

Załącznik nr 1 do zapytanie ofertowego nr CBS 3/2024

Opisy do wymagań ogólnych

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
3. Przedmiot zamówienia musi pochodzić z oficjalnego kanału dystrybucji.

Zadanie 1. Zakup sprzętu

Access Point (20 sztuk)

Urządzenie musi być w pełni kompatybilne z kontrolerem sieci przewodowej posiadanym przez Zamawiającego - co ma wynikać z dokumentacji producenta. Zamawiający posiada klaster UTM Fortinet FortiGate 100F).

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
 - a. Temperatura -20 – 45°C,
 - b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażona w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
 - a. 2.4 GHz 802.11b/g/n,

- b. 5 GHz 802.11a/n/ac.
- 4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
- 5. Urządzenie musi być wyposażone w moduł BLE.
- 6. Urządzenie musi być wyposażone w jeden interfejs 10/100/1000 Base-TX. Należy dołączyć niezbędne okablowanie typu patchcord wymagane do podłączenia punktu dostępowego dopasowane i kompatybilne z istniejącą infrastrukturą Zamawiającego (zarówno od strony AP jak i przełącznika).
- 7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
- 8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
 - a. Tunnel,
 - b. Bridge,
 - c. Mesh.
- 9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.
- 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
- 11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
 - a. MIMO – 2x2,
 - b. Maksymalna przepustowość dla poszczególnych modułów radiowych:
 - i. 400 Mbps;
 - ii. 867 Mbps;
 - c. Wymagana moc nadawania:
 - i. min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - ii. min. 24 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
 - d. Wsparcie dla 802.11n 20/40Mhz HT,
 - e. Wsparcie dla kanałów 80MHz,
 - f. Anteny – 4 zewnętrzne dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
 - g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
 - h. Maksymalna deklarowana liczba klientów per moduł radiowy:
 - i. 512;
 - ii. 512;
- 12. Funkcje dodatkowe:
 - a. 802.11ac MU-MIMO Wave 2
 - b. Transmit Beam Forming (TxBF)
 - c. Low-Density Parity Check (LDPC) Encoding
 - d. Maximum Likelihood Demodulation (MLD)
 - e. Maximum Ratio Combining (MRC)
 - f. A-MPDU and A-MSDU Packet Aggregation

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta do dnia 30.06.2026r., polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Przełącznik sieciowy (1 sztuka)

W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Zamawiający jest w posiadaniu rozwiązania UTM, model FortiGate 100F (klaster 2 sztuk). W ramach rozbudowy istniejącego systemu, której celem jest rozszerzenie mechanizmów bezpieczeństwa o warstwę dostępową, wymagany jest dostarczenie przełącznika w pełni kompatybilnego wg dokumentacji producenta z istniejącym rozwiązaniem Fortigate, w szczególności mieć możliwość obsługi protokołu FortiLink.

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Budżet mocy dla portów PoE min.: 370 W.
- Maksymalny pobór mocy bez budżetu dla PoE: 85 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
 - a) 24 porty GE RJ-45.
 - W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.
 - b) 4 porty 10 GE SFP+. Należy dołączyć do przełącznika 4 kompatybilne wkładki SFP+ MultiMode wraz odpowiednimi i kompatybilnymi do istniejącej instalacji okablowania strukturalnego Zamawiającego patchcordami optycznymi).

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.

- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element

leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

- Centralne zarządzanie konfiguracją urządzenia
 - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
 - Centralne zarządzanie sieciami VLAN.
 - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
 - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
 - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
 - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
 - Automatyczna detekcja i rekomendacje konfiguracji.
 - Przesyłanie logów na zewnętrzny serwer syslog.
 - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
 - Obsługa białych i czarnych list adresów MAC.
 - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
 3. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta do dnia 30.06.2026, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Zadanie 2. Zakup kontynuacji subskrypcji klastra HA Fortigate 100F

Przedmiotem dostawy jest przedłużenie subskrypcji na poziomie Hardware plus FortiCare Premium and FortiGuard Unified Threat Protection (UTP) od dnia 2024-12-13 do dnia 2026-06-30 posiadanego przez Zamawiającego klastra HA dwóch urządzeń Fortinet Fortigate 100F

Nr seryjne sprzętu: FG100FTK22048264; FG100FTK22048219

Zadanie 3. Usługi wdrożenia, konfiguracji i instalacji AccesPointów oraz konfiguracja z istniejącym urządzeniem typu UTM/firewall

1. Przegląd i analiza obecnej konfiguracji posiadanego firewall Fortigate.
2. Uruchomienie dedykowanego interfejsu zarządzającego z przełącznikami opisanymi w zadaniu nr 1.
3. Dodanie odpowiednich sieci VLAN zgodnie z wytycznymi Zamawiającego.
4. Konfiguracja nowych polityk bezpieczeństwa dla sieci WLAN.
5. Konfiguracja uwierzytelniania dla produkcyjnej sieci WLAN opartego o istniejącą Domenę Windows.
6. Konfiguracja, wdrożenie analogicznej do posiadanej dekrypcji SSL dla sieci produkcyjnej WLAN.
7. Konfiguracja polityk bezpieczeństwa (URL Filtering, antywirus, kontrola aplikacji, IPS) zgodnie z dobrymi praktykami dla sieci WLAN gościnnej oraz produkcyjnej.
8. Stworzenie optymalnych profili IDS/IPS pod kątem ruchu przychodzącego i wychodzącego zgodnie z charakterystyką systemów docelowych dla nowych sieci.
9. Utworzenie reguł komunikacyjnych dla istniejących sieci VLAN z siecią WLAN zgodnie z wytycznymi Zamawiającego
10. Szkolenie z obsługi systemu i konfiguracji dla administratora

W zakresie konfiguracji instalacji przełącznika sieciowego oraz AccesPointów :

- fizyczny montaż przełącznika w szafach rack i instalacja okablowania zgodnie z wytycznymi Zamawiającego,
- podłączenie okablowania do urządzeń klienckich i połączenie przełączników z Firewall oraz między sobą za pomocą łączy optycznych MM 10Gbit. Wykonawca zapewnia konieczne akcesoria do połączenia (odpowiednie patchcordsy miedziane i optyczne oraz wkładki optyczne kompatybilne z istniejącą infrastrukturą strukturalną Zamawiającego).
- Reorganizacja istniejących połączeń sieci zgodnie z dobrymi praktykami zapewniającymi wysoką dostępność, wydajność, bezpieczeństwo oraz skalowalność,
- Integracja zarządzania przełącznikami i punktami dostępowymi w interfejsie Firewall.
- Konfiguracja i optymalizacja protokołów transportu pod kątem wykorzystywanego pomiędzy systemami w sieci wykorzystującymi usługi disaster-recovery,

Dodatkowe wymagania:

- Wykonawca winien posiadać status partnera producenta oferowanego przez siebie rozwiązania,
- usługi instalacji i konfiguracji rozwiązania musi dokonywać specjalista posiadający certyfikat danego producenta poświadczający kompetencje w zakresie instalacji i konfiguracji. Certyfikaty należy złożyć wraz z ofertą, niezłożenie certyfikatów jest przesłanką do odrzucenia oferty.

- fizyczny montaż punktów dostępowych i instalacja okablowania zgodnie z wytycznymi Zamawiającego, podłączenie zasilaczy PoE pomiędzy przełącznikami a AP
- podłączenie okablowania do urządzeń klienckich i połączenie przełączników z Firewall oraz między sobą za pomocą łączy optycznych MM 10Gbit. Wykonawca zapewnia konieczne akcesoria do połączenia (odpowiednie patchcordsy miedziane i optyczne oraz wkładki optyczne kompatybilne z istniejącą infrastrukturą strukturalną Zamawiającego).
- połączenie z kontrolerem sieci Wifi i konfiguracja kontrolera zgodnie z dobrymi praktykami zapewniającymi wysoką dostępność, wydajność, bezpieczeństwo oraz skalowalność, integracja z Firewall i analizerem logów.
- wykonanie powdrożeniowego badania sieci wifi zawierającego reprezentację graficzną dla badanego obszaru zawierającego następujące informacje:
 - siła sygnału podstawowego dla określonego pasma sieci wifi (Primary signal strength)
 - siła sygnału zapasowego dla określonego pasma sieci wifi (Secondary signal strength)
 - stosunek sygnału do szumu (SNR)
 - zmierzony szum otoczenia (Noise)
 - Zakłócenia kanałowe - Channel Interference
 - wykryte inne interferencje (Interferers)
 - ścieżki pomiarowe
- Zamawiający wymaga przygotowania wstępnego schematu wdrożenia oraz harmonogramu planowanych prac w zakresie instalacji i wdrożenia, a także przedstawienie obu dokumentów do akceptacji zamawiającego na minimum 5 dni roboczych przed rozpoczęciem prac. Zamawiający ma prawo do wprowadzania zmian i wytycznych do wskazanych powyżej dokumentów, niezaakceptowanie ich przez Wykonawcę w ciągu 3 dni stanowi przesłankę do rozwiązania umowy. Zamawiający dostarczy podkłady mapowe.