|  |
| --- |
| Назва закупівлі: **Послуги із огляду можливостей та підготовки до самостійного налаштування замовником систем FortiGate за правилами FortiGate Security, FortiGate Infrastructure**Класифікатор та його відповідний код: **ДК 021:2015: 72240000-9: Послуги з аналізу та програмування систем**Процедура закупівлі: **Відкриті торги з особливостями**Очікувана вартість: **161 000,00 UAH з ПДВ**Дата оприлюднення: **25 травня 2023 року**Детальна інформація за посиланням: <https://prozorro.gov.ua/tender/UA-2023-05-25-008000-a> |

**ІНФОРМАЦІЯ ПРО ТЕХНІЧНІ ТА ЯКІСНІ**

**ХАРАКТЕРИСТИКИ ПРЕДМЕТА ЗАКУПІВЛІ**

**Послуги із огляду можливостей та підготовки до самостійного налаштування замовником систем FortiGate за правилами FortiGate Security, FortiGate Infrastructure**

**за кодом CPV за** **ДК 021:2015 - 72240000-9 Послуги з аналізу та програмування систем**

| **№****п/п** | **Найменування**  | **Кіль-****кість осіб** | **Технічні та якісні вимоги** |
| --- | --- | --- | --- |
| **Навчання з питань інформатизації за напрямом: FortiGate Security** |
| 1. | Навчання за напрямом:**FortiGate Security\***Кількість годин - 24 | 2 | 1. **За результатами даного курсу слухачі повинні вміти:**
* Огляд основних можливостей FortiGate
* Режими роботи
* Обліковий запис адміністратора, розмежування прав і доступу
* Відновлення пароля адміністратора
* Створення резервних копій та відновлення
* Оновлення програмного забезпечення
* Налаштування вбудованих серверів DNS і DHCP
* Ідеологія побудови Fortinet Security Fabric
* Розгортання Fortinet Security Fabric
* Розвиток Security Fabric додатковими компонентами і функціями
* Співвіднесення трафіку з правилами за адресами, портами, користувачами, інтерфейсами та зонами
* Налаштування політик брандмауера
* Використання номерів правил і ID правил
* Ідентифікація використаних об'єктів
* Зміна порядку правил для коректної роботи
* Ідеологія трансляції адрес і портів
* Режими роботи трансляції адрес
* Налаштування політики брандмауера для трансляції адрес джерела і одержувача (VIP)
* Налаштування централізованої трансляції (central NAT)
* Підтримка сесій на 7 рівні (session helpers), використання SIP session helper для VoIP
* Інтерпретація записів в таблиці сесій
* Аналіз виведення команди діагностики сесій, стану TCP, UDP і ICMP сесій
* Використання логів для вирішення спільних проблем з NAT, моніторинг сесій з NAT
* Основи аутентифікації, методи аутентифікації, протоколи
* Використання зовнішніх серверів аутентифікації
* Опис методів активної та пасивної аутентифікації
* Налаштування локальної, віддаленої і двофакторної аутентифікації
* Налаштування зовнішніх серверів аутентифікації
* Основи логування, типи і підтипи лог-записів, їх структура та рівні
* Вплив логування на продуктивність
* Опції локального логування, настройка
* Можливості логування на зовнішні пристрої, настройка
* Налаштування логування, робота демона miglogd
* Використання FortiView
* Поняття довірених і недовірених сертифікатів
* Встановлення SSL з'єднання між FortiGate і SSL сервером
* Налаштування інспектування SSL трафіку, два варіанти настройки
* Запит сертифіката, імпорт CRL, резервне копіювання і відновлення сертифікатів
* Опис режимів перевірки трафіку в FortiOS
* Використання повної інспекції SSL
* Профілі фільтрації web-трафіку
* Робота з категоріями
* Перевизначення категорій, настройка користувача категорій
* Запит рейтингу в FortiGuard, настройка квот
* Перевизначення web-профайлів, налаштування фільтрації пошукових запитів
* Фільтрація web-контенту
* фільтрація DNS
* Налаштування профайлів інспекції SSL / SSH трафіку, настройка винятків
* Основи управління додатками, визначення типів додатків
* Сервіси управління додатками в FortiGuard
* сигнатури додатків
* Налаштування управління додатками в режимі профайлів
* Налаштування управління додатками в режимі політик
* Використання управління додатками для шейпінгу трафіку
* Використання FortiView для детального перегляду логів
* Використання сигнатур антивірусу
* Режими роботи антивіруса
* Використання FortiSandbox
* Різні набори сигнатур FortiGuard
* Рекомендації по настройці антивіруса
* Управління оновленнями IPS через FortiGuard
* Налаштування сенсорів IPS
* Застосування IPS до трафіку через брандмауер
* Виявлення DOS-атак, настройка DOS-політики
* Виявлення атак на Web-трафік, настройка WAF-профайлів
* Вибір методології застосування IPS
* Налагодження роботи системи IPS
* Поняття VPN, відміну SSL і IPSec VPN
* Режими роботи SSL VPN
* Аутентифікація користувачів в SSLVPN
* Налаштування SSL VPN, портали, необхідні політики, realms, персональні закладки
* Налагодження роботи SSL VPN
* Архітектура і переваги IPsec VPN, використовувані протоколи
* Фази обміну ключами (IKEv1)
* Використання топології DialUp
* Побудова DialUP тунелю між двома пристроями FortiGate
* Побудова DialUP тунелю між FortiGate і FortiClient
1. **Вимоги до Виконавця:**

Навчання має проводитись Виконавцем, який має власний або орендований навчальний центр/клас, сертифікованих фахівців для проведення курсів «FortiGate Security», що підтверджується відповідними документами у складі пропозиції. |
| **Навчання з питань інформатизації за напрямом: FortiGate Infrastructure** |
| 2. | Навчання за напрямом:**FortiGate Infrastructure**Кількість годин - 16 | 2 | * Аналізувати таблицю маршрутизації FortiGate.
* Маршрутизувати трафік, використовуючи політики та статичні маршрути, включаючи балансування трафіку.
* Налаштовувати SD-WAN для ефективного балансування трафіку між кількома WAN з'єднаннями.
* Займатися інспекцією трафіку на 2 рівні.
* Розділяти FortiGate на два або більше віртуальних пристроїв, що працюють як незалежні FortiGate, за рахунок налаштування віртуальних доменів.
* Встановлювати IPsec VPN тунелі між пристроями FortiGate.
* Порівнювати policy-based та route-based IPsec VPN.
* Впроваджувати топології VPN з резервуванням.
* Діагностувати проблеми з процедурами протоколу IKE.
* Надавати доступ до ресурсів мережі з використанням FSSO, а також сервісів Microsoft Active Directory (AD).
* Розгортати пристрої FortiGate в кластері для підвищення надійності та продуктивності.
* Розгортати проксі з використанням політик міжмережевого екрану, аутентифікації та кешування.
* Діагностувати та виправляти найпоширеніші проблеми.
 |

**Для підтвердження відповідності технічним та якісним вимогам до предмету закупівлі Учасник у складі пропозиції повинен надати гарантійний лист з підтвердженням відповідності послуг, які будуть надаватися, кожному пункту вимог.**

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