

## CZĘŚĆ I – ZAKUP I DOSTAWA KOMPUTERÓW I APLIKACJI BIUROWYCH

### 1. Komputer All-in-one: 8 sztuk

Zamówienie obejmuje zakup, dostawę i wniesienie komputerów na 1 piętro budynku Urzędu.

#### Minimalne wymagania sprzętu:

- Ekran: przekątna min.: 23,8 cala
  - Rozdzielczość: 1920x1080 (Full HD)
  - Typ matrycy: TFT, IPS
  - Powierzchnia matrycy: matowa
- Procesor: min. 10-rdzeniowy
- Pamięć RAM: min. 16 GB
- Dysk twardy: min. 512 GB typu SSD M.2 2280 PCI-Express
- Interfejs sieciowy: Ethernet, WiFi
- Porty/Porty USB:
  - Min. 3 x USB Type-A
  - Min. 1 x USB Type-C
- Pozostałe porty wejście/wyjście:
  - 1 x Audio (Combo)
  - 1 x RJ-45
- System operacyjny: Windows 11 Pro
- Typ podstawy: Height Adjustable Stand
- W zestawie: mysz i klawiatura
- Obudowa: All-in-one
- Gwarancja Producenta: min 2 lata (on-site).
- Deklaracja zgodności CE (oświadczenie lub kopia Producenta) dołączona do dokumentacji Wykonawcy.

### 2. Microsoft Office Home and Business 2024 (BOX): 6 sztuk

## CZĘŚĆ II – PRZELĄCZNIK SIECIOWY Z OKABLOWANIEM

### 1. Przełącznik sieciowy z okablowaniem stackującym: 3 sztuki

Zamówienie obejmuje zakup, dostawę i wniesienie urządzeń na 1 piętro Urzędu.

#### 1) Charakterystyka sprzętowa

48 x 1000Base-T IEEE 802.3ab

2 x 10GBase-T IEEE 802.3ae

Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X).

Musi istnieć możliwość zmiany prędkości i duplexu każdego portu i wyłączenia trybu FlowControl dla każdego portu.

4 x SFP+ IEEE 802.3ae/802.3ak. Porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z;

Konsola szeregową RS-232 oraz dedykowany port Ethernet do zarządzania Out-of-Band.

Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 80 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie.

Zasilanie AC 230V. Możliwość użycia dodatkowego zasilacza nadmiarowego.

Pojemność przełączania nie mniej, niż 216 Gb/s. Wydajność przełączania nie mniej niż 161 Mp/s.

Architektura nieblokująca (wire-speed).

Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych.

Ilość RAM nie mniej, niż 2048 MB. Pamięć Flash - nie mniej niż 256 MB.

Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B.

Bufor pakietów nie mniej, niż 4 MB.

Temperatura pracy w zakresie co najmniej od 0C do 50 stopni Celsjusza.

Ochrona przeciwprzepięciową na portach miedzianych co najmniej do 6 kV.

MTBF > 270000 godzin.

Obudowa urządzenia powinna być wyposażona w mocowanie umożliwiające przypięcie zabezpieczenia fizycznego typu Kensington Lock.

#### 2) Funkcjonalności warstwy 2

IGMP Snooping v3 - obsługa nie mniej, niż 1020 grup multicast w tym co najmniej 512 grup statycznych.

MLD Snooping v2 - obsługa nie mniej, niż 1020 grup multicast w tym co najmniej 512 grup statycznych.

Możliwość uwierzytelniania przyłączania do grup multicast.

Możliwość wybiórczego filtrowania zapytań IGMP oraz wybiórczego filtrowania zapytań MLD.

IEEE 802.1D, 802.1w (co najmniej 32 instancji), 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN.

Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP.

Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP.

LLDP (802.1AB) oraz LLDP-MED.



ERPS (ITU-T G.8032) w wersji co najmniej 2. Jednoczesna obsługa co najmniej 24 pierścieni.

DHCP Relay w tym opcji 60 i 61 oraz opcji 82, DHCP Local Relay + opcja 82. DHCP Relay dla IPv6.

Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu oraz monitorowania ruchu na port w innym przełączniku (RSPAN).

Obsługa klastrów MS NLB.

PPPoE Circuit ID Tag Insertion

### 3) Obsługa sieci VLAN

802.1Q VLAN, co najmniej 4094, 802.1v GVRP, QinQ VLAN, VLAN Translation, w tym klasyfikacja co najmniej wg adresów MAC, adresów IP, CVID, priorytetu 802.1p, protokołu IP i portu.

Multicast VLAN (MVR) - co najmniej co najmniej 5 takich sieci VLAN.

Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN.

Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń.

Urządzenie powinno akceptować co najmniej 2040 wpisów MAC dla takiej sieci VLAN.

Urządzenie powinno umożliwiać tworzenie VLANów, które będą zapewniały funkcjonalność tworzenia wielu grup portów w ramach których porty będą mogły się komunikować, ale zablokowana będzie komunikacja pomiędzy portami w różnych grupach oraz wszystkie grupy będą mogły komunikować się z grupą portów wspólnych. Wszystkie porty należące do takich VLANów powinny pozostać nietagowane.

Przełącznik powinien umożliwiać realizację funkcji Super VLAN.

Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN.

Powinna istnieć możliwość liczenia w pakietach przepływającego przez VLAN ruchu.

### 4) Funkcjonalności warstwy 3

Urządzenie powinno posiadać funkcjonalność IGMP w wersji co najmniej 3 oraz obsługiwać nie mniej, niż 1020 grup multicast.

Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 128 takich interfejsów.

Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv6 na urządzeniu - co najmniej 128 takich interfejsów; oraz możliwość utworzenia wielu interfejsów IP na pojedynczej skonfigurowanej sieci VLAN - co najmniej 16 takich interfejsów.

Musi istnieć możliwość skonfigurowania specjalnego interfejsu IP, który jest cały czas dostępny w sieci niezależnie od pozostałej konfiguracji przełącznika (urządzenie powinno umożliwić konfigurację co najmniej 8 instancji takiego interfejsu).

Urządzenie powinno być wyposażone w funkcjonalność umożliwiającą odpowiadanie na zapytania ARP w imieniu urządzenia znajdującego się w innej podsieci VLAN.

Przełącznik musi posiadać funkcjonalność Gratuitous ARP.

Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci.

Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 10 pule adresów IP. Serwer DHCP musi mieć możliwość przydzielania dowolnych opcji DHCP.

Serwer DHCP musi także obsługiwać delegację prefiksów DHCPv6.

Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 4K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych.

Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 4090 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 2048 takich tras dla IPv6.

Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 1020 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 512 takich tras dla IPv6.

Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 510 takich tras) oraz dla IPv6 (co najmniej 250 tras).

Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery.

Przełącznik musi być wyposażony w funkcjonalność umożliwiającą trasowanie ruchu w różnych kierunkach w zależności od zawartości pakietów (np. na podstawie adresu źródłowego IP lub protokołu IP).

Przełącznik musi umożliwiać redystrybucję tras routingu pomiędzy różnymi protokołami routingu skonfigurowanymi na urządzeniu.

Urządzenie powinno umożliwiać konfigurację protokołów routingu dynamicznego: RIP v1 i v2, RIPng, OSPFv2, OSPFv3.

Przełącznik musi obsługiwać trasowanie protokołem OSPF wieloma drogami jednocześnie jeśli koszt trasowania różnymi drogami jest identyczny (maksymalnie 30 jednoczesnych tras), PIM-SM.

Urządzenie powinno obsługiwać także protokół umożliwiający utworzenie wirtualnego routera i zapewniającego dostępność sieci zewnętrznej po awarii jednego z urządzeń fizycznych bez potrzeby specjalnej rekonfiguracji klientów w sieci. Protokół powinien wspierać adresację IPv6.

##### 5) Quality of Service

Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, adresu IPv6, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6.

Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR.

Urządzenie powinno obsługiwać tzw. CIR z minimalną granulacją nie mniejszą, niż 8 kb/s.

Przełącznik powinien umożliwiać kontrolę kongestii ruchu SRED.

Przełącznik powinien umożliwiać kontrolę kongestii ruchu WRED.

Urządzenie powinno umożliwiać limitowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 8 kb/s oraz umożliwiać gwarantowanie pasma osobno dla każdej klasy ruchu (kolejki na porcie fizycznym) z granulacją co najwyżej 8 kb/s.

Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 8 kb/s.

Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 8 kb/s.

Powinna istnieć funkcjonalność limitowania pasma dla określonego typu ruchu (np. odbywającego się na danym porcie TCP lub UDP) z granulacją nie większą, niż 8 kb/s.

Przełącznik powinien mieć możliwość zarządzania QoS wg kalendarza.



#### 6) Filtrowanie ruchu

Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, pole EtherType, sieć VLAN, priorytet 802.1p, adres IP, adres IPv6, zawartość pola DSCP, typ protokołu, flagi protokołu TCP, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 dla ruchu wejściowego i wyjściowego z portów przełącznika i mieć możliwość uruchamiania reguł ACL wg kalendarza.

Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN.

Musi istnieć też możliwość niezależnej filtracji ruchu kierowanego do procesora przełącznika w celu jego dodatkowej ochrony.

#### 7) Funkcje bezpieczeństwa

Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 60 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie.

Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony.

Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika (co najmniej 440 użytkowników na każdym porcie).

Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL.

Przełącznik musi umożliwiać współpracę z serwerem RADIUS w celu realizacji tzw. Accountingu dla przyłączonych użytkowników.

Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta.

Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6.

Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN.

Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.

Urządzenie musi współpracować z funkcjonalnością Microsoft NAP w celu wymuszenia separacji maszyn nie będących w zgodzie z obowiązującą polityką bezpieczeństwa w sieci oraz z funkcjonalnością DHCP NAP.

Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC, z dodatkową możliwością przypisania pary IP-MAC do pojedynczego portu lub grupy portów przełącznika, jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.

Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.).

Urządzenie powinno posiadać możliwość filtrowanie protokołu sieci LAN NetBIOS.

Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.

Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany.

Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci.

Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU.

Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service.

Przełącznik powinien umożliwiać filtrowanie pakietów kontrolnych L3 (np. IGMP-Query, PIM, DVMRP) i nie dopuszczanie ich do wnętrza sieci.

Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 2 pps), Multicast (z krokiem minimalnym co najwyżej 2 pps), Broadcast (z krokiem minimalnym co najwyżej 2 pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.

Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast.

#### 8) Zarządzanie

Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+.

Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP.

Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywanie urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia.

Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia.

Urządzenie musi mieć wbudowaną funkcjonalność klienta Telnet - również poprzez adres IPv6.

W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3.

Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6.

Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON oraz RMONv2 i obsługiwać protokół sFlow.

Urządzenie musi obsługiwać protokół 802.1ag umożliwiający zdalne wykrywanie przerw połączeń w sieci oraz protokół Y.1731.

Przełącznik musi obsługiwać protokół 802.3ah umożliwiający separację domeny Ethernet operatora od sieci Ethernet klienta.



Urządzenie musi posiadać funkcję wykrywania połączeń jednokierunkowych.

Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu.

Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia.

Przełącznik powinien posiadać wbudowanego klienta SMTP.

Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN.

Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6.

Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.

Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.

Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6.

Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z którego polecenie zostało wydane.

Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware oraz wielu wersji konfiguracji.

Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.

Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).

Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach oraz wykrywanie długości linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych.

#### 9) Pozostałe

Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania.

Gwarancja min. 2 lata.

Deklaracja zgodności CE (oświadczenie lub kopia Producenta) dołączona do dokumentacji Wykonawcy.

**Urządzenie powinno posiadać kabel stackujący 10GbE do bezpośredniego podłączenia SFP+ o dł. 100 cm.**

### CZĘŚĆ III – NISZCZARKA

#### 1. Niszczarka do niszczenia dokumentów papierowych oraz nośników cyfrowych: 1 sztuka Zamówienie obejmuje zakup, dostawę i zniesienie niszczarki do piwnicy Urzędu.

##### Minimalne wymagania sprzętu:

- Rodzaj cięcia: cięcie na ścinki;
- Stopień bezpieczeństwa wg normy DIN 66399: min. E-3/F-1/O-3/P-4/T-4;
- Powierzchnia ścinka dla dokumentów papierowych: max 135mm<sup>2</sup>;
- Szerokość ścinka dla dokumentów papierowych max 6mm;
- Szerokość szczeliny wejściowej: min. 330mm;
- Wydajność: min. 40 kartek A4 jednorazowo (przy papierze 70g)
- Wałki tnące wykonane z jednego kawałka hartowanej stali oraz metalowe separatory zapewniające najwyższą jakość cięcia;
- Funkcja pracy ciągłej do niszczenia wąskiego (niestandardowego) materiału bez potrzeby celowania w fotokomórkę;
- Funkcja zabezpieczenia urządzenia kodem PIN chroniąca przed używaniem niszczarki przez osoby trzecie;
- System automatycznego oliwienia wałków tnących zintegrowany w górnej obudowie urządzenia z łatwym dostępem;
- Osłona/klapka bezpieczeństwa zapobiegająca przypadkowemu wciśnięciu materiału podczas niszczenia na całej szerokości podawczej;
- Dotykowy intuicyjny ekran LCD lub dotykowy panel LED informujący w sposób graficzny o tym co się dzieje z urządzeniem;
- Moc silnika: max 1300 W;
- Pojemność kosza na ścinki: min 145 L;
- Zasilanie: 230V;
- Poziom hałasu: 55 dB(A);
- Niszczone materiały: papier, zszywki i spinacze do papieru, karty kredytowe, CD/DVD;
- Pyłoszczelna obudowa urządzenia wykonana z płyty meblowej z okienkiem inspekcyjnym pozwalającym bez otwierania drzwi zweryfikować wypełnienie kosza bez potrzeby jego otwierania;
- Kółka ułatwiające przesuwanie urządzenia;
- Niszczarka przystosowana do pracy ciągłej przez 24h/dobę;
- Gwarancja: 5 lat na urządzenie, dożywotnia na wałki tnące;
- Olej o pojemności 250ml w zestawie;
- Serwis urządzenia prowadzony przez producenta w miejscu instalacji urządzenia
- Deklaracja zgodności CE (oświadczenie lub kopia Producenta) dołączona do dokumentacji Wykonawcy.
- Zamawiający nie dopuszcza wersji specjalnych urządzenia.



## **CZĘŚĆ IV – URZĄDZENIE FORTIGATE**

### **1. Fortigate: 1 sztuka**

Zamówienie obejmuje zakup, dostawę i wniesienie niszczarki na 1 piętro budynku Urzędu.

#### **1) 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 6 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

#### **2) 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.

#### **3) Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
  - 18 portami Gigabit Ethernet RJ-45.
  - 8 gniazdami SFP 1 Gbps.
  - 4 gniazdami SFP+ 10 Gbps.
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 2xAC.

#### **4) Parametry wydajnościowe:**

1. W zakresie Firewall'a obsługa nie mniej niż 3 mln. jednoczesnych połączeń oraz 140 tys. nowych połączeń na sekundę.

2. Przepustowość Stateful Firewall: nie mniej niż 39 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 35 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 5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.8 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

## 5) 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.
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).

## 6) 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.

## **7) 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. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń VPN oferowanym systemem. Oprogramowanie klienckie VPN jest dostępne jako opcja i nie jest wymagane w implementacji.

## **8) 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 RIPv2), 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.

## **9) 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).

#### **10) 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.

#### **11) 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.

#### **12) 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.



9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

### **13) 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).

### **14) 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.

### **15) Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
  - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
  - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
  - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
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.

## **16) 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.

## **17) 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.

## **18) Testy wydajnościowe oraz funkcjonalne**

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

Deklaracja zgodności CE (oświadczenie lub kopia Producenta) dołączona do dokumentacji Wykonawcy.

## **19) Gwarancja oraz wsparcie**

Gwarancja min. 12 miesięcy.