Załącznik 1.2

OPIS PRZEDMIOTU ZAMÓWIENIA

Wymagania ogólne:

1. Przedmiot zamówienia musi pochodzić z legalnego źródła i być przeznaczony do użytkowania w Polsce.
2. Zamawiający, w ramach gwarancji, zastrzega sobie możliwość zgłaszania awarii bezpośrednio w polskiej organizacji serwisowej producenta sprzętu. W przypadku wątpliwości Zamawiający może żądać dokumentów potwierdzających fakt świadczenia serwisu gwarancyjnego przez polską organizację serwisową producenta.
3. Oferowane urządzenia muszą być fabrycznie nowe i nieużywane.
4. Oferowane urządzenia muszą być wyprodukowane zgodnie z normą jakości ISO 9001 lub normą równoważną.
5. Oferowane oprogramowanie i urządzenia muszą posiadać wsparcie techniczne producenta na okres 12 miesięcy.
6. Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
7. Urządzenia muszą być dostarczone Zamawiającemu w oryginalnych fabrycznych opakowaniach producenta.
8. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
9. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta, iż wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

1. Zapora sieciowa typu UTM (1szt.)

Fortigate 600E (Licencja FortiGuard Unified Threat Protection w ramach niniejszego postępowania nie jest wymagana) lub równoważny,
Opis funkcjonalności urządzenia równoważnego:

1.1 Wymagania Ogólne

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

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

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

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall
- Ochrony w warstwie aplikacji
- Protokołów routingu dynamicznego

1.2 Redundancja, monitoring i wykrywanie awarii

a) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

b) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
c) Monitoring stanu realizowanych połączeń VPN.
d) System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

1.3 Interfejsy, dysk, zasilanie:

a) System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - gniazdami SFP+ 10 Gbps.
b) System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
c) W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
d) System musi być wyposażony w zasilanie AC.

1.4 Parametry wydajnościowe:

a) W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 450 tys. nowych połączeń na sekundę.
b) Przepustowość Stateful Firewall: nie mniej niż 36 Gbps dla pakietów 512 B.
c) Przepustowość Firewall z włączoną funkcją kontroli aplikacji: nie mniej niż 15 Gbps
d) Wydajność szyfrowania IPsec VPN nie mniej niż 20 Gbps
e) 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 10 Gbps.
f) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
g) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 8 Gbps.

1.5 Funkcje systemu bezpieczeństwa:

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

a) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
b) Kontrola Aplikacji.
c) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
d) Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
e) Ochrona przed atakami - Intrusion Prevention System.
f) Kontrola stron WWW.
g) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
h) Zarządzanie pasmem (QoS, Traffic shaping).
i) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
j) Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
k) Analiza ruchu szyfrowanego protokołem SSL.
l) Analiza ruchu szyfrowanego protokołem SSH.

1.6 Polityki, firewall:

a) Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

b) System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

c) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

d) Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu:
   - Amazon Web Services (AWS),
   - Microsoft Azure,
   - Cisco ACI,
   - Google Cloud Platform (GCP),
   - OpenStack,
   - VMware vCenter (ESXi).

1.7 Połączenia VPN:

a) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.

b) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

1.8 Routing i obsługa łączy WAN:
W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego,
   - Policy Based Routingu,
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

1.9 Zarządzanie pasmem:

a) System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

b) Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

c) System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

1.10 Ochrona przed malware:

a) Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
b) System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
c) System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
d) System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
e) System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

1.11 Ochrona przed atakami:

a) Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
b) System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
c) Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
d) Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
e) System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
f) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
g) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

1.12 Kontrola aplikacji:

a) Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
b) Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
c) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
d) Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
e) Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

1.13 Kontrola WWW:

a) Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
b) W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
c) Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
d) Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

e) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
f) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
g) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

1.14 Uwierzytelnianie użytkowników w ramach sesji:

a) System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
b) Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
c) Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

1.15 Zarządzanie:

a) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
b) Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
c) Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
d) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
e) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
f) Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
g) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

1.16 Logowanie:

a) Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
b) W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
c) Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
d) Musi istnieć możliwość logowania do serwera SYSLOG.

1.17 Certyfikaty:

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

1.18 Gwarancja oraz wsparcie:

- System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.
- W ramach serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

2. System zarządzania infrastrukturą sieciową

System musi być kompatybilny z przełącznikami posiadanymi przez Zamawiającego oraz z przełącznikami zakupionymi w ramach niniejszego postępowania. Zamawiający posiada przełączniki:

CISCO SG200-26P – 1 szt.
CISCO WS-C2960S-24TS-L – 1 szt.
CISCO WS-C2960S-48TS-S – 3 szt.
CISCO WS-C2960X-24PD-L - 3 szt.
CISCO WS-C2960X-24PS-L – 2 szt.
CISCO WS-C2960X-48FPD-L - 2 szt.
CISCO WS-C2960X-48TS-L – 2 szt.
CISCO WS-C3650-24PD – 12 szt.
CISCO WS-C4500X-32 – 1 szt.

System musi posiadać następujące funkcjonalności:

2.1 Platforma pod system do zarządzania:

a) Umożliwia synchronizację danych między systemami redundantnymi.
b) Instalacja w formie maszyny wirtualnej lub na serwerach fizycznych wspieranych przez producenta systemu.
c) Praca w formie maszyny wirtualnej pracującej pod Vmware ESXi
d) Maksymalne wymagania platformy sprzętowej na której postawiona zostanie maszyna wirtualna to:
   - Ilość pamięci RAM: 16 GB
   - Wielkość przestrzeni dyskowej: 1000 GB
   - Wydajność I/O dysku 320 MBps
   - Ilość procesorów: 8 wirtualnych CPU

2.2 W ogólnym zakresie funkcjonalności:

a) System musi w pełni wspierać obsługę przełączników posiadanych przez zamawiającego. Zamawiający posiada przełączniki: CISCO WS-C2960S, CISCO WS-C4500X, CISCO WS-C3650.
b) Praca w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego miejsca w sieci (po uzyskaniu odpowiednich uprawnień).
c) Interfejs bazujący na HTML5.
d) Budowanie widoków przez użytkownika.
e) Funkcje szybkiej nawigacji wraz z szybkim wyświetlaniem informacji przy zbliżeniu kursora myszy do interesującego obiektu.
f) Hierarchizacja zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów lub zewnętrznego serwera uwierzytelniającego.
g) Narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy.

h) Widok pozwalający na rozmieszczenie urządzeń/grup urządzeń na mapie geograficznej wraz z dynamiczną zmianą stanu ikony reprezentującej daną lokalizację w zależności od alarmów i ogólnej kondycji sieci w danej lokalizacji.
i) Współpraca z serwerami czasu (NTP).
j) Wbudowane formularze do konfiguracji usług na nowych urządzeniach.
k) Wbudowane formularze do weryfikacji możliwości urządzeń pod kątem uruchomienia nowych usług (np. IEEE 802.1X).
l) Narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku
m) Zbieranie Netflow z urządzeń sieciowych.
n) Narzędzie pozwalające na monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania, pozwalające na analizę, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacji oraz jakie jest ich wykorzystanie.
o) Narzędzie pozwalające na diagnostykę działania urządzenia przez wykonanie ping, traceroute, połączenie się z urządzeniem przez telnet, ssh, http, https.
p) Wyświetlanie wykresów korelujących zmiany w konfiguracji ze zdarzeniami na urządzeniu w celu lepszej i szybszej diagnostyki problemów.
q) Narzędzie pozwalające na analizę połączenia urządzeń klienckich i użytkowników podłączonych w sposób przewodowy oraz bezprzewodowy do infrastruktury; narzędzie powinno pozwalać na m.in.: zbieranie informacji o parametrach podłączenia i umożliwiać administratorowi szybką analizę problemów związanych z podłączeniem urządzenia do infrastruktury.
r) Współpraca z systemem od uwierzytelniania i autoryzacji urządzeń klienckich i użytkowników w celu zbierania informacji o polityce dostępowej nałożonej na urządzenie oraz w celu generowania raportów dotyczących statystyk AAA.
s) Posiada licencje na zarządzanie co najmniej 30 urządzeniami.

2.3 W zakresie zarządzania siecią przewodową:

a) Zarządzanie i zbieranie statystyk z wykorzystaniem co najmniej SNMP.
b) Narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci:
c) Możliwość manualnego dodawania urządzeń oraz automatycznego za pośrednictwem protokołów takich jak: LLDP, ARP, OSPF, BGP.
d) Narzędzia wyświetlania urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu.
e) Mapa topologii urządzeń w zakresie przynamniej interfejsów, list kontroli dostępu, wybranych protokołów routingu na routerach.
f) Wbudowane przykładowe wzorce konfiguracji: NTP, SNMP, NAT, itp.
g) Narzędzie do tworzenia wzorców konfiguracji dla urządzenia.
h) Narzędzie do przeprowadzania inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych.
i) Narzędzie do zarządzania obrazami oprogramowania urządzeń.
j) Narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, przynajmniej takich jak: zajętość CPU, zajętość pamięci, dostępność, ilość portów, utylizacja portów, itp.
k) Mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie.
l) Zbieranie statystyk za pomocą Netflow.
m) Monitoring wydajności sieci wraz z możliwością zbierania informacji o aplikacjach w sieci i parametrach ich działania pozwalające na analizę (np. ilość ruchu, czas odpowiedzi, czas transakcji oraz opóźnienie).
n) Narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku.
o) Narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów.
p) Informowanie o alarmach/incydentach przez notyfikację email.
q) Narzędzie do konfiguracji, monitoringu i optymalizacji usług WAN (technologia VPN, polityka routingu oraz polityka QoS z podziałem na aplikację).

3. Przełączniki dostępowy 48 portowy z obsługą 10 Gb (2 szt.)

Urządzenie musi być w pełni obsługiwane przez system zarządzania infrastrukturą sieciową (pkt 2. Niniejszego przedmiotu zamówienia)

Wymagania minimalne:

3.1. Urządzenie posiadające min. 48 portów dostępowych Ethernet 10/100/1000Base-T z MDIX.
3.2. Urządzenie posiadające gniazda na interfejsy światłowodowe 4*10Gb/s w standardzie SFP+. Porty SFP+ powinny wspierać następujące typy wkładek: 1000BaseT, 1000Base-SX, 1000Base-LH, 1000Base-EX, 1000Base-BX-D/U, wkładki 10 Gigabit Ethernet minimum: 10G-AOC10, 10G-ACU10 oraz wkładki 10GBase-LR, 10GBase-ER, 10GBase-SR.
3.3. Urządzenie o wysokości 1U przystosowane do montażu w szafie telekomunikacyjnej 19'' (zapewnienie pełnego wyposażenia montażowego).
3.4. Wydajność wewnętrzna przełącznika (Switching bandwidth) na poziomie 176 Gbps dla pakietów 64-bajtowych. Przepustowość przełącznika (Forwarding bandwidth) minimum 88 Gbps.
3.5. Urządzenie musi posiadać minimum 512MB DRAM i 256MB Flash.
3.6. Urządzenie posiadające możliwość obsługi co najmniej 16000 adresów MAC.
3.7. Urządzenie musi wspierać min. 256 aktywnych VLAN z puli 4094 dostępnych.
3.8. Urządzenie obsługujące protokoły 802.1w (RSTP) i 802.1s (MSTP).
3.9. Wsparcie dla protokołu NTP zapewniająca możliwość synchronizacji czasu z serwerami NTP.
3.10. Obsługę Trivial File Transfer Protocol (TFTP).
3.11. Urządzenie musi posiadać wsparcie dla IPv6 w zakresie IPv6 host, IPv6 DHCP client.
3.12. Urządzenie musi mieć wsparcie protokołów sieciowych zgodnie ze standardami:

- IEEE 802.1s
- IEEE 802.1w
- IEEE 802.3ad
- IEEE 802.1D STP
- IEEE 802.1p
- IEEE 802.1Q
- IEEE 802.3 10BASE-T
- IEEE 802.3u 100BASE-TX
- IEEE 802.3z 1000BASE-X
- IEEE 802.3ab 100BASE-T
- IEEE 802.3z 1000BASE-X

3.13. Urządzenie musi posiadać wsparcie dla 10,240-bajtowych ramek Jumbo.
3.14. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów.
3.15. Obsługa mechanizmów bezpieczeństwa typu Port Security i IP Source Guard na interfejsach link aggregation.

3.16. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

a) Możliwość uzyskania dostępu do urządzenia przez SSHv2, Kerberos i SNMPv3.
b) Możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS i TACACS+.
c) Autoryzacja użytkowników w oparciu o IEEE 802.1X.
d) Monitorowanie zapytań DHCP i odpowiedzi, tzw.: DHCP Snooping.
e) Funkcja tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika.
f) Ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe.
g) Obsługa list kontroli dostępu (ACL) z uwzględnieniem adresów MAC i IP, portów.
h) TCP/UDP bez spadku wydajności urządzenia. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
i) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
j) Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu

uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www oraz zapewniać wsparcie dla Network Edge Access Topology (NEAT).

k) Możliwość uwierzytelniania wielu użytkowników na jednym porcie.
l) Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6.
m) Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard.
n) Możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports).
o) Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
p) Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).
q) min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend).

3.17. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

a) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
b) Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek
c) Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
d) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.

3.18. Urządzenie musi posiadać wbudowane funkcje zarządzania energią:
- Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

3.19. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
3.20. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństwa typu Port Security i IP Source Guard na interfejsach link aggregation
3.21. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
3.22. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash.
3.23. Urządzenie wyposażone w zasilacz 230V AC, 50Hz
3.24. Możliwość zarządzania urządzeniem za pomocą bezpiecznego interfejsu (https) www
3.25. Zapewnia dostęp do konsoli CLI za pomocą urządzenia Bluetooth wpiętego do portu USB-A
3.26. Dedykowany port IP Managment służący do zarządzania do 8 urządzeń na jednym adresie IP
3.27. Obsługę VLAN Trunking Protocol (VTP)
3.28. Wykrywa broadcast, multicast, unicast storm i zapobiega na poziomie portu przeciążeniu stacji roboczych
3.29. Deklaracja producenta okresu bezawaryjnej pracy (MTBF) – min 1400000 godz.

4. Przełączniki dostępowy 48 portowy (1 szt.)

Urządzenie musi być w pełni obsługiwane przez system zarządzania infrastrukturą sieciową (pkt 2. Niniejszego przedmiotu zamówienia)

Wymagania minimalne:

4.1. Urządzenie posiadające min. 48 portów dostępowych Ethernet 10/100/1000Base-T MDIX

4.2. Urządzenie posiadające gniazda na interfejsy światłowodowe 4*1Gb/s w standardzie SFP. Porty SFP powinny wspierać następujące typy wkładek: minimum 1000BaseT, 1000Base-SX, 1000BaseLH, 1000Base-BX-D/U i modułami CWDM.
4.3. Urządzenie o wysokości 1U przystosowane do montażu w szafie telekomunikacyjnej 19'' (zapewnienie pełnego wyposażenia montażowego).
4.4. Wydajność wewnętrzna przełącznika (Switching bandwidth) na poziomie 104 Gbps dla pakietów 64-bajtowych. Przepustowość przełącznika (Forwarding bandwidth) minimum 52 Gbps
4.5. Urządzenie musi posiadać minimum 512MB DRAM i 256MB Flash
4.6. Urządzenie posiadające możliwość obsługi co najmniej 16000 adresów MAC
4.7. Urządzenie musi wspierać min. 256 aktywnych VLAN z puli 4094 dostępnych
4.8. Urządzenie obsługujące protokoły 802.1w (RSTP) i 802.1s (MSTP)
4.9. Wsparcie dla protokołu NTP zapewniająca możliwość synchronizacji czasu z serwerami NTP
4.10. Obsługę Trivial File Transfer Protocol (TFTP)
4.11. Urządzenie musi posiadać wsparcie dla IPv6 w zakresie IPv6 host, IPv6 DHCP client
4.12. Urządzenie musi mieć wsparcie protokołów sieciowych zgodnie ze standardami:

a) IEEE 802.1s
b) IEEE 802.1w
c) IEEE 802.3ad
d) IEEE 802.1D STP
e) IEEE 802.1p
f) IEEE 802.1Q
g) IEEE 802.3 10BASE-T
h) IEEE 802.3u 100BASE-TX
i) IEEE 802.3z 1000BASE-X
j) IEEE 802.3ab 100BASE-T
k) IEEE 802.3z 1000BASE-X

4.13. Urządzenie musi posiadać wsparcie dla 10,240-bajtowych ramek Jumbo
4.14. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

a) Możliwość autoryzacji prób logowania do urządzenia za pomocą serwerów RADIUS i TACACS+
b) Możliwość uzyskania dostępu do urządzenia przez SSHv2, Kerberos i SNMPv3
c) Autoryzacja użytkowników w oparciu o IEEE 802.1X
d) Monitorowanie zapytań DHCP i odpowiedzi, tzw.: DHCP Snooping.
e) Funkcja tworzenia portów monitorujących, pozwalających na kopiowanie na port monitorujący ruchu z innego dowolnie wskazanego portu lub sieci VLAN z lokalnego przełącznika
f) Ochrona przed rekonfiguracją struktury topologii Spanning Tree spowodowana przez niepowołane i nieautoryzowane urządzenie sieciowe
g) Obsługa list kontroli dostępu (ACL) z uwzględnieniem adresów MAC i IP, portów TCP/UDP bez spadku wydajności urządzenia. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
h) Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
i) Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www oraz zapewniać wsparcie dla Network Edge Access Topology (NEAT)
j) Możliwość uwierzytelniania wielu użytkowników na jednym porcie
k) Obsługa list kontroli dostępu (ACL) – dla portów (PACL) i interfejsów SVI (RACL) – zarówno dla IPv4 jak i IPv6
l) Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard
m) Możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLANu (tzw. protected ports)
n) Obsługa funkcjonalności Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

o) Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne)
p) min. 5 poziomów uprawnień do zarządzania urządzeniem (z możliwością konfiguracji zakresu dostępnych funkcjonalności i komend)

4.15. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

a) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowyt port TCP
b) Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym do obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek.
c) Możliwości obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
d) Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi.

4.16. Urządzenie musi posiadać wbudowane funkcje zarządzania energią:

a) Zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

4.17. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
4.18. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństwa typu Port Security i IP Source Guard na interfejsach link aggregation
4.19. Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli
4.20. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash.
4.21. Urządzenie wyposażone w zasilacz 230V AC, 50Hz
4.22. Możliwość zarządzania urządzeniem za pomocą bezpiecznego interfejsu (https) www
4.23. Zapewnia dostęp do konsoli CLI za pomocą urządzenia Bluetooth wpiętego do portu USB-A
4.24. Dedykowany port IP Managment służący do zarządzania do 8 urządzeń na jednym adresie IP
4.25. Obsługę VLAN Trunking Protocol (VTP)
4.26. Wykrywa broadcast, multicast, unicast storm i zapobiega na poziomie portu przeciążeniu stacji roboczych
4.27. Deklaracja producenta okresu bezawaryjnej pracy (MTBF) – min 1400000 godz.

5. Moduły światłowodowe SFP+ (8 sztuk)
Wymagania minimalne:

5.1. Porty: 2x 10 Gbps LC
5.2. Przesył sygnału: Single Mode
5.3. Długość fali TX: 1310
5.4. Długość fali RX: 1310
5.5. Zasięg portu: 2km
5.6. Prędkość transmisji: 10Gb/s
5.7. Obsługa funkcji diagnostycznych DDM
5.8. Kompatybilność z przełącznikami Cisco

6. Patchcordy światłowodowe (10 sztuk)
Wymagania minimalne:

6.1. Rodzaj: Single Mode
6.2. Złącze: LC/UPC-LC/UPC duplex
6.3. Standard włókna: G652D
6.4. Długość: 2m