ZAMAWIAJĄCY:

Wolbromski Zakład Wodociągów, Kanalizacji, Gospodarki Komunalnej i Mieszkaniowej Sp. z o.o.
ul. Wrzosowa 18, 32-340 Wolbrom
NIP 637-219-91-07

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Na potrzeby postępowania zakupowego pn.: „Wzmocnienie systemu cyberbezpieczeństwa w WZWKGKiM Sp. z o.o. – dostawy uzupełniające" w ramach projektu „Cyberbezpieczne Wodociągi" Inwestycja C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo: „Cyberbezpieczeństwo – Cyberbezpieczne Wodociągi". Krajowy Plan Odbudowy i Zwiększania Odporności finansowany ze środków Instrumentu na Rzecz Odbudowy i Zwiększania Odporności.

Spis treści

Wymagania ogólne 2
1. NGFW (Next Gen FireWall) – 1 szt. 3
2. Zarządzalne urządzenie sieciowe z obsługą PoE – 1 szt. 9
3. Zarządzalne urządzenie sieciowe 8-portowe – 1 szt. 11
4. Serwer do wykonywania kopii zapasowych wraz z dyskami i oprogramowaniem – 1 szt. 13
5. Urządzenie typu UPS wraz z akumulatorem – 1 kpl. 15
6. Szafa RACK wisząca – 1 szt. 16

Wymagania ogólne

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę/Producenta, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia za pomocą dostatecznie dokładnych określeń i jest to uzasadnione specyfiką przedmiotu zamówienia. W takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".

Za rozwiązanie równoważne Zamawiający uzna produkt lub usługę, które spełniają wszystkie parametry techniczne, funkcjonalne i użytkowe wskazane w SOPZ jako minimalne, zapewniają pełną kompatybilność z posiadaną przez Zamawiającego infrastrukturą sprzętowo-programową, nie powodują obniżenia poziomu bezpieczeństwa, wydajności, niezawodności ani funkcjonalności w stosunku do rozwiązania opisanego w SOPZ oraz posiadają certyfikaty i deklaracje zgodności równoważne wymaganym w SOPZ.

Wykonawca, który powołuje się na rozwiązania równoważne, jest obowiązany wykazać w treści oferty, że oferowany przedmiot zamówienia spełnia wymagania określone przez Zamawiającego. W tym celu Wykonawca zobowiązany jest złożyć wraz z ofertą przedmiotowe środki dowodowe, w szczególności karty katalogowe, specyfikacje techniczne producenta, deklaracje zgodności lub certyfikaty wydane przez niezależne jednostki, potwierdzające spełnienie wymagań, o których mowa powyżej.

Dostarczany sprzęt musi być nowy, nieużywany, nieregenerowany, kompletny, wyprodukowany nie wcześniej niż 01.01.2026 r., wolny od jakichkolwiek wad fizycznych i prawnych, sprawny technicznie, pochodzić z oficjalnego kanału dystrybucyjnego producenta, tj. od autoryzowanego przez producenta partnera lub dystrybutora działającego na terytorium Rzeczypospolitej Polskiej lub Unii Europejskiej, z gwarancją producenta realizowaną bezpośrednio lub za pośrednictwem autoryzowanego serwisu na terytorium Rzeczypospolitej Polskiej. Przez „wadę fizyczną" należy rozumieć również jakąkolwiek niezgodność ze szczegółowym opisem przedmiotu zamówienia.

Sprzęt musi być wyposażony we wszystkie niezbędne do jego działania i zapewnienia wymaganych funkcjonalności standardowe rozwiązania softwarowe wraz z prawem do bezterminowego korzystania przez Zamawiającego z tych rozwiązań w takiej funkcji, jednakże w każdym przypadku nie krócej, niż przez czas, w jakim będzie technicznie możliwe używanie sprzętu. Okresy licencji, subskrypcji i wsparcia wskazane w opisie poszczególnych pozycji stanowią okresy minimalne. O ile inaczej nie zaznaczono, wszelkie zapisy SOPZ zawierające parametry techniczne należy odczytywać jako parametry minimalne.

Przedmiot zamówienia obejmuje dostawę urządzeń wraz z oprogramowaniem, licencjami oraz usługami gwarancyjnymi i wsparcia określonymi w opisie poszczególnych pozycji, celem zabezpieczenia drugiej siedziby Zamawiającego.

1. NGFW (Next Gen FireWall) – 1 szt.

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. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.

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 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster 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:
   a) 10 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 10 Gbps dla pakietów 512 B.
3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4) Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 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 1.3 Gbps.
6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.

7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 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 - zapora ogniowa 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 wyciekiem 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:
   a) Translację jeden do jeden oraz jeden do wielu.
   b) 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.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure.
   c) Cisco ACI.
   d) Google Cloud Platform (GCP).
   e) OpenStack.
   f) VMware NSX.
   g) Kubernetes.

Połączenia VPN

1) System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
   a) Wsparcie dla IKE v1 oraz v2.
   b) Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode (GCM).
   c) Obsługa protokołu Diffie-Hellman grup 19, 20.
   d) Wsparcie dla pracy w topologii Hub and Spoke oraz Mesh.
   e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   h) Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
   i) Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
   j) Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
   k) Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   l) Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2) System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
   a) 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.
   b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
   c) 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 RIPng), 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 Injection, 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 kategorie 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:
   a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   c) Haseł 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

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 12 miesięcy.

Gwarancja oraz wsparcie

System jest objęty serwisem gwarancyjnym producenta przez okres minimum 12 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.

2. Zarządzalne urządzenie sieciowe z obsługą PoE – 1 szt.

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

Parametry fizyczne platformy

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 przy pełnym wykorzystaniu budżetu PoE: nie więcej niż 500 W.
4) Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1) Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
   a) 24 porty GE RJ-45, każdy z obsługą zasilania PoE/PoE+ zgodnie ze standardami IEEE 802.3af oraz IEEE 802.3at.
   b) 4 porty 10 GE SFP+.
2) Budżet mocy PoE: min. 330 W.

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.

Parametry wydajnościowe

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

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.
14) Zarządzanie zasilaniem PoE: możliwość włączania i wyłączania zasilania PoE na poszczególnych portach oraz monitorowania poboru mocy PoE.

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:
   a) Centralne zarządzanie konfiguracją urządzenia
   b) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   c) Centralne zarządzanie sieciami VLAN.
   d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
   f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   g) 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.
   h) Automatyczna detekcja i rekomendacje konfiguracji.
   i) Przesyłanie logów na zewnętrzny serwer syslog.
   j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   k) Obsługa białych i czarnych list adresów MAC.
   l) 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.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 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.

3. Zarządzalne urządzenie sieciowe 8-portowe – 1 szt.

W ramach postępowania wymaganym 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, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących z oferowanym systemem bezpieczeństwa, o następujących parametrach.

Parametry fizyczne platformy

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: 10 W.
4) Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

1) Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:
   a) 8 portów GE RJ-45.
   b) 2 porty GE SFP.

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.

Parametry wydajnościowe

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

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.

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:
   a) Centralne zarządzanie konfiguracją urządzenia
   b) Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   c) Centralne zarządzanie sieciami VLAN.
   d) Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   e) Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.
   f) Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   g) 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.
   h) Automatyczna detekcja i rekomendacje konfiguracji.
   i) Przesyłanie logów na zewnętrzny serwer syslog.
   j) Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   k) Obsługa białych i czarnych list adresów MAC.
   l) 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.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 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.

4. Serwer do wykonywania kopii zapasowych wraz z dyskami i oprogramowaniem – 1 szt.

Przedmiotem zamówienia jest dostawa serwera do wykonywania kopii zapasowych typu NAS wraz z zainstalowanymi dyskami HDD i SSD oraz oprogramowaniem do wykonywania kopii zapasowych, przeznaczonego do zabezpieczenia danych w budynku Zamawiającego przy ul. 1 Maja 59.

Parametry sprzętowe

Lp.	Parametr	Wymaganie minimalne
1.	Obudowa	Typu desktop (wolnostojąca). Wymiary umożliwiające ustawienie urządzenia na półce w szafie RACK 19" o głębokości 600 mm, dostarczanej w ramach zamówienia.
2.	Procesor	Procesor wielordzeniowy (min. 4 rdzenie), 64-bitowy, osiągający wynik min. 4 000 pkt w teście PassMark CPU Mark (www.cpubenchmark.net).
3.	Pamięć RAM	Min. 8 GB DDR4 z korekcją błędów ECC. Min. 2 gniazda pamięci, możliwość rozbudowy do min. 32 GB.
4.	Kieszenie na dyski	Min. 8 kieszeni na dyski 3,5" SATA, z obsługą dysków 2,5" SATA SSD. Wymiana dysków bez wyłączania urządzenia (hot-swap).
5.	Gniazda M.2	Min. 2 wbudowane gniazda M.2 2280 NVMe do instalacji dysków SSD, z możliwością wykorzystania dysków jako pamięci podręcznej (cache) lub puli pamięci masowej.
6.	Rozbudowa	Możliwość podłączenia jednostek rozszerzających i zwiększenia liczby obsługiwanych dysków do łącznie min. 18.
7.	Zainstalowane dyski HDD	8 szt. dysków 3,5" SATA 6 Gb/s o pojemności min. 16 TB każdy, zgodnych z listą kompatybilności producenta serwera NAS, o parametrach: a) prędkość obrotowa min. 7 200 obr./min, b) pamięć podręczna min. 256 MB, c) technologia zapisu CMR (konwencjonalny zapis magnetyczny), d) przystosowanie do pracy ciągłej 24/7, obciążenie robocze min. 180 TB/rok, e) średni czas między awariami (MTTF/MTBF) min. 1 000 000 godzin, f) możliwość aktualizacji oprogramowania układowego dysków z poziomu systemu operacyjnego serwera NAS.
8.	Zainstalowane dyski SSD	2 szt. dysków SSD M.2 2280 NVMe (PCIe 3.0 x4 lub nowszy) o pojemności min. 400 GB każdy, zgodnych z listą kompatybilności producenta serwera NAS, o parametrach: a) wytrzymałość min. 490 TBW, b) możliwość aktualizacji oprogramowania układowego dysków z poziomu systemu operacyjnego serwera NAS.
9.	Interfejsy sieciowe	Min. 2 porty 2,5GbE RJ-45. Obsługa agregacji łączy (link aggregation) i przełączania awaryjnego (failover), sieci VLAN (IEEE 802.1Q) oraz ramek Jumbo Frame.
10.	Gniazdo rozszerzeń	Min. 1 gniazdo PCIe umożliwiające instalację karty sieciowej 10GbE lub szybszej (SFP+ lub RJ-45).
11.	Porty zewnętrzne	Min. 2 porty USB 3.2 Gen 1. Min. 1 port do podłączenia jednostek rozszerzających.
12.	Wskaźniki LED	Min. wskaźniki stanu systemu, zasilania, sieci LAN oraz stanu dysków.
13.	Obsługa RAID	Konfiguracje: pojedynczy dysk (basic), JBOD, RAID 0, 1, 5, 6, 10. Obsługa dysków zapasowych typu hot spare. Rozbudowa pojemności przez dodanie dysków lub wymianę dysków na większe oraz zmiana poziomu RAID w trybie online (min. z RAID 1 na RAID 5 oraz z RAID 5 na RAID 6) bez utraty danych.
14.	System plików	Dla dysków wewnętrznych Btrfs lub równoważny, z obsługą migawek (snapshot) oraz wykrywania i samoczynnej naprawy uszkodzonych danych w oparciu o sumy kontrolne. Dla dysków zewnętrznych min.: ext4, NTFS, FAT32, exFAT.
15.	Protokoły i usługi	SMB, NFS, FTP, WebDAV, rsync, iSCSI (min. 32 obiekty docelowe), SSH, SNMP. Integracja z Microsoft Active Directory i LDAP, obsługa uprawnień Windows ACL.

Lp.	Parametr	Wymaganie minimalne
16.	Funkcje bezpieczeństwa i dostępności	a) harmonogramowane migawki (snapshot) udziałów sieciowych i jednostek LUN z polityką retencji, w tym migawki niezmienne (immutable) chronione przed modyfikacją i usunięciem przez określony czas, b) replikacja migawek do innego serwera NAS, c) szyfrowanie AES-256 udziałów sieciowych, d) wbudowana zapora sieciowa (firewall) oraz serwer VPN, e) uwierzytelnianie dwuskładnikowe kont administracyjnych, f) możliwość utworzenia kilku wolumenów w ramach jednej puli pamięci masowej, g) wbudowany mechanizm wirtualizacji umożliwiający uruchamianie maszyn wirtualnych bez zewnętrznego hiperwizora, h) możliwość utworzenia klastra wysokiej dostępności (aktywny-pasywny) z automatycznym przełączaniem awaryjnym, po dołączeniu drugiego, identycznego urządzenia.
17.	Zarządzanie	Zarządzanie przez przeglądarkę WWW, interfejs w języku polskim. Monitorowanie stanu dysków (S.M.A.R.T.), powiadomienia e-mail o zdarzeniach, aktualizacje systemu udostępniane przez producenta. Obsługa zasilaczy awaryjnych UPS (USB lub SNMP) z automatycznym, bezpiecznym wyłączeniem urządzenia.
18.	Zasilanie i chłodzenie	Zasilacz 230 V AC o mocy zapewniającej pracę urządzenia przy pełnym obsadzeniu dysków. Typowy pobór mocy podczas pracy nie większy niż 100 W. Min. 2 wentylatory z regulacją prędkości obrotowej.
19.	Certyfikaty	CE, RoHS.
20.	Gwarancja	Min. 36 miesięcy gwarancji producenta na serwer NAS oraz zainstalowane dyski HDD i SSD. W przypadku awarii nośnika danych uszkodzony dysk pozostaje u Zamawiającego.

5. Urządzenie typu UPS wraz z akumulatorem – 1 kpl.

Przedmiotem zamówienia jest dostawa zasilacza awaryjnego (UPS) współpracującego z zewnętrznym akumulatorem, wraz z akumulatorem, przeznaczonego do podtrzymania zasilania urządzeń zainstalowanych w szafie RACK w budynku przy ul. 1 Maja 59.

Lp.	Parametr	Wymaganie minimalne
1.	Typ urządzenia	Zasilacz awaryjny (UPS) z przetwornicą DC/AC o czystym przebiegu sinusoidalnym, wbudowaną ładowarką akumulatora oraz automatycznym stabilizatorem napięcia (AVR), współpracujący z zewnętrznym akumulatorem 12 V DC.
2.	Moc	Moc chwilowa (szczytowa) min. 2 200 VA. Moc ciągła min. 1 200 W.
3.	Napięcie wejściowe	230 V AC, 50 Hz. Zakres napięcia wejściowego w trybie pracy sieciowej min. 170–270 V AC.
4.	Napięcie wyjściowe	230 V AC, 50 Hz, czysty przebieg sinusoidalny, współczynnik zniekształceń harmonicznych (THD) nie większy niż 3%. Dokładność napięcia wyjściowego w trybie pracy z akumulatora nie gorsza niż ±3%.
5.	Stabilizacja napięcia (AVR)	Automatyczna stabilizacja napięcia w trybie pracy sieciowej, utrzymująca napięcie wyjściowe w zakresie 230 V AC ±10%.
6.	Czas przełączenia	Nie dłuższy niż 10 ms.
7.	Ładowarka	Wbudowana ładowarka akumulatora o prądzie ładowania min. 20 A, przystosowana do akumulatorów AGM i żelowych (GEL).
8.	Zabezpieczenia	Min.: przeciążeniowe, zwarciowe, termiczne, przed głębokim rozładowaniem akumulatora oraz przed przeładowaniem akumulatora.
9.	Sygnalizacja	Wyświetlacz lub wskaźniki LED informujące min. o pracy z sieci lub z akumulatora, ładowaniu oraz stanie akumulatora.
10.	Wyjście	Wyjście 230 V AC w postaci gniazda lub listwy zaciskowej, umożliwiające podłączenie listwy zasilającej szafy RACK.
11.	Warunki pracy	Temperatura pracy min. 0–40°C. Chłodzenie wentylatorem sterowanym temperaturą lub obciążeniem.
12.	Akumulator	1 szt. akumulatora 12 V o pojemności min. 100 Ah, wykonanego w technologii AGM (VRLA), szczelnego, bezobsługowego, przystosowanego do pracy buforowej i cyklicznej, kompatybilnego z zaoferowanym zasilaczem.
13.	Wyposażenie	Przewody do połączenia akumulatora z zasilaczem. Instrukcja obsługi w języku polskim.
14.	Gwarancja	Min. 24 miesiące na zasilacz i akumulator.

6. Szafa RACK wisząca – 1 szt.

Lp.	Parametr	Wymaganie minimalne
1.	Przedmiot zamówienia	Szafa teleinformatyczna RACK 19", wisząca (do montażu na ścianie).
2.	Standard	19", zgodny z IEC 60297 lub równoważny.
3.	Szerokość	600 mm (wymiar nominalny).
4.	Głębokość	600 mm (wymiar nominalny).
5.	Wysokość	Min. 12U.
6.	Konstrukcja	Stalowa, malowana proszkowo, przystosowana do montażu na ścianie. Nośność min. 40 kg.
7.	Drzwi przednie	Szklane lub perforowane, w stalowej ramie, zamykane na klucz.
8.	Panele boczne	Zdejmowane.
9.	Profile montażowe	Min. 1 para profili montażowych 19".
10.	Wentylacja i przepusty	Otwory wentylacyjne lub możliwość montażu panelu wentylacyjnego. Przepusty kablowe w górnej i dolnej części szafy.
11.	Uziemienie	Punkt uziemienia szafy.
12.	Wyposażenie dodatkowe	Dostarczane wraz z szafą: a) min. 2 półki 19" o głębokości min. 250 mm i nośności min. 15 kg każda, b) listwa zasilająca 19" (PDU) z min. 5 gniazdami 230 V, c) komplet śrub montażowych z nakrętkami koszykowymi (min. 20 kpl.).
13.	Stopień ochrony	Min. IP20.
14.	Gwarancja	Min. 24 miesiące.