Załącznik 1b do SIWZ

**Szczegółowy opis przedmiotu zamówienia dla Cześć 2 : Dostawa i instalacja urządzeń sieciowych**– dotyczy przetargu nieograniczonego na Informatyzację w ZOZ Ostrowiec Świętokrzyskim ramach projektu: „Informatyzacja Placówek Medycznych Województwa Świętokrzyskiego”

# Wymagania ogólne dla dostarczanych rozwiązań:

1. System powstały w wyniku niniejszego zamówienia musi funkcjonować zgodnie z obowiązującymi przepisami prawa w szczególności uwzględniać zmiany dotyczące przedmiotu realizacji projektu.
2. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów.
3. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 9 miesięcy przed datą złożenia oferty) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez Wykonawcę i wyłącznie w celu weryfikacji poprawności działania.
4. Zamawiający zastrzega sobie prawo żądania przeprowadzenia testów poszczególnych funkcjonalności przed wyborem oferty.
5. Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
6. Oferowane urządzenia w dniu składania oferty nie mogą być przeznaczone przez ich producenta do wycofania z produkcji lub sprzedaży.
7. Oferowane oprogramowanie w dniu składania oferty nie może być przeznaczone przez jego producenta do wycofania z produkcji, sprzedaży lub wsparcia technicznego.
8. Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień składania ofert.
9. Dla zaoferowanego oprogramowania należy dostarczyć: licencje, nośniki instalacyjne oraz instrukcje obsługi.
10. Zamawiający wymaga, aby cały dostarczony sprzęt został skonfigurowany, uruchomiony i przetestowany przez Wykonawcę pod nadzorem pracowników Zamawiającego
11. Dostawy wymaganego i opisanego poniżej sprzętu do lokalizacji Zamawiającego
12. Instalacji sprzętu
13. Uruchomienia i konfiguracji system ochrony danych (UTM).
14. Instalacji dostarczonych urządzeń sieciowych oraz konfiguracji sieci LAN, w tym podsieci VLAN zgodnie z wymaganiami Zamawiającego

# Warunki gwarancji

1. Zamawiający wymaga minimum 36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia.

Maksymalny czas naprawy sprzętu - 30 dni.

1. Zgłaszanie awarii musi następować w trybie 8x5.
2. Serwis musi być świadczony bezpośrednio przez producenta sprzętu lub autoryzowany serwis w języku polskim.

Spis treści

[1. Przełącznik rdzeniowy 2](#_Toc34121594)

[2. Firewall 5](#_Toc34121595)

[3. Przełącznik zarządzający 17](#_Toc34121596)

[4. Punkty dostępowe 19](#_Toc34121597)

## Przełącznik rdzeniowy

|  |  |
| --- | --- |
| **Przełącznik rdzeniowy – 2 sztuki**  **Karta katalogowa - TAK** | |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Ilość portów** | Urządzenie musi umożliwiać obsadzenie minimum 48 portów 1GE/10GE definiowanych za pomocą wkładek SFP/SFP+,  Urządzenie musi zapewniać 6 portów 40G QSFP+,  Wszystkie porty 1GE/10GE/40GE muszą być aktywne,  Urządzenie musi obsługiwać wkładki typu 1GE RJ45, 1GE-SX, 10GE-SR oraz 10GE-LR lub równoważne,  Urządzenie musi obsługiwać kable typu 10GE Twinax lub równoważne. |
| **Parametry wydajnościowe** | Wymagana jest prędkość przełączania „wirespeed” dla każdego portu,  Wymagana jest przepustowość przełączania min. 720 Gbps (1440 Gbps duplex),  Wymagany rozmiar tablicy MAC min. 92000. |
| **Wymiary** | Obudowa musi być przeznaczona do montażu w szafie rackowej 19”,  Wysokość urządzenia maksymalnie 1 RU. |
| **Implementacja zaleceń IEEE** | Urządzenie musi obsługiwać następujące protokoły:  IEEE 802.1ab LLDP,  IEEE 802.1p Class of Service,  IEEE 802.1d Spanning Tree Protocol,  IEEE 802.1Qau Congestion Notification,  IEEE 802.1Qaz Enhanced Transmission Selection (ETS),  IEEE 802.1Qbb Priority Flow Control (PFC),  IEEE 802.1q VLAN,  IEEE 802.1s Multiple Spanning Tree Protocol,  IEEE 802.1w Rapid Spanning Tree Protocol,  IEEE 802.1x Port Based Network Access Control,  IEEE 802.3ad LACP,  IEEE 802.3x Flow Control. |
| **Link aggregation** | Urządzenie musi zapewniać:   * Wsparcie dla Static LAG oraz LACP, * Obsługę 32 portów w LAG, |
| **Mechanizmy Data Center oraz wirtualizacji** | Urządzenie musi zapewniać:   * Wsparcie dla Data Center Bridging (DCB) * Wsparcie dla Edge Virtual Bridging (EVB) * Obsługę DCVPN lub EVPN |
| **Zarządzanie, zabezpieczenia** | Urządzenie musi zapewniać:   * Port konsoli CLI, * Port RJ45 10/100/1000Mbps do zarządzania urządzeniem, * Port USB, * Wsparcie dla SSHv2, * Wsparcie dla NETCONF oraz OVSDB, * Wsparcie dla protokołów Authentication, authorization, and accounting (AAA), * Wsparcie dla RADIUS, * Wsparcie dla SNMP v2c, v3, * Wsparcie dla Remote monitoring (RMON). |
| **Zasilanie** | Oferowane urządzenia muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej. |
| **Wyposażenie dodatkowe** | Wraz z przełącznikiem sieciowym należy dostarczyć oraz zainstalować:   * Kompatybilne z przełącznikiem wkładki 10G SFP+ SR (na światłowód wielomodowy) – 10 sztuk/przełącznik * Kompatybilne z przełącznikiem wkładki 1G SFP (na światłowód wielomodowy) – 10 sztuk/przełącznik * Każdy przełącznik wyposażony 10 x DAC 5m SFP+ to SFP+ umożliwiające podłączenie przełączników z dostarczanym sprzętem IT (serwerami wirtualizacji, backupu, bazy danych, macierzami, UTM-ami) * 10 sztuk kabli LC-LC co najmniej OM3 i długości min. 10m |
| **Gwarancja** | Minimum 3 letni serwis producenta obejmujący wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający reakcję w miejscu instalacji maksymalnie na następny dzień roboczy. Wymagana jest dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego. |
| **Uwagi** | Oferowany towar w dniu dostawy nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży (End Of Life, End Of Sale). |

## Firewall

|  |  |
| --- | --- |
| **Firewall – ilość – 1 komplet**  **Karta katalogowa - TAK** | |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa 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 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 bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.  Należy dostarczyć dwa urządzenia UTM skonfigurowane w klastrze HA.  System musi wspierać IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. | |
| **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. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. 3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 4. Monitoring stanu realizowanych połączeń VPN. 5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. |
| **Interfejsy, Dysk, Zasilanie** | 1. System realizujący funkcję Firewall musi dysponować minimum:  * 22 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 2 gniazdami SFP+ 10Gbps  1. System Firewall musi posiadać gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q. 3. System firewall musi posiadać wewnętrzna pamięć SSD min. 480GB 4. System musi być wyposażony w redundantne zasilanie AC. |
| **Parametry wydajnościowe**  **Funkcje Systemu Bezpieczeństwa** | 1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 56.000 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 Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.2 Gbps. 5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 11.5 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.6 Gbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 750 Mbps. |
| W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. 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. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH. |
| **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:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  1. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * 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. * Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
| **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.  1. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
| **Zarządzanie pasmem** | 1. System Firewall 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. |
| **Kontrola Antywirusowa** | 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). |
| **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. Ochrana 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. |
| **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 2100 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. |
| **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 avoidance. 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. 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. 6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
| **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 2. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| **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. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| **Logowanie** | 1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) 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 pełniący funkcję Firewall 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. |
| **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall. * ICSA lub NSS Labs dla funkcji IPS. * ICSA dla funkcji IPSec VPN. * ICSA dla funkcji SSL VPN. |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrole 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 36 miesięcy. |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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. |
| **Uwagi** | Oferowany towar w dniu dostawy nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży (End Of Life, End Of Sale). |
| **System ochrony poczty – 1 sztuka** | |
| Dodatkowo, niezależnie od firewall Wykonawca musi dostarczyć system ochrony poczty, który musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.  Dopuszcza się aby poszczególne elementy wchodzące w skład systemu 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.  Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.  Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:  1. Tryb Gateway.  2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). | |
| **Parametry fizyczne systemu antyspamowego** | 1. System musi być wyposażony w interfejsy, min. 4 porty Gigabit Ethernet RJ-45.  2. System musi być wyposażony w lokalną przestrzeń dyskową o pojemności minimum 1 TB .  3. System musi posiadać wbudowany port konsoli szeregowej.  4. Zasilanie z sieci 230V/50Hz. |
| **Funkcja serwera poczty** | W ramach oferowanego systemu musi zostać dostarczony moduł realizujący funkcję serwera poczty umożliwiający zdefiniowanie co najmniej 150 lokalnych skrzynek pocztowych. Moduł serwera poczty musi integrować się z serwerem LDAP obsługując tym samym pełną listę zdefiniowanych tam użytkowników i przypisanych do nich kont pocztowych.  W tym zakresie dostarczony system musi zapewniać:  1. Obsługę serwisów pocztowych: SMTP, POP3, IMAP.  2. Wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).  3. Definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników.  4. Szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, oraz TLS 1.2).  5. Polski interfejs użytkownika przy dostępie przez WebMail.  6. Lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP.  7. Uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP. |
| **Funkcje systemu ochrony poczty** | Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:  1. Wsparcie dla co najmniej 20 domen pocztowych.  2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 28 tys wiadomości/godzinę.  3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).  4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.  5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).  6. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.  7. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.  8. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.  9. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.  10. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail oraz IMAP.  11. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.  12. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.  13. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.  14. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.  15. Ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention). |
| **Kontrola antywirusowa i ochrona przed malware** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:  1. Skanowanie antywirusowe wiadomości SMTP.  2. Kwarantannę dla zainfekowanych plików.  3. Skanowanie załączników skompresowanych.  4. Definiowanie komunikatów powiadomień w języku polskim.  5. Blokowanie załączników w oparciu o typ pliku.  6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.  7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.  8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.  9. Ochronę typu wirus outbrake. |
| **Kontrola antyspamowa** | System musi zapewniać poniższe funkcje i metody filtrowania spamu:  1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.  2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.  3. Szczegółowa kontrola nagłówka wiadomości.  4. Analiza Heurystyczna.  5. Współpraca z zewnętrznymi serwerami RBL, SURBL.  6. Filtrowanie w oparciu o filtry Bayes’a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.  7. Możliwością dostrajania filtrów Bayes’a przez poszczególnych użytkowników.  8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.  9. Kontrola w oparciu o Greylisting oraz SPF.  10. Filtrowanie treści wiadomości i załączników.  11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.  12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.  13. Ochrona typu outbrake.  14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).  15. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. |
| **Ochrona przed atakami na usługę poczty** | System musi zapewniać poniższe funkcje i metody filtrowania:  1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).  2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.  3. Defniowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.  4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).  5. Weryfikacja poprawności adresu e-mail nadawcy. |
| **Funkcje logowania i raportowania** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:  1. Logowanie do zewnętrznego serwera SYSLOG.  2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.  3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.  4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.  5. Możliwość analizy przebiegu sesji SMTP.  6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.  7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.  8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu. |
| **Funkcje pracy w trybie wysokiej dostępności (HA)** | System ochrony poczty musi posiadać możliwość (po rozbudowie o drugie urządzenie) poniższych funkcji:  1. Konfigurację HA w każdym z trybów: gateway, transparent.  2. Tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP.  3. Wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu.  4. Monitorowanie stanu pracy klastra. |
| **Aktualizacje sygnatur, dostęp do bazy spamu** | W tym zakresie dostarczony system ochrony poczty musi zapewniać:  1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.  2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. |
| **Zarządzanie** | System ochrony poczty musi zapewniać poniższe funkcje:  1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.  2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.  3. Powinna istnieć możliwość zdefiniowania co najmniej 7 lokalnych kont administracyjnych. |
| **Certyfikaty** | VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified. |
| **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować min. kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu virus outbrake, na okres 36 miesięcy. |
| **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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. |
|  |  |

## Przełącznik zarządzający

|  |  |
| --- | --- |
| **Przełącznik zarządzający – ilość – 1 sztuka**  **Karta katalogowa - TAK** | |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Obudowa** | Urządzenie przystosowane jest do montażu w szafie stelażowej 19”, wysokość – 1U. Głębokość nie większa niż 50cm |
| **Interfejsy** | * Minimum 24 porty gigabitowe w standardzie 100/1000BaseT * Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Każdy przełącznik wyposażony w 2 sztuki kabli DAC SFP+ o długości co najmniej 3m oraz 2 wkładki SFP+, 10Gb SR LC, optic transceiver |
| **Wydajność** | * Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika) * Wydajność: minimum 95 Mp/s * Tablica adresów MAC o wielkości minimum 32000 pozycji * Wielkość sprzętowej tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6 * Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN |
| **Środowisko** | * Minimalny zakres temperatur pracy od 0°C do 45°C |
| **Zasilanie** | * Dwa (wewnętrzne, modularne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. * Maksymalny pobór mocy nie większy niż 75W |
| **Funkcjonalność** | 1. Obsługa ramek Jumbo 2. Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów) 3. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów) 4. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping 5. Obsługa VXLAN 6. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol 7. Funkcja Root Guard oraz BPDU protection 8. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie 9. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping 10. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI 11. Obsługa standardu 802.1p – min. 8 kolejek na porcie 12. Funkcja mirroringu portów 13. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) 14. Funkcja autoryzacji użytkowników zgodna z 802.1x 15. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ 16. RADIUS Accounting 17. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3 18. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic. 19. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP) 20. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow. 21. Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow. 22. Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az 23. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https 24. Obsługa Syslog 25. Obsługa NTP lub SNTPv4 26. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku 27. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej 28. Wsparcie dla funkcji Private VLAN lub równoważnego 29. Obsługa protokołu VTP lub MVRP 30. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego |
| **Gwarancja** | Dożywotnia (tak długo jak Zamawiający posiada produkt, minimum 3 lata od zakończenia produkcji urządzenia, jednak nie krócej niż 10 lat) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez okres co najmniej 3 lat. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |
| **Uwagi** | Oferowany towar w dniu dostawy nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży (End Of Life, End Of Sale). |

## Punkty dostępowe

|  |  |
| --- | --- |
| **Punkty dostępowe AP – ilość – 50 sztuk**  **Karta katalogowa - TAK** | |
| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| **Funkcjonalność** | Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej lub firewalla.  Obudowa urządzenia musi być wykonana z tworzywa sztucznego i umożliwiać montaż na suficie wewnątrz budynku.  Musi być wyposażone w dwa niezależne moduły radiowe pracujące w pasmach i obsługiwać następujące standardy:   1. 2.4 GHz b/g/n 2. 5 GHz a/n/ac   Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID  Liczba interfejsów Ethernet – 1 w standardzie 10/100/1000 Base-TX  Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz  Interfejs radiowy urządzenia powinien wspierać następujące funkcje:   1. MIMO – 2x2 2. Maksymalna przepustowość interfejsu dla poszczególnych pasm: 3. 2.4GHz – min. 300 Mbps 4. 5 GHz – min. 867 Mbps 5. Wymagana moc nadawania min. 23 dBm 6. Wsparcie dla 802.11n 20/40Mhz HT 7. Wsparcie dla kanału 80 MHz dla 802.11ac 8. Anteny – 4 wbudowane o zysku min. 4dBi dla pasma 2.4GHz, oraz 5dBi dla pasma 5GHz   Punkty dostępowe powinny być dostarczone z zasilaczami PoE. |
| **Gwarancja** | System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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. |
| **Uwagi** | Oferowany towar w dniu dostawy nie może być przeznaczony przez producenta do wycofania z produkcji lub sprzedaży (End Of Life, End Of Sale). |