załącznik nr 2a do Zarządzenia nr 6/2021
Dyrektora Instytutu Nenckiego PAN

instytut biologii doświadczalnej
im. Marcelego Nenckiego PAN

Warszawa, dnia 17.09.2024 r.
(wypełnia Dział Zamówień publicznych i Zaopatrzenia)

OGŁOSZENIE O ZAMIARZE PRZEPROWADZENIA WSTĘPNYCH KONSULTACJI RYNKOWYCH DOTYCZĄCYCH DOSTAWY PRZEŁĄCZNIMÓW SIECIOWYCH PEŁNIĄCYCH FUNKCJĘ PRZEŁĄCZNIKÓW CORE WRAZ Z NIEZBĘDNYMI LICENCJAMI, GWARANCJĄ PRODUCENTA, URUCHOMIENIEM, WDROŻENIEM I ZAPEWNIENIEM WSPARCIA TECHNICZNEGO

organizowanych przez
Instytut Biologii Doświadczalnej im. Marcelego Nenckiego Polskiej Akademii Nauk
z siedzibą w Warszawie przy ul. Ludwika Pasteura nr 3, kod poczt. 02-093.

I. PODSTAWA PRAWNA

Wstępne konsultacje rynkowe prowadzone są na podstawie i zgodnie z przepisami art. 84 ustawy z dnia 11 września 2019 roku Prawo zamówień publicznych (Dz.U. poz. 2019 ze zm.) oraz zgodnie z Regulaminem przeprowadzania wstępnych konsultacji rynkowych, opublikowanym w załączeniu do niniejszego ogłoszenia.

II. PRZEDMIOT ORAZ CEL PROWADZENIA WSTĘPNYCH KONSULTACJI RYNKOWYCH

Zamawiający ogłasza Konsultacje związane z postępowaniem o udzielenie zamówienia publicznego, którego przedmiotem jest:

- Zakup urządzeń wraz z elementami montażowymi.
- Dostawa rozwiązania wraz z oprogramowaniem, niezbędnymi licencjami i gwarancją opartą na kontrakcie serwisowym producenta urządzeń świadczonym w reżimie 24x7x4 przez okres minimum 60.
- Objęte wsparciem Wykonawcy przez cały okres trwania gwarancji (minimum 60 miesięcy) zapewniającym:
  a) pomoc inżyniera w zdiagnozowaniu awarii (zdalna, komunikacja z Zamawiającym z wykorzystaniem poczty e-mail lub telefonicznie w języku polskim)
  b) możliwość założenia i procesowania zgłoszenia serwisowego w Centrum Wsparcia Serwisowego producenta w przypadku problemów z oprogramowaniem (błędy, braki w funkcjonalnościach, nieprawidłowe działanie, itp.)
  c) wsparcie dla procesu obsługi wymiany uszkodzonego urządzenia (logistyka)
  d) zapewnienie udostępnienia nowego oprogramowania.
- Wykonawca, na czas wdrożenia, zapewni wsparcie zdalne inżyniera w wymiarze 40h, w ciągu maksymalnie 60 dni od momentu dostawy urządzeń. Po wykonaniu usług wdrożenia, w ciągu 14 dni należy dostarczyć dokumentację powykonawczą w formie elektronicznej oraz papierowej. Ewidencję czasu pracy inżyniera prowadzi Zamawiający.
- Dodatkowo, Wykonawca zapewni wsparcie zdalne inżyniera, w wymiarze 60 h, realizowane w okresie 24 miesięcy od zakończenia usługi wdrożeniowej, świadczone w dni powszednie, w godzinach pracy 9-17. Każda konsultacja rozliczana jest jako rzeczywisty czas trwania konsultacji. Wykonawca podejmie zlecenie konsultacji w czasie nie dłuższym niż do końca następnego dnia

roboczego liczonego od dnia, w którym wpłynęło zgłoszenie. Ewidencję czasu pracy Inżyniera prowadzi Zamawiający.

Czterech przełączników sieciowych pełniących funkcję przełączników Core:

1. **Typ 1: 2 x przełącznik 32 x 40/100G**
2. **Typ 2: 2 x przełącznik 48 x 1/10/25G**

Jest to jedna z części postępowania „Zwirtualizowane środowisko informatyczne" zaplanowanego w pkt 2.2.11 Planu Postępowań na 2024 rok opublikowanego na stronie internetowej www.nencki.edu.pl w zakładce „Zamówienia Publiczne/Przetargi). Postępowanie będzie finansowane z przedsięwzięcia „ Infrastruktura obrazowania biologicznego i biomedycznego - Bio-Imaging Poland" KPOD.01.18-IW.03-0017/23

Przełączniki sieciowe Core Typu 1 muszą spełniać następujące minimalne wymagania:

Rodzaj urządzenia:

1. Przełącznik typu standalone wyposażony w min. 32 porty 40/100 Gigabit Ethernet QSFP28,
2. Przełącznik powinien umożliwiać przekształcenie portów 40G w porty 1/10G (SFP/SFP+) poprzez zastosowanie adapterów konwertujących 40G QSFP->1G/10G SFP/SFP+. Umożliwia to wówczas zastosowanie następujących wkładek interfejsowych: GE 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10Gigabit Ethernet typu twinax (10GE SFP – 10GE SFP) o dł. min. 1, 3 lub 5 metrów,
3. Porty QSFP28 powinny umożliwiać zastosowanie min. następujących modułów interfejsowych:
   - Dla transmisji 40Gb/s: 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, adapter 40G QSFP->10G SFP+, 40Gigabit Ethernet typu twinax (QSFP - QSFP);
   - Dla transmisji 100Gb/s: 100GBASE-SR4, 100GBASE-LR4, 100Gigabit Ethernet typu twinax (QSFP - QSFP);

Architektura:

1. Możliwość wyposażenia w wymienne moduły wentylatorów,
2. Możliwość wyposażenia w zasilacz redundantny do pracy w trybie 1:1;

Wydajność:

1. Urządzenie powinno posiadać min. 2x32MB (2xASIC) bufor pamięci,
2. Min. 16GB pamięci DRAM i 16GB pamięci flash,
3. Przepustowość przełącznika (switching capacity) powinna wynosić min. 6.4 Tbps,
4. Prędkość przesyłania (forwarding rate) powinna wynosić min. 2 miliardy pps (2Bpps),
5. Obsługa min.:
   - 1000 aktywnych sieci VLAN,
   - 80 000 adresów MAC,
   - 212 000 tras IPv4,
   - 212 000 tras IPv6,
   - Ilość wpisów w listach kontroli dostępu Security ACL – 27 000,
   - ilość wpisów w listach kontroli dostępu QoS ACL – 16 000,
   - 1000 interfejsów SVI L3,

- Jumbo frame 9198B,
- 128 połączeń zagregowanych typu „port channel”,
- 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP;

Oprogramowanie/funkcjonalność:

1. Obsługa protokołu NTP,
2. Obsługa IGMPv1/2/3,
3. Obsługa standardu IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika,
4. System operacyjny przełącznika powinien umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,
5. System operacyjny przełącznika powinien być konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwiać eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów,
6. Wsparcie dla protokołu RESTCONF,
7. Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia,
8. Przełącznik powinien realizować następujące mechanizmy związane 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 min. 1000 instancji protokołu STP;
9. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED,
10. Funkcja serwera DHCP,
11. Obsługa min. 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik powinien umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
12. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
13. Obsługa list kontroli dostępu (ACL) następujących typów:
    - Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
    - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
    - Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
    - Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
14. Przełącznik powinien realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:
    - Min. 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
    - Implementacja algorytmu Shaped Round Robin lub podobnego 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 z dokładnością do 8 Kbps (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;

15. Przełącznik powinien posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
16. Urządzenie powinno realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:
    - Routing statyczny dla IPv4 i IPv6,
    - Routing dynamiczny dla IPv4: OSPF, BGP, ISIS,
    - Routing dynamiczny dla IPv6: OSPFv3,
    - Funkcjonalności Policy-based routing,
    - Multicast routing (PIM-SM, PIM-SSM),
    - Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup,
    - Obsługa min. 200 tuneli GRE (Generic Routing Encapsulation),
    - Obsługa min. 1000 wirtualnych instancji routingu (VRF),
17. Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa min. 100 sesji BFD,
18. Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji,
19. Urządzenie powinno umożliwiać enkapsulację ruchu przy pomocy VXLAN'ów,
20. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,
21. Urządzenie powinno być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze powinny zachowywać się jak jedno urządzenie z punktu widzenia protokołów L2 i L3,
22. Przełącznik powinien umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
23. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),
24. Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,
25. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
    - Statycznie w oparciu o port, do którego podłączona jest stacja,
    - Statycznie w oparciu o VLAN, w którym pracuje stacja,
    - Statycznie w oparciu o adres IP stacji,
    - Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;
26. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
27. Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,
28. Urządzenie powinno mieć możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku SATA

Funkcjonalności z zakresu MPLS:

1. Urządzenie powinno realizować następujące funkcjonalności z zakresu MPLS:
   - L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC,
   - L2VPN - Virtual Private LAN Services (VPLS) - obsługa 1000 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,
   - L3 VPN - MPLS Virtual Private Network (VPN),
   - Multicast VPN (MVPN);

Zarządzanie i konfiguracja:

1. Urządzenie powinno realizować sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi min. 98 000,
2. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który powinien umożliwiać monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
3. Urządzenie powinno posiadać dedykowany port Ethernet do zarządzania out-of-band,
4. Urządzenie powinno posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie powinno mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
5. Urządzenie powinno być wyposażone w port konsoli USB,
6. Urządzenie powinno umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
7. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
8. Przełącznik powinien posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,
9. Przełącznik powinien posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.

Obudowa:

1. Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU

Wyposażenie urządzenia:

1. Przełącznik powinien być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,
2. Przełącznik powinien być wyposażony w następujące moduły QSFP:
   - 100GBASE-LR (QSFP28 LR4 1310nm 10km LC SINGLE RATE 100GbE Single Mode) – 18 sztuk na każdy przełącznik
   - 100Gigabit Ethernet typu twinax (QSFP - QSFP) o długości 1 metra – po 1 sztuce na każdy przełącznik;
3. Urządzenie powinno być wyposażone w licencje na wymagane funkcjonalności na okres minimum 5 lat
4. Urządzenie powinno być wyposażone w zewnętrzną pamięć w postaci dysku M2 SATA o pojemności 240GB.

Przełączniki sieciowe Core Typu 2 muszą spełniać następujące minimalne wymagania:

Rodzaj urządzenia:

1. Przełącznik typu standalone wyposażony w min. 48 portów 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz min. 4 porty uplink 40/100 Gigabit Ethernet QSFP,
2. Porty SFP/SFP+/SFP28 powinny umożliwiać zastosowanie następujących wkładek interfejsowych: 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-ZR, 10Gigabit Ethernet typu twinax (10GE SFP – 10GE SFP), 25GBASE-SR, 25Gigabit Ethernet typu twinax (SFP28 – SFP28), 10/25GBASE-LR (SMF);
3. Porty QSFP powinny umożliwiać zastosowanie następujących modułów interfejsowych:
    - Dla transmisji 40Gb/s: 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, adapter 40G QSFP->10G SFP+, 40Gigabit Ethernet typu twinax (QSFP - QSFP);
    - Dla transmisji 100Gb/s: 100GBASE-SR4, 100GBASE-LR4, 100Gigabit Ethernet typu twinax (QSFP - QSFP);

Architektura:

1. Urządzenie powinno mieć możliwość wyposażenia w wymienne moduły wentylatorów,
2. Urządzenie powinno mieć możliwość wyposażenia w zasilacz redundantny do pracy w trybie 1:1;

Wydajność:

1. Urządzenie powinno posiadać min. 32MB bufor pamięci,
2. Min. 16GB pamięci DRAM i 16GB pamięci flash,
3. Przepustowość przełącznika (switching capacity) powinna wynosić min. 3.2 Tbps,
4. Prędkość przesyłania (forwarding rate) powinna wynosić min. 1 miliard pps (1Bpps),
5. Obsługa min.:
    - 1000 aktywnych sieci VLAN,
    - 80 000 adresów MAC,
    - 212 000 tras IPv4,
    - 212 000 tras IPv6,
    - Ilość wpisów w listach kontroli dostępu Security ACL – 27 000,
    - ilość wpisów w listach kontroli dostępu QoS ACL – 16 000,
    - 1000 interfejsów SVI L3,
    - Jumbo frame 9198B,
    - 128 połączeń zagregowanych typu „port channel”,
    - 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP;

Oprogramowanie/funkcjonalność:

1. Obsługa protokołu NTP,
2. Obsługa IGMPv1/2/3,
3. Obsługa standardu IEEE 802.1ae (MACSec) szyfrowanie ruchu z kluczami o długości 256-bitów dla wszystkich interfejsów przełącznika. Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,
4. System operacyjny przełącznika powinien umożliwiać wgrywanie poprawek bez konieczności restartowania platformy,
5. System operacyjny przełącznika powinien być konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelów danych YANG (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów,
6. Wsparcie dla protokołu RESTCONF,

7. Możliwość uruchamiania zdefiniowanych w Pythonie skryptów w chwili zaistnienia określonego zdarzenia,
8. Przełącznik powinien realizować następujące mechanizmy związane 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 min. 1000 instancji protokołu STP;
9. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED,
10. Realizacja funkcji 802.1Q tunneling (QinQ)
11. Funkcja serwera DHCP,
12. Obsługa min. 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),
13. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
14. Obsługa list kontroli dostępu (ACL) następujących typów:
   - Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
   - VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
   - Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
   - Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
15. Przełącznik powinien realizować następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:
   - Min. 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
   - Implementacja algorytmu Shaped Round Robin lub podobnego 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 z dokładnością do 8 Kbps (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;
16. Przełącznik powinien posiadać wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),
17. Realizacja funkcji Private VLAN zarówno na portach dostępowych oraz portach trunk (obsługa wielu sieci primary VLAN na jednym porcie trunk oraz wielu sieci secondary vlan na jednym porcie trunk),
18. Urządzenie powinno realizować routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:
   - Routing statyczny dla IPv4 i IPv6,
   - Routing dynamiczny dla IPv4: BGP, ISIS, OSPF
   - Routing dynamiczny dla IPv6: OSPFv3,
   - Funkcjonalności Policy-based routing,
   - multicast routing (PIM-SM, PIM-SSM) ,
   - Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup,
   - Obsługa min. 200 tuneli GRE (Generic Routing Encapsulation),

- Obsługa min. 1000 wirtualnych instancji routingu (VRF),

19. Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,
20. Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 3000 translacji,
21. Urządzenie powinno umożliwiać enkapsulację ruchu przy pomocy VXLAN'ów,
22. Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border,
23. Obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia,
24. Urządzenie powinno być przygotowane sprzętowo do łączenia w klaster z drugim takim samym urządzeniem (tzw. wirtualne stakowanie). Urządzenia w klastrze będą zachowywać się jak jedno urządzenie w punktu widzenia protokołów L2 i L3,
25. Klastrowanie powinno wspierać funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami,
26. Przełącznik powinien umożliwiać lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN,
27. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN),
28. Funkcjonalność sondy IP SLA do aktywnego generowania ruchu testowego i mierzenia parametrów ruchu w celu oceny jakości działania sieci dla następujących protokołów sieciowych: dhcp, dns, ftp, http, icmp-echo, icmp-jitter, tcp-connect, udp-echo, udp-jitter,
29. Przełącznik powinien posiadać funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap" do dalszej analizy przy pomocy oprogramowanie zewnętrznego,
30. Wbudowany analizator pakietów,
31. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:
    - Statycznie w oparciu o port, do którego podłączona jest stacja,
    - Statycznie w oparciu o VLAN, w którym pracuje stacja,
    - Statycznie w oparciu o adres IP stacji,
    - Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;
32. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
33. Propagacja informacji o przypisaniu stacji danego znacznika bezpieczeństwa (secure tag) bezpośrednio w ramce Ethernet (metoda in-line) lub za pomocą mechanizmu out-of-band, który przekazuje do urządzeń dokonujących wymuszenia polityki mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa,
34. Urządzenie powinno umożliwiać uruchamianie dodatkowych aplikacji w kontenerach Docker,
35. Urządzenie powinno mieć możliwość wyposażenia w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA
36. Możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 200 AP oraz 4000 klientów bezprzewodowych. Jeśli funkcjonalność wymaga dostarczenia dodatkowych licencji do obsługi AP to nie należy ich dostarczać.

37. Możliwość modyfikacji programowej takich parametrów urządzenia jak: ilości pozycji w tablicy MAC, ilość tras routingowych unicast i multicast, ilości tras w sieci MPLS VPN, ilości obsługiwanych sesji netflow,

Funkcjonalności z zakresu MPLS:

1. Urządzenie powinno realizować następujące funkcjonalności z zakresu MPLS:
   - L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC,
   - L2VPN - Virtual Private LAN Services (VPLS) - obsługa 1000 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,
   - L3 VPN - MPLS Virtual Private Network (VPN),
   - Multicast VPN (MVPN);
   - Inter AS Option A i B,
   - EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS),
   - MPLS over GRE,

Zarządzanie i konfiguracja:

1. Urządzenie powinno realizować sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi min. 98 000,
2. Realizacja rozszerzenia protokołu NetFlow w postaci tzw. Flexible NetFlow, który umożliwia monitorowanie większej ilości informacji zawartej w pakiecie danych od warstw 2 do 7, bardziej granularne monitorowanie ruchu i definiowanie monitorowanych przepływów (flow) poprzez elastyczne definiowanie pól kluczowych,
3. Urządzenie powinno posiadać dedykowany port Ethernet do zarządzania out-of-band,
4. Możliwość realizacji dostępu do konsoli znakowej lub wbudowanego graficznego interfejsu zarządzającego poprzez połączenie bezprzewodowe Bluetooth przy pomocy dodatkowego adaptera usb Bluetooth podłączanego do portu USB przełącznika. Funkcjonalność umożliwia kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
5. Urządzenie powinno posiadać port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
6. Urządzenie powinno być wyposażone w port konsoli USB,
7. Urządzenie powinno umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,
8. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6,
9. Przełącznik powinien posiadać wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,
10. Przełącznik powinien posiadać diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
11. Funkcja programowego resetu urządzenia do ustawień fabrycznych wraz z całkowitym i nieodwracalnym (3-krotne nadpisanie) wyczyszczeniem takich danych jak: konfiguracja urządzenia, pliki logów, zmienne bootowania (startowe), dane uwierzytelniające (tzw. credentials), obrazy oprogramowania, klucze szyfrujące,

Obudowa:

1. Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU. Głębokość chassis urządzenia z wentylatorami, i zasilaczami mniejsza niż 50 cm,

Wyposażenie urządzenia:

1. Przełącznik powinien być wyposażony w zasilacz redundantny identyczny jak zasilacz podstawowy,
2. Przełącznik powinien być wyposażony w następujące moduły interfejsowe SFP / SFP+:
   - 10GBase-SR (SFP+ SR 10Gbs 850nm LC DDM MMF 300m) – 48 wkładek na każdy przełącznik
3. Przełącznik powinien być wyposażony w następujące moduły QSFP:
   - 100Gigabit Ethernet typu twinax (QSFP - QSFP) o długości 1 metra – po dwie sztuki na każdy przełącznik;
4. Urządzenie powinno być wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres minimum 5 lat,
5. Urządzenie powinno być wyposażone w zewnętrzną pamięć w postaci dysku M2 SATA o pojemności 240GB.

Wymagania dla wszystkich urządzeń Typu 1 i Typu 2

Gwarancja:

1. Dostarczony sprzęt wraz z oprogramowaniem musi być objęty gwarancją opartą na kontrakcie serwisowym producenta urządzenia świadczonym w reżimie 24x7x4 przez okres minimum 60 miesięcy, co oznacza:
   a) przyjmowanie zgłoszeń 24h/dobę
   b) wymiana uszkodzonego sprzętu w reżimie 4 godzin
   c) czas obsługi zgłoszenia jest liczony od momentu potwierdzenia zgłoszenia u producenta
   d) nielimitowana ilość zgłoszeń w Centrum Wsparcia Technicznego producenta (z możliwością podglądu statusu złożonego zgłoszenia).
   e) Możliwość składania zgłoszeń serwisowych do Centrum Wsparcia Technicznego producenta bezpośrednio przez Zamawiającego
   f) dostęp do baz wiedzy.
   g) W ramach gwarancji Zamawiający będzie miał zapewniony samodzielny dostęp do najnowszych wersji oprogramowania oraz jego poprawek
2. Zamawiający oczekuje pewności obsługi jak również, że zaoferowana gwarancja zapewni obsługę zgłoszeń awarii i zapytań o pomoc techniczną nawet w przypadku, gdy wybrany Oferent utraci autoryzację producenta.
3. Dodatkowo urządzenie musi być objęte wsparciem Wykonawcy przez cały okres trwania gwarancji (minimum 60 miesięcy) zapewniającym:
   e) pomoc inżyniera w zdiagnozowaniu awarii (zdalna, komunikacja z Zamawiającym z wykorzystaniem poczty e-mail lub telefonicznie w języku polskim)
   f) możliwość założenia i procesowania zgłoszenia serwisowego w Centrum Wsparcia Serwisowego producenta w przypadku problemów z oprogramowaniem (błędy, braki w funkcjonalnościach, nieprawidłowe działanie, itp.)
   g) wsparcie dla procesu obsługi wymiany uszkodzonego urządzenia (logistyka)
   h) zapewnienie udostępnienia nowego oprogramowania.
4. Wykonawca, na czas wdrożenia, zapewni wsparcie zdalne inżyniera w wymiarze 40h, w ciągu maksymalnie 60 dni od momentu dostawy urządzeń. Po wykonaniu usług wdrożenia, w ciągu 14 dni należy dostarczyć dokumentację powykonawczą w formie elektronicznej oraz papierowej. Ewidencję czasu pracy inżyniera prowadzi Zamawiający.
5. Dodatkowo, Wykonawca zapewni wsparcie zdalne inżyniera, w wymiarze 60 h, realizowane w okresie 24 miesięcy od zakończenia usługi wdrożeniowej, świadczone w dni powszednie, w godzinach pracy 9-17. Każda konsultacja rozliczana jest jako rzeczywisty czas trwania konsultacji. Wykonawca podejmie

zlecenie konsultacji w czasie nie dłuższym niż do końca następnego dnia roboczego liczonego od dnia, w którym wpłynęło zgłoszenie. Ewidencję czasu pracy Inżyniera prowadzi Zamawiający.

Wymagania ogólne:

1. Wszystkie Urządzenia muszą być nowe i nieużywane.
2. Urządzenia i elementy wyposażenia muszą być dostarczone w ramach oficjalnego kanału sprzedaży Producenta dla Unii Europejskiej.

Warunki dotyczące zdolności technicznej i zawodowej Wykonawcy:

1. Wykonawca powinien wykazać doświadczenie w zrealizowaniu w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie:
   – co najmniej trzech dostaw przełączników sieciowych, o łącznej wartości nie mniejszej niż 800 000,00 zł brutto;

2. Wykonawca powinien dysponować co najmniej trzema certyfikowanymi osobami posiadającymi wiedzę z zakresu konfigurowania oraz zarządzania rozwiązaniami sieciowymi z uwzględnieniem aspektów bezpieczeństwa oferowanego rozwiązania oraz co najmniej 3 letnie doświadczenie. Dedykowany zespół techniczny inżynierów zaangażowanych w realizację projektu (dostawa i wsparcie serwisowe) powinien posiadać aktualne na dzień składania ofert certyfikaty potwierdzające niezbędne kompetencje:

   a) co najmniej 2 osoby na poziomie eksperckim w zakresie sieciowym z zaproponowanego rozwiązania,
   b) co najmniej 2 osoby na poziomie profesjonalnym z zaproponowanego rozwiązania, przy czym dopuszczalne jest by były to te same osoby spełniające kwalifikacje wskazane w pkt. a),
   c) co najmniej jedna osoba na poziomie eksperckim w zakresie bezpieczeństwa z zaproponowanego rozwiązania,
   d) co najmniej 2 osoby dysponujące certyfikatem bezpieczeństwa informacji ISC2 CISSP przy czym dopuszczalna jest sytuacja by były to te same osoby spełniające kwalifikacje wskazane w pkt. b) lub c),
   e) co najmniej jednej osoby z wiedzą z zakresu zarządzania projektami legitymującej się certyfikatem Project Management Professional.

Osoby o wskazanych powyżej kwalifikacjach powinny legitymować się biegłą znajomość języka polskiego w mowie i piśmie oraz języka angielskiego co najmniej w stopniu umożliwiającym swobodne posługiwanie się dokumentacją techniczną systemów.

Osobą/Osobami uprawnionymi do prowadzenie po stronie Zamawiającego wstępnych konsultacji rynkowych jest/są: ***Agnieszka Kowaluk, Maciej Maszewski***

- Celem wstępnych konsultacji rynkowych jest doradztwo/uzyskanie informacji w zakresie:
  1) Oszacowania wartości zamówienia z podziałem na przełączniki sieciowe oraz wkładki światłowodowe /kable twinax.
  2) Wskazania modelów urządzeń wraz ze specyfikację techniczną.

- Warunki stawiane Uczestnikom Konsultacji (o ile dotyczą):
  NIE DOTYCZY
- Podczas wstępnych konsultacji rynkowych Zamawiający jest uprawniony do ograniczenia lub rozszerzenia zakresu konsultacji do wybranych przez siebie zagadnień, o ile w jego ocenie pozwoli to

na uzyskanie wszystkich istotnych informacji dla planowanego postępowania o udzielenie zamówienia.

III. ZGŁOSZENIE DO UDZIAŁU WE WSTĘPNYCH KONSULTACJACH RYNKOWYCH

1. Zgłoszenie powinno zostać przygotowane według wzoru stanowiącego **załącznik nr 2 do niniejszego Ogłoszenia.**
2. Do zgłoszenia należy załączyć dokument poświadczający umocowanie do reprezentacji podmiotu zgłaszającego. Podmiot zainteresowany nie ma obowiązku złożenia dokumentów, poświadczających należyte umocowanie do reprezentacji, jeżeli Zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych.
3. Zgłoszenia należy składać za pośrednictwem poczty elektronicznej na adres (podać adres osoby/osób prowadzących Konsultacje): a.kowaluk@nencki.edu.pl w terminie do: **25.09.2024 r.**
4. Zamawiający nie jest zobowiązany do zaproszenia do udziału we wstępnych konsultacjach rynkowych podmiotów, które złożą zgłoszenie do udziału po wyznaczonym terminie.

IV. ZASADY PROWADZENIA WSTĘPNYCH KONSULTACJI RYNKOWYCH

1. Zamawiający zaprosi do udziału we Wstępnych konsultacjach rynkowych poprzez wysłanie zaproszenia. Zaproszenie zostanie przesłane na adres e-mail wskazany w Zgłoszeniu do udziału we wstępnych konsultacjach rynkowych.
2. Termin zakończenia Wstępnych konsultacji rynkowych przewidywany jest na dzień **30.09.2024** r.
3. Zamawiający uprawniony jest do przesunięcia terminu zakończenia Wstępnych konsultacji rynkowych. Zamawiający niezwłocznie poinformuje o nowym terminie końcowym, poprzez publikację informacji na stronie internetowej Zamawiającego.

załącznik nr 1 do Ogłoszenia - Regulamin wstępnych konsultacji rynkowych

załącznik nr 2 do Ogłoszenia – formularz zgłoszenia do udziału w konsultacjach

PODPIS ZAUFANY
AGNIESZKA
KOWALUK
17.09.2024 14:09:23 [GMT+2]
Dokument podpisany elektronicznie
podpisem zaufanym

.....
data i podpis Kierownika pracowni/Działu/Projektu