W ramach postępowania wymaganym jest dostarczenie elementów niezbędnych do zbudowania systemu bezpieczeństwa infrastruktury dostępowej i sieciowej. Zamawiający wymaga dostarczenia systemu bezpieczeństwa w postaci 1 systemu UTM, 4 zarządzalnych przełączników sieciowych, 4 urządzeń dostępowych WiFi, o określonych poniżej parametrach.

1. **Wymagania dotyczące systemu UTM.**

Dostarczony system UTM musi stanowić system bezpieczeństwa zapewniający wszystkie wymienione poniżej funkcje sieciowe i  bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa urządzenia UTM były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System UTM realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu UTM musi być zapewniona możliwość budowy minimum   
2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

Urządzenie musi wspierać IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

Zamawiający jest w posiadaniu urządzenia FortiGate-101E z aktywną licencją do 01.11.2025r. Wymagane jest aby nowo dostarczone urządzenie posiadło licencję na okres 1 roku oraz była możliwość przeniesienia licencji ze starego urządzenia na nowe. Licencja po przeniesieniu ma przedłużyć ważność licencji nowego urządzenia.

Wymagania minimalne:

|  |  |  |
| --- | --- | --- |
| **Grupa parametrów systemu** | **Szczegółowe cechy** | **Spełnia / nie spełnia** |
| 1. Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |  |
| 1. Interfejsy, Dysk, Zasilanie | 1. System UTM realizujący funkcję Firewall musi dysponować minimum:    1. 16 portami Gigabit Ethernet RJ-45.    2. 8 gniazdami SFP 1 Gbps.    3. 2 gniazdami SFP+ 10 Gbps. 2. System UTM musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. W ramach systemu UTM powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 4. System UTM musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB. 5. System UTM musi być wyposażony w dwa zasilania AC. |  |
| 1. Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 56 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. 3. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B. 4. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 1518 B. 5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.2 Gbps. 6. Wydajność szyfrowania IPSec VPN nie mniej niż 11 Gbps. 7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.6 Gbps. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. |  |
| 1. Funkcje Systemu Bezpieczeństwa | 1. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 2. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 3. Kontrola Aplikacji. 4. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 5. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 6. Ochrona przed atakami - Intrusion Prevention System. 7. Kontrola stron WWW. 8. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3 9. Zarządzanie pasmem (QoS, Traffic shaping). 10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 11. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 12. Analiza ruchu szyfrowanego protokołem SSL. 13. Analiza ruchu szyfrowanego protokołem SSH. |  |
| 1. Polityki, Firewall | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:    1. Translację jeden do jeden oraz jeden do wielu.    2. Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu:    1. Amazon Web Services (AWS).    2. Microsoft Azure    3. Cisco ACI.    4. Google Cloud Platform (GCP).    5. Nuage Networks VSP.    6. OpenStack.    7. VMware vCenter (ESXi).    8. VMware NSX. |  |
| 1. Połączenia VPN | 1. System UTM musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:    1. Wsparcie dla IKE v1 oraz v2.    2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).    3. Obsługa protokołu Diffie-Hellman grup 19 i 20.    4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.    5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.    6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.    7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.    8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.    9. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System UTM musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:    1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.    2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.    3. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| 1. Połączenia VPN | 1. System UTM musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:    1. Wsparcie dla IKE v1 oraz v2.    2. Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).    3. Obsługa protokołu Diffie-Hellman grup 19 i 20.    4. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.    5. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.    6. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.    7. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.    8. Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.    9. Mechanizm „Split tunneling” dla połączeń Client-to-Site. 2. System UTM musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:    1. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.    2. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.    3. Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. |  |
| 1. Routing i obsługa łączy WAN | 1. W zakresie routingu system UTM powinien zapewniać obsługę:    1. Routingu statycznego.    2. Policy Based Routingu.    3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. |  |
| 1. Zarządzanie pasmem | 1. System UTM musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. 3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |  |
| 1. Ochrona przed malware | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. 5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. |  |
| 1. Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. 7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |  |
| 1. Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |  |
| 1. Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. 7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji. |  |
| 1. Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:    1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.    2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.    3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. 2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |  |
| 1. Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. |  |
| 1. Logowanie | 1. Elementy systemu UTM muszą realizować logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. W ramach logowania system UTM musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 4. Musi istnieć możliwość logowania do serwera SYSLOG. |  |
| 1. Certyfikaty | Poszczególne elementy oferowanego systemu UTM powinny posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall. |  |
| 1. Serwisy i licencje | Wraz z systemem Firewall powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy. |  |
| 1. Gwarancja oraz wsparcie | 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, 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. 2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty będą weryfikowane na etapie zawarcia umowy. Brak wymaganego dokumentu będzie skutkować uchylaniem się Wykonawcy od zawarcia umowy i zastosowaniem przez Zamawiającego art. 263 ustawy PZP.** |  |

1. **Wymagania dotyczące zarządzalnych przełączników sieciowych.**

Zamawiający wymaga dostarczenia 4 zarządzalnych przełączników sieciowych, z których każdy musi spełnić poniższe parametry.

Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych.

Zamawiający jest w posiadaniu urządzenia FortiSwitch-124F, wymagane jest aby zaoferowane przez Wykonawcę urządzenia były kompatybilne z obecnie posiadanym urządzeniem. Zarządzanie dostarczonymi przełącznikami sieciowymi ma odbywać się poprzez urządzenie UTM, Zamawiający wymaga, aby możliwość zarządzania z poziomu UTM dla urządzeń sieciowych była dla posiadanego urządzenia oraz nowych urządzeń.

**Wymagania minimalne:**

|  |  |  |
| --- | --- | --- |
| Grupa parametrów | Szczegółowe cechy | Spełnia / nie spełnia |
| 1. Parametry fizyczne | 1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Maksymalny pobór mocy: 25 W. 4. Minimalny zakres temperatury pracy: 0-45ᵒC. |  |
| 1. Interfejsy sieciowe | 1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:    1. 48 porty GE RJ-45.    2. 4 porty 10GE, SFP+. |  |
| 1. Zarządzanie | 1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. 2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 3. Wsparcie dla SNMP w wersjach 1-3 4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 9. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 10. Automatycznie wykonywane rewizje konfiguracji. |  |
| 1. Parametry wydajnościowe | 1. Przepustowość urządzenia - min. 100 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 155 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 16 k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 5 mikrosekund. |  |
| 1. Wymagane funkcje | 1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames. 3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Agregacja portów zgodna ze standardem 802.3ad. 5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. 6. Obsługa routingu statycznego. 7. Port-mirroring. 8. Uwierzytelnianie 802.1x na poziomie portu. 9. Uwierzytelnianie 802.1x w oparciu o adres MAC. 10. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). 11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. 13. Obsługa protokołu sFlow. |  |
| 1. 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:    1. Centralne zarządzanie konfiguracją urządzenia    2. Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania    3. Centralne zarządzanie sieciami VLAN.    4. Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u    5. Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..    6. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.    7. 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.    8. Automatyczna detekcja i rekomendacje konfiguracji.    9. Przesyłanie logów na zewnętrzny serwer syslog.    10. Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.    11. Obsługa białych i czarnych list adresów MAC.    12. 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    1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.    2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |  |
| 1. Gwarancja oraz wsparcie | 1. System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, 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. 2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty będą weryfikowane na etapie zawarcia umowy. Brak wymaganego dokumentu będzie skutkować uchylaniem się Wykonawcy od zawarcia umowy i zastosowaniem przez Zamawiającego art. 263 ustawy PZP.** |  |

1. **Wymagania dotyczące urządzeń dostępowych WiFi:**

Zamawiający jest w posiadaniu urządzenia FortiAP-221E, wymagane jest aby zaoferowane przez Wykonawcę urządzenia były kompatybilne z obecnie posiadanym urządzeniem. Zarządzanie dostarczonymi urządzeniami AP ma odbywać się poprzez urządzenie UTM, Zamawiający wymaga, aby możliwość zarządzania z poziomu UTM dla urządzeń AP była dla posiadanego urządzenia oraz nowych urządzeń.

Zamawiający wymaga dostarczenia 4 urządzeń, z których każde musi spełnić poniższe parametry:

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

**Wymagania minimalne:**

|  |  |  |
| --- | --- | --- |
| **Grupa parametrów** | **Szczegółowe cechy** | **Spełnia / nie spełnia** |
| 1. Parametry fizyczne | 1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:    1. Temperatura 0–50°C,    2. 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. |  |
| 1. Moduły radiowe | 1. Urządzenie musi być wyposażone w trzy 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/ax,  c. 5/6 GHz 802.11a/n/ac/ax  4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID. |  |
| 1. Interfejsy | 1. Urządzenie musi być wyposażone w moduł BLE.  2. Urządzenie musi być wyposażone w dwa interfejsy Ethernet: 10/100/1000 Base-TX oraz 100/1000/2500 Base-TX,  3. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz. |  |
| 1. Tryby przesyłania danych | 1. Tunnel, 2. Bridge, 3. Mesh. |  |
| 1. Standardy i metody uwierzytelnienia | 1. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja. 2. 10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST). |  |
| 1. Interfejs radiowy urządzenia powinien wspierać następujące funkcje: | 1. MIMO – 2x2,  2. Maksymalna przepustowość dla poszczególnych modułów radiowych:   1. 574 Mbps; 2. 1201 Mbps; 3. 2401 Mbps;   3. Wymagana moc nadawania:  a) min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;  b) min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;  c) min. 21 dBm dla pasma 6GHz z możliwością zmiany co 1dBm;  4. Wsparcie dla 802.11n 20/40Mhz HT,  5. Wsparcie dla kanałów 80 i 160MHz,  6. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4,5dBi dla pasma 2.4GHz, 5,5dBi dla pasma 5GHz, 5.5dBi dla pasma 6GHz.  7. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,  8. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512; |  |
| 1. Funkcje dodatkowe | 1. OFDMA UL i DL 2. Spatial Reuse (BSS Coloring) 3. UL-MU-MIMO 4. DL-MU-MIMO 5. Enhanced Target Wake Time (TWT) 6. Wbudowany analizator widma 7. Wbudowane mechanizmy WIPS/WIDS |  |
| 1. Gwarancja oraz wsparcie | 1. Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, 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. 2. Wykonawca musi świadczyć pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest zatrudnianie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji) oraz ISO 9001 w zakresie serwisowania urządzeń informatycznych. **Wszystkie certyfikaty będą weryfikowane na etapie zawarcia umowy. Brak wymaganego dokumentu będzie skutkować uchylaniem się Wykonawcy od zawarcia umowy i zastosowaniem przez Zamawiającego art. 263 ustawy PZP.** |  |