлюзів захищеного доступу до мережі інтернет (основний та резервний) та централізованої системи управління (апаратне рішення або віртуальна машина) |  |  |
| 1.3 | Централізована система управління повинна забезпечувати керування апаратними шлюзами захищеного доступу до мережі Інтернет (зазначених в п. 1.2) та спеціалізованими поштовими шлюзами, які призначені для захисту електронної пошти від усіх типів загроз, які впроваджені у замовника (Cisco ESA c690 – 2шт.) |  |  |
| 1.4 | Система управління має підтримувати рольову модель доступу (RBAC) з гнучким розмежуванням прав |   |  |
| 1.5 | Підтримка роботи як у режимі Upstream, так і у режимі Downstream Proxy |   |  |
| 1.6 | Підтримка отримання копії трафіку в режимі Web Traffic Tap (WTT)  |   |  |
| 1.7 | Система управління повинна мати функціонал розмежування інтерфейсів для обробки клієнтського трафіку та трафіку управління з підтримкою двох незалежних таблиць маршрутизації |   |  |
| 1.8 | Можливість використовувати як Internet root DNS-сервери, так і DNS-сервери замовника |   |  |
| 1.9 | Можливість вказати вторинні DNS-сервери для обробки запитів, якщо основний DNS-сервер не відповідає |   |  |
| 1.10 | Можливість забезпечення відмовостійкого рішення (HA), а саме включення не менш ніж 2-х пристроїв в єдиний програмно-апаратний комплекс за допомогою VRRP/CARP в режимі Explicit та забезпечення HA в режимі Transparent |   |  |
| 1.11 | Можливість обслуговування не менше 2500 абонентів та мати можливість розширення не менше ніж до 5000 абонентів |   |  |
| 1.12 | Можливість роботи проксі-серверу в режимі Transparent Mode  |   |  |
| 1.13 | SOCKS Proxy для моніторингу трафіку на 4 рівні для забезпечення контролю і виявлення проблем |   |  |
| 1.14 | FTP Proxy для здійснення фільтрації трафіку FTP з'єднань, забезпечуючи безпеку та контроль доступу до файлових ресурсів |   |  |
| **2** | **Вимоги до функцій управління** |
| 2.1 | Система управління повинна бути реалізована у вигляді веб-консолі, підтримувати всі актуальні версії веб-браузерів |   |  |
| 2.2 | Можливість АПК зберігати та надавати файл PAC для автоматичного налаштування клієнтських пристроїв |   |  |
| 2.3 | Можливість зберігання журналів подій (logs) на сторонньому FTP сервері |   |  |
| 2.4 | Можливість налаштування часу бездіяльності сеансу на консолі системи управління |   |  |
| 2.5 | Підтримка мультифакторної аутентифікації для доступу до системи керування |   |  |
| 2.6 | Підтримка наступних засобів аутенифікації: локальний, RADIUS, LDAP для доступу до системи керування |   |  |
| 2.7 | Підтримка обмеження доступу до системи керування за допомогою IP-адреси, діапазону IP або CIDR |   |  |
| 2.8 | Можливість автоматичного оновлення ключів компонентів рішення  |   |  |
| 2.9 | Наявність інструменту емуляції запиту клієнта для відстеження відпрацювання політики |   |  |
| 2.10 | Можливість зберігати файл конфігурації системи для повторного використання або налаштування централізованого управління декількома АПК з єдиної консолі |   |  |
| 2.11 | Функція автоматичного резервного копіювання файлу конфігурації пристрою при кожному застосуванні змін та передача попередньої версії файлу конфігурації на віддалений резервний сервер за допомогою FTP або SCP |   |  |
| 2.12 | Можливість створювати власні сповіщення для кінцевих користувачів |   |  |
| 2.13 | Можливість обмеження налаштованої кількості одночасних підключень, ініційованих клієнтом. Коли кількість з’єднань перевищує налаштований ліміт, з’єднання розриваються, а адміністратору надсилається сповіщення |   |  |
| **3** | **Вимоги до захисту веб-комунікацій** |
| 3.1 | Можливість створення політик доступу для контролю відвідування користувачем різних веб-ресурсів та додатків  |   |  |
| 3.2 | Підтримка політик доступу як за моделлю Role Based Access Policy (користувачу призначається роль, яка визначає його права доступу) так і Rule Based Access Policy (динамічний доступ до ресурсів в залежності від комбінації AD group, до яких належить користувач) |   |  |
| 3.3 | Можливість контролювати відвідування користувачем різних веб-ресурсів та додатків  |   |  |
| 3.4 | Наявність функціоналу статичної URL-фільтрації та на основі попередньо налаштованих або користувацьких URL-категорій |   |  |
| 3.5 | Розшифровка HTTPS (TLS) трафіку користувачів для визначених категорій URL-адрес з метою забезпечення більшої видимості і контролю. Обов’язкова підтримка TLS 1.3 |   |  |
| 3.6 | Наявність вбудованої системи веб-репутації та налаштування дій щодо визначеного рівня репутації веб-ресурсів |   |  |
| 3.7 | Можливість обирати дію для URL-категорії:- Block- Redirect- Allow- Monitor- Warn- Quota-Based |   |  |
| 3.8 | Створення користувацьких категорій URL для гнучкого управління |   |  |
| 3.9 | Можливість перенаправлення визначених веб-ресурсів на встановлену веб-сторінку |   |  |
| 3.10 | Можливість налаштувати дію за замовчуванням для опрацювання запиту, якщо не прийнято рішення на основі категорії URL-адреси чи рейтингу Web Reputation |   |  |
| 3.11 | Можливість створення та застосування квот або часових проміжків для обмеження обраного типу трафіку |   |  |
| 3.12 | Наявність не менше ніж 85 передналаштованих категорій URL |   |  |
| 3.13 | Запобігання поширенню шкідливого й шпигунського програмного забезпечення в мережу, шляхом блокування вихідних файлів з потенційно шкідливим вмістом |   |  |
| 3.14 | Наявність функціоналу контролю додатків (App Control) з контролем доступу до популярних додатків  |   |  |
| 3.15 | Можливість налаштувати політики на основі визначених характеристик пристроїв та ідентифікації користувачів |   |  |
| 3.16 | Можливість встановити винятки для певних веб-сайтів або категорій, у разі якщо веб-сайт посилається на заборонений вміст та класифікується як ресурс, на який він посилається |   |   |
| 3.17 | Можливість застосування дій для обраних категорій YouTube |   |   |
| 3.18 | Система управління повинна підтримувати моніторинг та захист в реальному часі  |   |  |
| 3.19 | Можливість блокування з'єднання з відомими шкідливими веб-сайтами або відповідно до оцінки їх веб-репутації |   |  |
| 3.20 | Можливість контролю протоколів та блокування визначених клієнтських агентів (браузерів) |   |   |
| **4** | **Розширені вимоги для захисту даних** |
| 4.1 | Можливість перевірки файлів, що передаються по HTTP(S) протоколу |   |  |
| 4.2 | Виявлення та блокування підозрілих файлів |   |  |
| 4.3 | Виявлення та блокування як відомих, так і невідомих видів зловмисного програмного забезпечення |   |  |
| 4.4 | Відправлення невідомих файлів до пісочниці для перевірки їх рівня шкідливості, автоматичне повідомлення адміністратору у випадку знаходження. Ліцензія на доступ до пісочниці повинна входити в склад рішення |   |  |
| 4.5 | Можливість експортувати звіти про зловмисне програмне забезпечення в форматі PDF |   |  |
| 4.6 | Можливість редагувати список користувацьких категорій, щоб вибрати категорії URL-адрес для сканування файлів |   |   |
| 4.7 | Можливість застосовувати дії відповідно до критерію репутації |   |   |
| 4.8 | Можливість налаштування для яких категорій URL-адрес заборонено вивантаження будь-яких об’єктів з ПК користувачів |   |   |
| 4.9 | Можливість встановлення порогу рівня веб-репутації для сайту, при якому будь-яке завантаження об'єктів на нього буде заборонено |   |   |
| 4.10 | Налаштування блокування передачі даних на основі таких характеристик файлів, як розмір, тип та ім'я |   |   |
| **5** | **Ідентифікація користувачів** |
| 5.1 | Можливість ідентифікувати користувачів за наступними параметрами:- ІР-адреса- облікові дані AD- Cisco ISE- LDAP-каталог |   |   |
| 5.2 | Підтримка наступних методів аутентифікації AD: Basic, NTLMSSP, Kerberos |   |   |
| 5.3 | Можливість створювати статичні та динамічні групи користувачів |   |   |
| 5.4 | Можливість заборонити або надати гостьовий доступ до веб-ресурсу для користувачів, які не пройшли аутентифцікацію |   |   |
| 5.5 | Можливість налаштувати як буде відслідковуватись автентифікований користувач:- ІР-адреса- Постійний файл cookie- Файли cookie сеансу- No Surrogat (запит на аутентифікацію при кожному новому TCP-з’єднанні) |   |   |
| **6** | **Інтеграції** |
| 6.1 | Підтримка інтеграції з існуючим LDAP-сервером IBM Domino версії 9.0 і вище |   |   |
| 6.2 | Підтримка нативної інтеграції з рішенням Cisco ISE, що впроваджений у замовника (OS version 3.1.0.135) |   |   |
| 6.3 | Підтримка інтеграції рішення з системою реагування на вразливості |   |   |
| 6.4 | Підтримка інтеграції з зовнішнім FTP сервером |   |   |
| 6.5 | Підтримка API для інтеграції з зовнішніми системами, включаючи SIEM |   |   |
| 6.6 | Можливість інтеграції з зовнішніми DLP-системами для більш глибокої перевірки |   |   |
| 6.7 | Можливість інтеграції з SMTP сервером для надсилання сповіщень та звітів поштою |   |   |
| **7** | **Інформаційні панелі, події та звітність** |
| 7.1 | Вбудована централізована звітність, можливість створення звітів щодо роботи системи, наявність вбудованих шаблонів звітів про: - мережеві додатки, - найбільш активних користувачів, - найбільш часто відвідувані веб-ресурси |   |   |
| 7.2 | Система має мати можливість створення запланованих звітів або генерації звітів за запитом |   |   |
| 7.3 | Сповіщення електронною поштою про події з різними рівнями важливості (Critical, Warning, Info), пов'язаних із конкретним компонентом або функцією системи |   |   |
| 7.4 | Сповіщення електронною поштою, коли термін дії ліцензії закінчується |   |   |
| 7.5 | Логування подій системи для моніторингу та виявлення несправностей пристрою |   |   |
| **8** | **Роботи з розгортання та налаштування** |  |  |
| 8.1 | Передпроектне обстеження інфраструктури, архітектурні сесії щодо впровадження Системи та обговорення сценаріїв побудови |   |   |
| 8.2 | Розгортання Системи та початкове налаштування, оновлення ПЗ до актуальної версії |   |   |
| 8.3 | Побудова відмовостійкості (HA) Системи |   |   |
| 8.4 | Інтеграція Системи з інфраструктурними сервісами (SMTP, LDAP, ISE) |  |  |
| 8.5 | Функціональне тестування та налагодження |  |  |
| 8.6 | Технічна консультація персоналу Замовника щодо роботи з Системою |  |  |
| 8.7 | Розробка інструкції з розгортання Системи |  |  |
| 8.8 | Розробка інструкції адміністратора |  |  |
| 8.9 | Підготовка Технічного паспорту |  |  |
| **9** | **Вимоги щодо навчання спеціалістів замовника** |
| 9.1 | Постачальник має забезпечити проходження спеціалізованих навчальних курсів по роботі з обладнанням, що постачається для 6 спеціалістів замовника |  |  |
| 9.2 | Курси мають проходити в режимі «offline» (аудиторія чи навчальний клас) в спеціалізованому навчальному центрі  |  |  |
| 9.3 | Курси мають включати як теоретичну так і практичну частину (лабораторні роботи) |  |  |

## Вимоги до SLA постачальника

|  |
| --- |
| **Вимоги до SLA постачальника** |
| **Рівень критичності** | **Опис** | **Час реакції** | **Час відновлення** | **Постачальник не /частково /забезпечує дану вимогу** | **Коментар постачальника** |
| Критичний | ***Система не працює:***ПАК не функціонує та не захищає від веб-комунікації кінцевих користувачів | до 2 годин  | до 8 годин |   |   |
| Високий | ***Система в небезпеці:***- Не працює централізована система управління ПАК Немає з'єднання між шлюзами захищеного доступу до мережі інтернет та централізованою сиситемою управління- Порушення роботи відмовостійкості системи | до 4 годин | до 12 годин |   |   |
| Середній | ***Погіршення продуктивності:***- Не оновлюється централізована система управління - Не відображається аналітика на інформаційних панелях- Не надходять звіти електронною поштою | до 6 годин | до 18 годин |   |   |
| Інформаційний запит | ***Загальна допомога:***Питання щодо конфігурацій Proxy та консультацій стосовно роботи системи | до 24 годин | - |   |   |

**На підтвердження відповідності тендерної пропозиції технічним, якісним, кількісним вимогам до предмета закупівлі, учасником у складі тендерної пропозиції надається:**

1. Довідка (форма довільна) щодо можливості поставки товару відповідно до вимог.

2. Учасник надає Замовнику лист від виробника програмного забезпечення (офіційного представника виробника на території України) про те, що Учасник є авторизованим партнером такого виробника, що підтверджує наявність партнерських відносин Учасника з виробником (за наявності), із зазначенням найменування Замовника, номера оголошення в електронній системі закупівель ProZorro.

3. Копія експертного висновку Державної служби спеціального зв'язку та захисту інформації України щодо відповідності вимогам нормативних документів з технічного захисту інформації.

4. У разі, як що Учасник пропонує еквівалент, то додається порівняльна таблиця у довільній формі на відповідність функціоналу та характеристикам предмету закупівлі.

5. Довідка (форма довільна) щодо застосування заходів із захисту довкілля.