

OPIS PRZEDMIOTU ZAMÓWIENIA

1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa niżej opisanych urządzeń o parametrach technicznych i funkcjonalnych nie gorszych niż wyspecyfikowane.

Przedmiot zamówienia musi pochodzić z legalnego źródła i być przeznaczony do użytkowania w Polsce.

Adres dostawy:
Politechnika Warszawska
Dom Studencki Mikrus,
ul. Waryńskiego 10 pok.1 ,
00-631 Warszawa

2. ZAKRES PRZEDMIOTU ZAMÓWIENIA

Dostawa przełączników

DOSTAWA 14 szt. PRZEŁĄCZNIKÓW Z MOŻLIWOŚCIĄ POŁĄCZENIA W STOS

Specyfikacja przełącznika

1. Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości nie większej niż 1U przystosowanym do montowania w szafie rack 19 cali, wyposażonym w wymienne zasilacze oraz wentylatory.
2. Urządzenie musi być wyposażone w redundanthy zasilacze dostosowane do napięcia zmiennego 220-230V.
3. Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z zabudowanymi interfejsami tranzytowymi 1 oraz 10Gbps.
Przełącznik musi mieć przepustowość nie mniejszą niż 376 Gbps oraz obsługiwać nie mniej niż 279 Mpps (milionów pakietów na sekundę) - przepustowości nieblokujące dla wszystkich wymaganych specyfikacją portów i dla pakietów 85-bajtowych
4. Przełącznik musi być wyposażony co najmniej w następujące interfejsy, zgodne z właściwymi standardami IEEE 802.3
 - 48 portów 1 Gigabit Ethernet RJ-45
 - 4 porty 1/10 Gigabit Ethernet (oddzielne od wymienionych w poprzednim podpunkcie). Typ złącza interfejsu musi być określany przez wymienny moduł SFP+. Lista kompatybilnych modułów SFP28 musi uwzględniać co najmniej
 - Dla prędkości 1Gbps: 1GBase-SX, 1GBase-LX, 1GBase-LH (do min. 70km)
 - Dla prędkości 10Gbps: 10GBase-T, 10GBase-SR, 10GBase-BXD/U, 10GBase-LR, 10GBase-ER, 10GBase-ZR (80km), a także interfejsy typu direct attach (DA) o długościach kabli od 1m do nie mniej niż 7m, co najmniej 3 różne długości w tym zakresie
 - 4 porty 10/25 Gigabit Ethernet (oddzielne od wymienionych w poprzednich podpunktach). Typ złącza interfejsu musi być określany przez wymienny moduł SFP28. Lista kompatybilnych modułów SFP28 musi uwzględniać:
 - Dla prędkości 10Gbps: zgodnie z poprzednim podpunktem
 - Dla prędkości 25Gbps: 25GBase-SR i 25GBase-LR, a także interfejsy typu direct attach (DA) o długościach kabli od 1m do nie mniej niż 7m, co najmniej 3 różne długości w tym zakresie.
5. Wraz z przełącznikiem muszą zostać dostarczone następujące interfejsy wymienne:
 - kable DAC umożliwiające implementację przełącznika wirtualnego o prędkości połączenia z pojedynczego urządzenia fizycznego nie mniej niż 50Gbps. Długość połączeń: 1m; z wyjątkiem kabli dla dwóch odrębnych połączeń w ramach zestawu o długości nie mniej niż 3m.

6. Przełącznik musi być wyposażony w co najmniej jeden interfejs zarządzania OOB GE 1GBase-T RJ-45 oraz port szeregowy konsoli zarządzającej.
7. Przełącznik musi obsługiwać ramki Jumbo o wielkości 9KB
8. Urządzenie musi obsługiwać sprzętowo routing IPv4 oraz IPv6. Pakiety muszą być przełączane w warstwie drugiej i trzeciej modelu OSI bez udziału procesora zarządzającego urządzeniem.
9. Urządzenie musi obsługiwać routing statyczny IPv4 oraz routing dynamiczny IPv4 – co najmniej dla protokołów routingu OSPF, IS-IS oraz BGP. Jeżeli którykolwiek z tych protokołów wymaga dodatkowej licencji, to musi ona zostać dostarczona wraz z urządzeniami. Wymagana skalowalność: 32k tras w tablicy forwardingu sprzętowego unicast, 16k tras multicast
10. Urządzenie musi obsługiwać routing statyczny IPv6 oraz routing dynamiczny IPv6 – co najmniej dla protokołów routingu OSPFv3, IS-IS oraz BGP. Jeżeli którykolwiek z tych protokołów wymaga dodatkowej licencji, to musi ona zostać dostarczona wraz z urządzeniami. Wymagana skalowalność: 16k tras w tablicy forwardingu sprzętowego unicast (można przyjąć prefiksy nie dłuższe niż /64), 8k tras multicast
11. Urządzenie umożliwia konfigurację min. 200 instancji routingowych
12. Urządzenie wspiera agregację linków Ethernet, statyczną oraz z wykorzystaniem protokołu LACP, min. 8 portów per grupa oraz minimum 128 różnych grup per zagregowana grupa urządzeń.
13. Urządzenie musi jednocześnie obsługiwać sprzętowo nie mniej niż 64 tysięcy wpisów w tablicy adresów MAC i 32 tysięcy wpisów w tablicy ARP
14. Urządzenie musi obsługiwać tunelowanie VXLAN. Wymagana jest możliwość następujących konfiguracji urządzenia:
 - Obsługa EVPN/VXLAN z sygnalizacją przez Multiprotocol BGP. Implementacja musi obejmować lokalną replikację broadcastów / unknown unicastów / multicastów
 - Replikacja multicastów z uwzględnieniem snoopingu IGMP.
 - Obsługa ESI dla implementacji redundantnego połączenia urządzeń końcowych z LACP do 2 różnych przełączników jednocześnie
 - Routing pomiędzy segmentami VXLAN, zarówno dla pakietów unicast jak i multicast, z uwzględnieniem podziału na instancje routingowe VRF.
 - Dynamiczny routing w sieci nakładkowej (overlay) z wykorzystaniem protokołów OSPF, ISIS oraz BGP. Musi istnieć możliwość dynamicznego zestawienia sesji protokołu routingu zarówno przez bezpośrednio dołączony interfejs, jak i przez tunel VXLAN (tzn. do przełącznika zdalnego). W szczególności, musi być poprawnie obsługiwany scenariusz wielu peeringów protokołu routingu w jednej podsiaci L3 VXLAN, do różnych przełączników, lokalnych lub zdalnych z perspektywy urządzeń do nich fizycznie przyłączonych.
 - Obsługa tagów bezpieczeństwa (SGT) przez sieć VXLAN i możliwość filtracji na ich podstawie, z uwzględnieniem ruchu lokalnego (wewnątrz pojedynczego przełącznika).
15. Urządzenie musi obsługiwać protokół redundancji VRRP, dla min. 250 rozłącznych grup.
16. Dla protokołu OSPF musi być wspierany mechanizm BFD, nie mniej niż 30 jednoczesnych sesji.
17. Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów (ACL). Filtrowanie musi odbywać się co najmniej na podstawie adresów MAC oraz IPv4/IPv6 łącznie, tzn. pojedyncza definicja ACE (access control entry) może objąć zarówno nagłówki L2 jak i L3. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza. Wymagana jest obsługa filtrów klasy:
 - Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
 - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samej sieci VLAN w obrębie przełącznika,
 - Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN
18. Urządzenie musi obsługiwać protokół SNMP w wersjach 1, 2 i 3. Urządzenie musi udostępniać za pomocą protokołu SNMP co najmniej liczniki ramek i bajtów wysłanych i odebranych na poszczególnych interfejsach tranzytowych.
19. Urządzenie wspiera funkcjonalność SPAN, tzn. wysłanie kopii ruchu na porcie/vlanie na inny port fizyczny, vlan, a także adres IP (z przetunelowaniem nagłówka L2). Ponadto musi istnieć możliwość wysłania kopii nagłówków przechwyconego ruchu przez zaszyfrowany kanał komunikacyjny na podstawie żądania systemu telemetrycznego gRPC.
20. Urządzenie musi posiadać mechanizmy pozwalające na ograniczanie pasma dla ruchu wejściowego na wszystkich interfejsach tranzytowych (z uwzględnieniem filtrów ruchu – ACL).
21. Urządzenie musi posiadać mechanizmy klasyfikowania i znakowania ruchu w oparciu co najmniej 802.1p, DSCP, ToS, oraz adresację z nagłówków L2/L3 na wszystkich portach tranzytowych oraz dla poszczególnych sieci VLAN.
22. Urządzenie musi obsługiwać co najmniej 8 kolejek wyjściowych dla każdego portu tranzytowego z możliwością priorytetyzacji.
23. Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q. Urządzenie musi pozwalać na skonfigurowanie i uruchomienie nie mniej niż 1000 sieci VLAN jednocześnie. Urządzenie wspiera tunelowanie enkapsulacji 802.1Q (Q-in-Q).
24. Urządzenie musi obsługiwać protokoły Spanning Tree – zgodnie z co najmniej IEEE 802.1d, 802.1w i 802.1s. Ponadto przełącznik musi zapewniać kompatybilność z infrastrukturą pracującą zgodnie z protokołem Per-Vlan Spanning Tree.

25. Urządzenie musi wspierać protokół IEEE 802.1X:

- 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 (zarówno istniejącej na urządzeniu, jak i wysłanej przez serwer RADIUS)
- 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,
- Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
- możliwość przypisania klienta do grupy bezpieczeństwa (SGT) w sieci EVPN VXLAN

26. Urządzenie umożliwia edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany.

27. Urządzenie wspiera automatyzację i skryptowanie zarówno w zakresie off-box, jako zewnętrzne oprogramowanie komunikujące się z urządzeniem przez interfejs typu Netconf lub podobny, oraz on-box, jako skrypt podejmujący akcje administracyjne z uwzględnieniem zmiany konfiguracji wykonywalnej jako reakcja na zdarzenia definiowalne na urządzeniu.

28. Urządzenie ma możliwość pracy jako pojedynczy, administrowany z pojedynczej konsoli i pod wspólnym adresem IP przełącznik logiczny w grupie do 10 urządzeń; dystans pomiędzy poszczególnymi urządzeniami fizycznymi może przekraczać 100m. Jeżeli funkcjonalność ta wymaga dodatkowego licencjonowania, to licencje te muszą zostać dostarczone wraz z urządzeniem

29. Obsługa protokołów SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,

30. Możliwość uruchomienia funkcji lokalnego serwera DHCP

31. Inne 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),
- Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+
- 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),
- Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
- Funkcja Private VLAN;

32. Gwarancja producenta na okres min. 5 lat na poniższych warunkach:

- Serwis gwarancyjny ma być świadczony w miejscu instalacji,
- Serwis gwarancyjny musi obejmować dostęp do poprawek oprogramowania w ciągu min. 5 lat od daty zakupu na żądanie Zamawiającego, nie rzadziej niż raz na 3 miesiące, o ile są one dostępne.

CI.ZP.261.11.2022

- Zamawiający musi otrzymać konto pozwalające na samodzielne pobieranie najnowszych wersji oprogramowania i dostęp do biuletynów technicznych dotyczących kwestii bezpieczeństwa, błędów sprzętowych i programowych w odniesieniu do zamawianych modeli urządzeń.
- Serwis gwarancyjny musi obejmować dostęp do nowych wersji oprogramowania, w ciągu min. 5 lat od daty podpisania protokołu odbioru,
- Bieg gwarancji rozpoczyna się w dniu podpisania protokołu odbioru,
- Firma serwisująca posiada wdrożony i stosowany system zarządzania jakością zgodny z normą ISO 9001 lub normą równoważną na świadczenie usług serwisowych w ramach gwarancji.
- Wymiana wadliwego sprzętu następnego dnia roboczego od zgłoszenia awarii.