

PAKIET III – zakup urządzeń infrastruktury IT

1. Zakup urządzenia UTM wraz z licencją, wsparciem producenta oraz wdrożeniem 1 szt. dla Schroniska Młodzieżowego w Śmiglu.

Wymagania Ogólne

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę 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 7 administratorów do poszczególnych instancji systemu.

System wspiera protokoły 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 – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 5 portami Gigabit Ethernet RJ-45.
2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System jest wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 950 Mbps.
4. Wydajność szyfrowania IPsec VPN protokołem AES z kluczem 128 nie mniej niż 4 Gbps.
5. 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 1 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 500 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekami poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są 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. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje 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.

3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.

5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.

6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.

7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure.
- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.
- Kubernetes.

Połączenia VPN

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
 - Wsparcie dla IKE v1 oraz v2.
 - Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
 - Obsługa protokołu Diffie-Hellman grup 19, 20.
 - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
 - 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.
 - Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
 - Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
 - Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
 - Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
 - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv3), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPsec).

Zarządzanie pasmem

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.

5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia 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).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorii tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
 - Hasel statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasel statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasel dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencje

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych

1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego

zastosowania), został uzyskany 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. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

Zakres wdrożenia i wsparcia technicznego:

Do zamawianego sprzętu Wykonawca zapewni usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta świadczone w języku polskim w zakresie na okres 60 miesięcy :

- wsparcie telefoniczne zespołu certyfikowanych inżynierów
- pomoc w prawidłowej i zgodnej z wymaganiami producenta rejestracji produktu
- doradztwo w zakresie konfiguracji
- zdalne wsparcie techniczne
- pomoc w zakładaniu zgłoszeń serwisowych u producenta
- pomoc w procesie realizacji naprawy i wymiany w ramach gwarancji producenta (również za granicą)
- przygotowanie urządzenia do zdalnej konfiguracji
- zdalna konfiguracja urządzenia (połączenia szyfrowane) zgodnie z wymaganiami użytkownika
- rekonfiguracja urządzenia w związku ze zmianą środowiska lub wymagań klienta
- usługa upoważnia do maksymalnie 10 zdalnych zmian w konfiguracji

2.Zakup przełącznika sieciowego zarządzalnego wraz z wdrożeniem 1 szt. dla Schroniska Młodzieżowego w Śmiglu.

Przełącznik sieciowy

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.

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymagany jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach:

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.: 65 W.
- Maksymalny pobór mocy bez budżetu dla PoE: 10 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

- 8 porty GE RJ-45 - w tym porty PoE w ilości co najmniej: 8, zgodne ze standardem: 802.3af oraz 802.3at.
- 2 porty GE, SFP.

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. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 30 Mpps.
- Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 5 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.

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

System musi być objęty serwisem gwarancyjnym producenta przez okres 60 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.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Wymagania dot. montażu, instalacji i konfiguracji sprzętu

Dostarczone urządzenie zostanie podłączone i skonfigurowane z najlepszą wiedzą techniczną i zaleceniami producenta.

Wymagany zakres:

- fizyczny montaż urządzenia w miejscu wskazanym przez Zamawiającego;
- podłączenie urządzenia do istniejącej instalacji prądowej;
- wykonanie weryfikacji prawidłowego działania dostarczonego rozwiązania;

Wykonawca dostarczy komponenty potrzebne do zamontowania dostarczonego urządzenia we wskazanej przez Zamawiającego szafie RACK.

3. Zakup punktów dostępowych 4 szt. dla Schroniska Młodzieżowego w Śmiglu.

Każde z czterech urządzeń 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 0–50°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 wyposażone w złącze typu Kensington.

3. 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. Skaner 2.4GHz i 5GHz

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 dwa interfejsy Ethernet 10/100/1000 Base-TX,

7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3at lub zewnętrzny zasilacz.

8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:

- . Tunnel,
- a. Bridge,
- b. 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, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).

11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:

- . MIMO – 2x2,
- a. Maksymalna przepustowość dla poszczególnych modułów radiowych:
 - i. 574 Mbps;
 - ii. 1201 Mbps;
- b. Wymagana moc nadawania:
 - . min. 23 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
 - i. min. 22 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
- c. Wsparcie dla 802.11n 20/40Mhz HT,
- d. Wsparcie dla kanałów 80MHz,

e. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.

f. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,

g. Maksymalna deklarowana liczba klientów per moduł radiowy:

. 512;

i. 512;

12. Funkcje dodatkowe:

. OFDMA UL i DL

a. Spatial Reuse (BSS Coloring)

b. UL-MU-MIMO 802.11ax

c. DL-MU-MIMO

d. Enhanced Target Wake Time (TWT)

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 60 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.

Wymagania dot. montażu, instalacji i konfiguracji sprzętu

Dostarczone urządzenie zostanie podłączone i skonfigurowane z najlepszą wiedzą techniczną i zaleceniami producenta.

Wymagany zakres:

- fizyczny montaż urządzenia w miejscu wskazanym przez Zamawiającego;
- podłączenie urządzenia do istniejącej instalacji prądowej;
- wykonanie weryfikacji prawidłowego działania dostarczonego rozwiązania;

4. Zakup systemu ochrony poczty zapewniającego kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników dla Urzędu Miejskiego Śmigla

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane

rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure.

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

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Ogólne 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. 25 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. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.
14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.

17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

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.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

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. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.
16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. 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. Definiowanie 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 zapewniać poniższe funkcje:

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 3 lokalnych kont administracyjnych.

Certyfikaty

Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji:

1. VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

Serwisy i licencje

System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

Kontrola Antyspam, URL Filtering, kontrola antywirusowa, ochrona typu Virus Outbreak, Sandbox w chmurze, ochrona typu Click Protect, Content Disarm & Reconstruction, Business Email Compromise na okres 60 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 60 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): 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.

- Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Wymagania dot. montażu, instalacji i konfiguracji sprzętu

Dostarczone urządzenie zostanie podłączone i skonfigurowane z najlepszą wiedzą techniczną i zaleceniami producenta.

Wymagany zakres:

- fizyczny montaż urządzenia w miejscu wskazanym przez Zamawiającego;
- podłączenie urządzenia do istniejącej instalacji prądowej;
- wykonanie weryfikacji prawidłowego działania dostarczonego rozwiązania.

5.Zakup zasilania awaryjnego UPS wraz z konfiguracją - 1 szt. dla Urząd Miejskiego Śmigła

Lp.	Nazwa elementu, parametru lub cechy	Opis wymagań
1	Moc pozorna	3000VA
2	Moc rzeczywista	3000W
3	Technologia (klasyfikacja IEC 62040-3)	Line-Interactive o wysokiej częstotliwości (czysta sinusoida, booster + fader)
4	Współczynnik mocy PF	1.0
5	Gniazda wyjściowe	8 x IEC C13 (10A), 2 x IEC C19 (16A)
6	Gniazda zdalnie sterowane	1 grupa 2 x IEC C13 (10 A) oraz 1 grupa 2 x IEC C13 (10 A) + 1 x IEC C19 (16A)
7	Typ gniazda wejściowego	IEC C20 (16A)
8	Czas podtrzymania dla obciążenia 3000W	20 min.

9	Czas podtrzymania dla obciążenia 1300W	50 min.
10	Dodatkowe moduły bateryjne	Możliwość dodania co najmniej 4 dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do 76 minut dla obciążenia 3000W
11	Zakres napięcia wejściowego bez użycia baterii	160 V-294 V (regulowany do 150 V-294 V)
12	Zakres częstotliwości wejściowej bez użycia baterii	47 do 70 Hz (system 50 Hz), 56,5 do 70 Hz (system 60 Hz), 40 Hz w trybie niskiej czułości
13	Napięcie wyjściowe	230 V (+6/-10%) (regulowane do 200 V* / 208 V / 220 V / 230 V / 240 V), 50/60 Hz +/- 0,1 Hz (autodetekcja)
14	Zarządzanie bateriami	Ładowanie uzależnione od temperatury (wybór przez użytkownika), automatyczny test baterii, ochrona przed głębokim rozładowaniem, automatyczne rozpoznawanie zewnętrznych modułów baterii.
15	System zarządzania pracą baterii	System nieciągłego ładowania baterii. Wraz ze sprzętem dostarczyć należy opis algorytmu ładowania nieciągłego baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta lub musi być przez niego potwierdzony.
16	Możliwość uruchomienia bez napięcia w sieci	Tak
17	Porty komunikacyjne	1 port USB (HID) + 1 port szeregowy RS232 + 1 mini złącze dla zdalnego zał./wył. + 1 mini złącze dla zdalnego wył. + 1 mini złącze dla wyjściowego styku przekaźnikowego
18	Gniazdo komunikacyjne	1 slot na kartę SNM/Ethernet

19	Panel sterowania z wyświetlaczem LCD i paskiem stanu pracy LED	Czytelne informacje dotyczące danych pomiarowych takich jak: aktualne obciążenie [W/VA/%], napięcie i częstotliwość wejścia i wyjścia [V,f], sprawność [%], dane dotyczące baterii [%], minuty, V, ilość podłączonych zewnętrznych modułów bateryjnych]. Możliwość wykonania testu baterii z poziomu wyświetlacza. Możliwość włączania/wyłączania poszczególnych grup gniazd wyjściowych. Wyświetlanie alarmów i rejestrów zdarzeń. Pasek stany pracu LED określający status pracy urządzenia i sygnalizujący konieczność wymiany baterii.
20	Typ obudowy	Uniwersalna Tower/Rack 2U
21	Wypożyczenie standardowe	1 x kabel szeregowy RS-232, 1 x kabel komunikacyjny USB, 1 x kabel zasilający, 2 x kable wyjściowe IEC 10A, komplet szyn montażowych rack 19", komplet uchwytów montażowych tower
22	Wypożyczenie opcjonalne	Zasilacz UPS powinien posiadać możliwość rozbudowy o gigabitową kartę sieciową SNMP/Ethernet (SNMP v1/v3 and IP v4/v6 // Ethernet 10/100/1000BaseT). Ethernet 10Mbps - Half duplex - 10Mbps - Full duplex - 100Mbps - Half duplex - 100Mbps - Full duplex - 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP. Możliwość podłączenia czujników środowiskowych m.in. temperatury i wilgotności. Protokoły: MQTT/RNDIS/LDAP/NVD/SSH/PKI. Podwójne certyfikaty cyberbezpieczeństwa UL 2900-1 i IEC 62443-4-2. RoHS. Dostawca musi zapewnić możliwość automatycznego uaktualniania oprogramowania sprzętowego (firmware) karty poprzez sieć LAN.
23	Pomiar zużycia energii	Pomiar zużycia energii na poziomie grup gniazd. Zmierzone kWh mogą być monitorowane przy użyciu wyświetlacza LCD lub oprogramowania producenta.
24	Maksymalna głębokość UPS i modułu baterijnego	603 mm
25	Maksymalna wysokość UPS / modułu baterijnego	2U / 2U
26	Maksymalny ciężar UPS	31,8 kg
27	Maksymalny ciężar modułu baterijnego	40,5 kg
28	Poziom hałasu w odl. 1m	<40 dB

29	Znaki bezpieczeństwa	CE, cTUVus, EAC, Cm, Ukr, UKCA, Energy Star
30	Gwarancja producenta	36 miesięcy potwierdzone przez producenta

===

Wymagania dot. montażu, instalacji i konfiguracji sprzętu

Dostarczone urządzenie zostanie podłączone i skonfigurowane z najlepszą wiedzą techniczną i zaleceniami producenta.

Wymagany zakres:

- fizyczny montaż urządzenia w miejscu wskazanym przez Zamawiającego;
- podłączenie urządzenia do istniejącej instalacji prądowej;
- wykonanie weryfikacji prawidłowego działania dostarczonego rozwiązania;

6.Zakup serwera plików (NAS) wraz z dyskami dla Urzędu Miejskiego Śmigla.

SPECYFIKACJA SPRZĘTOWA

Procesor	Procesor 32 bit o taktowaniu nie mniejszym niż 1,7 GHz
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 8GB SODIMM DDR3
Pamięć Flash	Nie mniej niż 512MB
Liczba zatok na dyski twarde	Minimum 4
Obsługiwane dyski twarde	3.5" oraz 2.5" SATA oraz 2.5" SSD SATA
Pojemność dysków twardych	do 24TB
Porty LAN 1 Gb/s	Minimum 2 RJ-45
Porty LAN 10 Gb/s	Minimum 1 SFP+
Diody LED	Status, LAN, HDD, USB
Porty USB 3.2	Minimum 4
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 1U

Dopuszczalna temperatura pracy	od 0 do 40°C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Zasilacz o mocy min. 100 W

SPECYFIKACJA OPROGRAMOWANIA

Agregacja łączy	tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Łączenie usług z interfejsem	Tak
Szyfrowanie wolumenów	Tak, min AES 256
Szyfrowanie dysków zewnętrznych	Tak
Zarządzanie dyskami	Pojedynczy Dysk, RAID 0,1, 5, 6, 10, 5+Hot Spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Globalny Hot Spare, Pula pamięci masowej
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL

Obsługa Windows AD	Logowanie użytkowników do domeny poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP,
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox,
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer baz danych MySQL Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN, L2TP
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Możliwość ręcznej aktualizacji oprogramowania Ustawienia: Back up, przywracania, resetowania systemu

Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek *.QPKG
Gwarancja	3 lata

W ramach zamówienia wykonawca dostarczy również dwa dyski o pojemności co najmniej 6TB każdy.

Instalacja: Serwera naz z dyskami i konfiguracja według wskazówek Zamawiającego

7. Hosting i konfiguracja usług pocztowych

1.Przedmiot zamówienia

Przedmiotem zamówienia jest usługa serwera pocztowego w chmurze dla potrzeb Zamawiającego. Serwer powinien umożliwiać zainstalowanie dodatkowej bramki filtrującej. Serwer musi być zlokalizowany fizycznie na terenie Unii Europejskiej i zapewniać pełną funkcjonalność poczty elektronicznej, w tym zarządzanie kontami pocztowymi, przekierowaniami oraz zmianą haseł.

2. Wymagania ogólne

Lokalizacja usługi: Serwer pocztowy musi być zlokalizowany w centrum danych na terenie Unii Europejskiej, aby zapewnić zgodność z przepisami RODO.

Bezpieczeństwo:

- Szyfrowanie danych: Wsparcie dla protokołów SSL/TLS w celu zabezpieczenia transmisji danych.
- Ochrona danych osobowych: Dostawca musi gwarantować zgodność z RODO i przedstawić odpowiednie certyfikaty bezpieczeństwa.

Dostępność usługi: Gwarantowana dostępność na poziomie co najmniej 99,9% w skali miesiąca.

Skalowalność: Możliwość rozszerzenia liczby kont pocztowych oraz przestrzeni dyskowej w przyszłości.

3. Wymagania funkcjonalne

3.1. Zarządzanie kontami pocztowymi

Dodawanie kont: Możliwość tworzenia nowych kont pocztowych przez administratora.

Modyfikacja kont: Edycja ustawień konta, takich jak:

- Zmiana danych użytkownika.
- Przydzielanie i zmiana przestrzeni dyskowej.
- Ustawienia kwot i limitów.

Usuwanie kont: Bezpieczne usuwanie kont pocztowych wraz z danymi.

3.2. Przekierowania poczty

Ustawianie przekierowań: Możliwość przekierowania poczty z jednego konta na inne adresy e-mail.

Aliasowanie: Tworzenie aliasów dla istniejących kont.

3.3. Zmiana haseł

- Przez użytkownika: Użytkownicy muszą mieć możliwość samodzielnej zmiany haseł do swoich kont.
- Przez administratora: Administrator musi mieć możliwość resetowania haseł użytkowników.

4. Interfejs i dostęp

Webmail: Dostęp do poczty przez przeglądarkę internetową z intuicyjnym interfejsem w języku polskim.

Protokoły pocztowe:

- IMAP/IMAPS: Dostęp do poczty przy użyciu protokołu IMAP z obsługą SSL/TLS.
- POP3/POP3S: Wsparcie dla protokołu POP3 z obsługą SSL/TLS.
- SMTP/SMTPS: Wysyłanie poczty przez protokół SMTP z obsługą SSL/TLS.

Kompatybilność: Usługa musi być kompatybilna z popularnymi klientami pocztowymi (np. Microsoft Outlook, Mozilla Thunderbird, klientami mobilnymi).

5. Bezpieczeństwo poczty

Serwer powinien mieć możliwość zainstalowania dodatkowej bramki filtrującej jako kontener lub maszynę wirtualną. Bramka filtrująca powinna być skonfigurowana jako filtr antyspamowy i ochrona antywirusowa pod kątem skanowania złośliwego oprogramowania.

Serwer powinien mieć możliwość instalacji zewnętrznego certyfikatu SSL.

Autoryzacja i autentykacja:

- SPF (Sender Policy Framework).
- DKIM (DomainKeys Identified Mail).
- DMARC (Domain-based Message Authentication, Reporting & Conformance).

6. Przestrzeń dyskowa

Pojemność: Zaplanowanie jest komunikacja za pośrednictwem protokołu POP3S, przez co szacowana przestrzeń to 400GB.

Dodatkowa bramka filtrująca z miejscem do instalacji o pojemności 50GB.

Rozszerzenie pojemności: Opcja zwiększenia przestrzeni dyskowej w razie potrzeby.

7. Panel administracyjny

Dostęp dla administratora: Intuicyjny panel do zarządzania wszystkimi aspektami serwera pocztowego.

Funkcje panelu: Zarządzanie użytkownikami.

Bezpieczeństwo panelu: Dostęp zabezpieczony poprzez uwierzytelnianie dwuskładnikowe (2FA).

8. Wsparcie techniczne

Język wsparcia: Wsparcie techniczne świadczone w języku polskim.

Godziny wsparcia: Minimum w dni robocze od 7:00 do 15:00.

Czas reakcji:

- Krytyczne awarie: Maksymalny czas reakcji – 1 godzina.
- Pozostałe zgłoszenia: Maksymalny czas reakcji – 4 godziny.

Sposób kontaktu: Telefonicznie i poprzez e-mail.

9. Szkolenie i dokumentacja

Szkolenie administratora: Przeprowadzenie szkolenia dla osoby odpowiedzialnej za administrację serwerem.

Dokumentacja:

- Instrukcje obsługi panelu administracyjnego.
- Schemat podłączenia, opis komunikacji i przekazanie dostępu.

10. Zgodność z przepisami

RODO: Usługa musi być w pełni zgodna z Rozporządzeniem o Ochronie Danych Osobowych.

Polityka prywatności: Dostawca musi dostarczyć szczegółową politykę prywatności i bezpieczeństwa danych.

Umowa powierzenia danych: Konieczność zawarcia umowy powierzenia przetwarzania danych osobowych.