

I. Specyfikacja przełącznika - 6 sztuk:

1. Typ i liczba portów:
 - 48 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at);
 - 4 porty uplink x 1G/10G .
2. Moc dostępna dla PoE
 - pojedynczy zasilacz 740W;
 - podwójny zasilacz – 1440W.
3. Porty SFP akceptujące następujące typy wkładek:
1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U
4. Przełącznik musi mieć możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:
 - Przepustowość w ramach stosu - 80Gb/s;
 - Min. 8 urządzeń w stosie;
 - Zarządzanie poprzez jeden adres IP;
 - Możliwość tworzenia połączeń cross-stack Link Aggregation zgodnie z IEEE 802.3ad.
5. Zasilanie i chłodzenie
Możliwość instalacji zasilacza redundantnego. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap). Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia.
6. Parametry wydajnościowe:
 - Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów;
 - również dla pakietów 64-bajtowych (przełącznik line-rate);
 - Bufor pakietów – min. 6MB;Obsługa :
 - Min. 4096 VLAN IDs;
 - Min. 16.000 adresów MAC;
 - Min. 3.000 tras IPv4;
 - Min. 1.500 tras IPv6;
 - Ramki Jumbo minimum 9198 bajtów;
 - Min. 16.000 strumieni Netflow;
 - Min. 512 Switched Virtual Interfaces (SVIs);
 - Szybkość przełączania min. 176 Gbps;
 - Szybkość przekazywania min. 130,95 Mpps.
7. Wymagana obsługa protokołu VTP
8. Wymagana obsługa protokołu NTP
9. Pamięć:
 - DRAM – min. 2GB;
 - Pamięć flash – min. 4GB.
10. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
11. Wymagane wsparcie dla mechanizmów związanych z zapewnieniem ciągłości pracy sieci:
 - IEEE 802.1w Rapid Spanning Tree;
 - Per-VLAN Rapid Spanning Tree (PVRST+);
 - IEEE 802.1s Multi-Instance Spanning Tree;
 - Obsługa 64 instancji protokołu STP.
12. Obsługa protokołu LLDP i LLDP-MED.
13. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym oraz docelowym adresie MAC.
14. Wymagana obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych

oraz ruchu głosowego.

15. Wymagana możliwość uruchomienia funkcji serwera DHCP.

16. Wymagane mechanizmy związane z bezpieczeństwem sieci:

- Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level);
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN;
- Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL;
- Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X;
- Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC;
- Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X;
- Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem;
- Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176;
- 1500 wpisów dla list kontroli dostępu (Security ACE);
- Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www);
- Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard;
- Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard);
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+;
- Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL;
- Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch oraz switch-host);
- Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP);
- Funkcja Private VLAN.

17. Wymagane mechanizmy związane z zapewnieniem jakości usług w sieci:

- Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi;
- Implementacja algorytmu Shaped Round Robin dla obsługi kolejek;
- Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority);
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP;
- Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting);
- Kontrola sztormów dla ruchu broadcast/multicast/unicast;
- Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

18. Wymagana obsługa protokołów routingu:

- Routing statyczny dla IPv4 i IPv6;
- Routing dynamiczny – RIP, OSPF (do 1000 tras);

- Policy-based routing (PBR);
 - Obsługa protokołu redundancji bramy (VRRP).
19. Wymagana obsługa mechanizmów SPAN i RSPAN do lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego.
 20. Wymagane predefiniowane (prekonfigurowane) wzorce konfiguracji portów z ustawieniami rekomendowanymi zależnie od typu urządzenia dołączonego do portu (np. telefon IP).
 21. Wymagana możliwość uruchamiania skryptów Python w zależności od zdarzeń, jakie zaszły w urządzeniu.
 22. Wymagane mechanizmy zarządzania urządzeniem:
 - Port konsoli;
 - Dedykowany port Ethernet do zarządzania out-of-band;
 - Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją;
 - Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6;
 - Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów;
 - Port USB umożliwiający podłączenie zewnętrznego nośnika danych z możliwością uruchomienia z nośnika danych umieszczonego w porcie USB.
 23. Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU.
 24. Wsparcie dla próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym – NetFlow.
 25. Jeżeli którakolwiek z funkcjonalności opisanych wyżej wymaga dodatkowych licencji, należy je dostarczyć na min. 3 lata.

Gwarancja i serwis :

Zamawiający wymaga zapewnienia świadczenia serwisu u Producenta lub Partnera dla dostarczanego sprzętu i oprogramowania na okres co najmniej 36 miesięcy.

Wymagany reżim serwisu to (8x5xNBD) wymiana uszkodzonego urządzenia (w lokalizacji Zamawiającego) na następnny dzień roboczy .

Zgłoszenie awarii (potrzebę wsparcia technicznego) Zamawiający dokona u Wykonawcy.

Licencje :

Licencje związane z dostarczonym sprzętem muszą być zarejestrowane na użytkownika końcowego tj. Zamawiającego.

Dodatkowe wymagania stawiane przez Zamawiającego dla przedmiotu zamówienia :

1. Zaoferowane urządzenia muszą umożliwić Zamawiającemu łączenie w stos z posiadanymi przełącznikami CISCO model C9200L-48P-4X-E (2 szt) .
2. Urządzenia w ilości 6 szt. muszą być fabrycznie nowe i nieużywane wcześniej w żadnych innych projektach. Nie dopuszcza się urządzeń typu refurbished/odnowionych (zwróconych do producenta i później odsprzedawanych ponownie przez producenta).
3. Urządzenia muszą pochodzić z legalnego kanału sprzedaży producenta urządzenia. Kupujący zastrzega sobie możliwość weryfikacji numerów seryjnych dostarczonego urządzenia u producenta w celu sprawdzenia czy urządzenie pochodzi z legalnego kanału sprzedaży.
4. Wykonawca, który powołuje się na rozwiązania równoważne opisywane przez Zamawiającego, jest obowiązany wykazać, że oferowane przez niego dostawy, usługi spełniają wymagania określone przez Zamawiającego.

5. Wykonawca oferując produkt równoważny, w ofercie przedstawi dokładną specyfikację oraz ilość dostarczanych elementów (uwzględniając numery katalogowe Producenta) oferowanego rozwiązania.
6. Dokumentacja do urządzenia musi być publicznie dostępna na stronie internetowej producenta.
7. Producent musi publikować na swojej stronie internetowej informacje o wykrytych lukach bezpieczeństwa w oprogramowaniu systemowym urządzenia.

Wkładki

Zamawiający wymaga, aby wkładki w ilości 12 szt. pochodziły od tego samego producenta co oferowany przełącznik.

Wkładki muszą pochodzić z legalnego kanału sprzedaży producenta urządzenia.

Kupujący zastrzega sobie możliwość weryfikacji numerów seryjnych dostarczonego urządzenia u producenta w celu sprawdzenia czy urządzenie pochodzi z legalnego kanału sprzedaży.

II. Specyfikacja systemu zarządzania infrastrukturą sieci przewodowej (LAN):

1. Funkcjonalności 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: możliwość manualnego dodawania urządzeń oraz automatycznego za pośrednictwem protokołów takich jak: LLDP, ARP, OSPF, BGP;
 - c. narzędzia wyświetlania urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu;
 - d. mapa topologii urządzeń z połączeniami oraz wizualizacja alarmów na urządzeniach;
 - e. narzędzia do konfiguracji urządzeń w zakresie przynajmniej interfejsów, list kontroli dostępu, wybranych protokołów routingu na routerach;
 - f. wbudowane przykładowe wzorce konfiguracji urządzeń, takie jak: konfiguracja usług bezpieczeństwa, agregacji linków, konfiguracji: NTP, SNMP, NAT, itp.;
 - g. narzędzie do tworzenia wzorców konfiguracji na urządzenia;
 - h. funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń;
 - i. narzędzie do przeprowadzania inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego urządzeń sieciowych;
 - j. narzędzie do zarządzania obrazami oprogramowania urządzeń;
 - k. narzędzie umożliwiające zbieranie informacji o parametrach urządzeń, przynajmniej takich jak: zajętość CPU, zajętość pamięci, dostępność, ilość portów, użycie portów, itp.;
 - l. mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie;
 - m. zbieranie statystyk za pomocą Netflow;
 - n. 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);
 - o. monitoring, którzy użytkownicy generują najwięcej ruchu, z jakich korzystają aplikacje oraz jakie jest ich wykorzystanie;
 - p. narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku;

- q. narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów;
- r. informowanie o alarmach/incydentach przez notyfikację email;
- s. narzędzie do konfiguracji, monitoringu i optymalizacji usług WAN (technologia VPN, polityka routingu oraz polityka QoS z podziałem na aplikacje).

2. Cechy w ogólnym zakresie funkcjonalności:

- a. praca w trybie przeglądarkowym pozwalając administratorowi na dostęp z dowolnego (po uzyskaniu odpowiednich uprawnień) miejsca w sieci;
- b. interfejs bazujący na HTML5;
- c. budowanie widoków przez użytkownika;
- d. funkcje szybkiej nawigacji wraz z szybkim wyświetlaniem informacji przy zbliżeniu kursora myszy do interesującego obiektu;
- e. hierarchizacja zarządzania – możliwość określenia domen administracyjnych dla administratorów, możliwość wykorzystania wbudowanej bazy administratorów lub zewnętrznego serwera uwierzytelniającego;
- f. narzędzia pozwalające na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy;
- g. 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;
- h. współpraca z serwerami czasu (NTP);
- i. wbudowane formularze do konfiguracji usług na nowych urządzeniach;
- j. wbudowane formularze do weryfikacji możliwości urządzeń pod kątem uruchomienia nowych usług (np. IEEE 802.1X);
- k. narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku;
- l. tworzenie raportów dotyczących urządzeń sieciowych, urządzeń klienckich oraz wydajności sieci;
- 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 aplikacje oraz jakie jest ich wykorzystanie, itp.;
- 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. API REST do integracji z innymi narzędziami/systemami;
 - t. otwieranie i zarządzanie zgłoszeniami dotyczącymi problemów ze sprzętem lub jego konfiguracją do wsparcia producenta bezpośrednio w systemie do zarządzania;
 - u. narzędzie umożliwiające przeszukiwanie forum producenta w celu otrzymania informacji dotyczących problemu lub pomocy diagnostycznej.
3. System powinien zostać dostarczony w formie maszyny wirtualnej pracującej w środowisku VMware ESXi zapewnianym przez Zamawiającego. Maksymalne dopuszczalne wymagania sprzętowe platformy dla systemu zarządzania:
- a. ilość pamięci RAM: 16 GB;
 - b. wielkość przestrzeni dyskowej: 600 GB;
 - c. wydajność I/O dysku: 200 MBps;
 - d. ilość procesorów: 8 wirtualnych CPU.
4. System do zarządzania powinien posiadać w przyszłości możliwość rozbudowy do działania w konfiguracji z wysoką dostępnością (High Availability) w trybie active-standby z synchronizacją danych między systemami redundantnymi. W ramach niniejszego postępowania Zamawiający nie wymaga dostarczenia licencji pozwalających na pracę w wysokiej dostępności.
5. Należy dostarczyć licencje na zarządzanie wszystkimi oferowanymi przełącznikami oraz dla dwóch przełączników, które zamawiający już posiada (model C9200L-48P-4X-E) wraz ze wsparciem serwisowym Producenta i Partnera dla wszystkich licencji na okres 3 lat (8 szt.).

Warunki techniczne opracował:

INSPEKTOR

w Wydziale Administracyjno-Organizacyjnym
i Zarządzania Kryzysowego

Marcin Ślusarz

.....

/podpis i imienna pieczętka/

Zatwierdziła

KIEROWNIK

Wydziału Administracyjno-Organizacyjnego
i Zarządzania Kryzysowego

Agnieszka Bajor

.....

/podpis i imienna pieczętka/