Załącznik nr 1 do SWZ

**Opis przedmiotu zamówienia – specyfikacja techniczna oferowanego sprzętu**

**„Dostawa sprzętu sieciowego na potrzeby Katedry Sztucznej Inteligencji Katolickiego Uniwersytetu Lubelskiego Jana Pawła II”**

**Katolicki Uniwersytet Lubelski Jana Pawła II prowadzi szereg zajęć w ramach „Cisco Networking Academy Program” którego jest członkiem od wielu lat (ID 3072711)**

**Obecnie w celu poprawienia efektywności dydaktycznej istnieje konieczność wymiany bazy szkoleniowej na nową z aktualnym oprogramowaniem zgodnie z poniższymi wymogami.**

**Zadanie 1**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** | **\*** |
| **Producent:** | **\*** |
| **Typ/model/kod producenta:** | **\*** |
| **Router z licencjami i akcesoriami - typ 1 – 6 szt.** | |

**Przedmiot zamówienia**

Przedmiotem zamówienia jest:

* 1. **Dostawa 6 urządzeń**, obejmująca sprzedaż̇ i dostarczenie przez Wykonawcę̨ do Lokalizacji Zamawiającego Urządzeń wraz z dokumentacją i Oprogramowaniem;
  2. Urządzenia będą̨ objęte wsparciem technicznym na Oprogramowanie przez okres 36 miesięcy od dnia podpisania protokołu odbioru dostawy.

1. **Wymagania Ogólne**
   1. Wykonawca wraz z Urządzeniami dostarczy zestaw montażowy rack tj. wszystkie niezbędne elementy konieczne do ich montażu w Lokalizacjach Zamawiającego, w szczególności: śrubki, nakrętki koszykowe, kable zasilające, szyny montażowe, itp.
   2. Urządzenia muszą pochodzić od tego samego producenta oraz być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą̨ znajdować się̨ na liście „end- of-sale”, „end-of-life” oraz „end-of-support” producenta.
   3. Urządzenia muszą posiadać najnowszą dostępną stabilną wersję Oprogramowania.
   4. Nie dopuszcza się oferowania urządzeń, dla których producent nie udostępnia już najnowszej wersji oprogramowania / systemu operacyjnego.
2. **Szczegółowe wymagania dla każdego z Urządzeń**
   1. Musi posiadać co najmniej 4 interfejsów 1GE, z czego dwa powinny umożliwiać wykorzystanie wkładki optycznej SFP. Jeśli oferowane urządzenie posiada 4 wbudowane porty RJ-45, wymagane jest doposażenie o dodatkowy moduł z 2 portami optycznymi SFP.
   2. Urządzenie musi umożliwiać rozszerzenie o moduł łączności poprzez sieć komórkową przynajmniej w standardzie LTE kategorii 6. Moduł powinien pozwalać na przełączania między co najmniej dwoma różnymi operatorami sieci komórkowej.
   3. Komponent sprzętowy zawierający sprzętowy certyfikat X.509v3 oraz łańcuch zaufania, pozwalający realizować bezpieczne uwierzytelnienie urządzenia – w tym również proces automatycznego i bezpiecznie uwierzytelnionego dodania urządzenia do sieci bez konieczności wpisywania haseł jednorazowych, ani logowania się do urządzenia za pomocą WifI, linii poleceń.
   4. Urządzenie mieć możliwość rozszerzenia funkcjonalności o porty telefonii analogowej FXS do podłączania telefonów jako wbudowane w urządzenie lub w ramach modułów rozszerzenia. Oczekuje się możliwości rozszerzenia o minimum 4 porty FXS.
   5. Urządzenie musi mieć możliwość rozszerzenia o obsługę transkodowania strumieni głosowych przynajmniej dla 200 kanałów z sesjami G.711.
   6. Musi być wyposażone w identyfikator RFID i mieć możliwość umieszczenia etykiety z kodem QR.
   7. Musi być wyposażone w co najmniej 4 GB pamięci RAM.
   8. Musi umożliwiać na rozbudowę pamięci RAM do co najmniej 32GB RAM.
   9. Musi być wyposażone w pamięć o pojemności co najmniej 8 GB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych. Musi umożliwiać na rozbudowę pamięci do co najmniej 32GB.
   10. Musi obsługiwać co najmniej 800 000 prefiksów w tablicach routingu IPv4/IPv6 i umożliwiać na rozbudowę przez odpowiednie moduły – do co najmniej 2 500 000 prefiksów IPv4/IPv6.
   11. Musi oferować sumaryczną wydajność dla pakietów 1400B na poziomie przynajmniej 3Gbps dla ruchu IPv4;
   12. Musi oferować sumaryczną wydajność dla pakietów szyfrowanych 1400B na poziomie przynajmniej 500 Mbps dla ruchu IPv4;
   13. Musi być przystosowane do montażu w szafie 19”, obudowa wykonana z metalu;
   14. Musi posiadać zasilacz przystosowany do zasilania prądem naprzemiennym 230V.
3. **Funkcje Oprogramowania**
   1. Musi obsługiwać routing dynamiczny: RIP, OSPF, ISIS, EIGRP, BGP dla IPv4 i IPv6;
   2. Urządzenie mieć możliwość rozszerzenia funkcjonalności o MPLS i MPLS VPN (L2: VPLS, VPWS i L3: VPNv4, VPNv6, mVPN);
   3. Musi być w stanie obsłużyć co najmniej 1000 instancji VRF (Virtual Route Forwarding);
   4. Urządzenie mieć możliwość rozszerzenia funkcjonalności o podłączenia wewnętrznym logicznym interfejsem wirtualny router (VRF) z globalną tablicą routingu.
   5. Musi posiadać ochronę̨ warstwy zarządzającej (Control Plane Policing);
   6. Musi obsługiwać conajmniej 4000 ACL (Access Control Lists) z 20 000 wpisów ACE (Access Control Entries);
   7. Musi wspierać multicast w szczególności: PIM sparse/SSM/Bi-directional, IGMP, MLDv2;
   8. Musi obsługiwać RPF (Reverse Path Forwarding);
   9. Musi obsługiwać zarzadzanie ruchem (QoS):
      1. Minimum 16000 kolejek per system
      2. Hierarchiczne polityki QoS
      3. 3 poziomy hierarchii;
      4. dwie kolejki priorytetowe LLQ per polityka.
   10. Urządzenie mieć możliwość rozszerzenia funkcjonalności o możliwość definicji własnych sygnatur aplikacji, na bazie których nastąpi klasyfikacja ruchu do kolejki QoS.
   11. Musi obsługiwać funkcjonalność Sflow lub odpowiednik (J-Flow, NetFlow);
   12. Musi posiadać funkcjonalność VRRP lub odpowiednika;
   13. Musi umożliwiać zarzadzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3;
   14. Musi posiadać wsparcie dla systemów AAA (RADIUS, TACACS);
   15. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do Urządzenia i uruchomiona;
   16. Urządzenie musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń Urządzenia, dzięki stosowaniu wyrażeń-filtrów;
   17. Urządzenie powinno wspierać standardy szyfrowania ruchu – IPSec z wykorzystaniem co najmniej AES-256 w trybie CBC lub GCM, HMAC-SHA1, ECDSA (256/384 bit), SHA-1 i SHA-2.
4. **Wyposażenia Urządzenia:**
   1. Musi być wyposażony w licencję umożliwiającą skorzystanie z przepustowości
      1. 25/25Mbps (sumarycznie 50Mbps) dla ruchu szyfrowanego.
5. **Wyposażenie 4 z 6 Urządzeń**
   1. 2 portowa karta serialowa WAN z przewodami Smart Serial ok 1 m.
   2. Przewód konsolowy USB-RJ45 do zarządzania urządzeniem
   3. Urządzenie objęte gwarancją i wsparciem technicznym producenta przez okres minimum 12 miesięcy od dnia podpisania protokołu odbioru dostawy.

\*Uwaga, wymagane jest uzupełnienie tabeli

**Zadanie 2**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** | **\*** |
| **Producent:** | **\*** |
| **Typ/model/kod producenta:** | **\*** |
| **Przełącznik 24 portów GE - L2 - typ 1 – 2 szt** | |

**Przedmiot zamówienia**

1. Typ i liczba portów:

24 porty 10/100/1000BaseT RJ-45 + uplink 4x1G SFP

2. Porty SFP możliwe do obsadzenia następującymi rodzajami wkładek:

* Gigabit Ethernet 1000Base-SX,
* Gigabit Ethernet 1000Base-LX/LH,

3. Urządzenie posiadające unkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi,

4. Zasilanie i chłodzenie:

* Urządzenie wyposażone jest w wbudowany zasilacz AC230V,
* Urządzenie wykonanie jest w wersji bezwentylatorowej, głębokość urządzenie nie przekracza 33 cm,

5. Parametry wydajnościowe:

* Przepustowość przełącznika (switching bandwidth):
  + 56 Gb/s (full duplex),
* Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3:
  + 41.67 Mpps,
* Pamięć DRAM – 512 MB
* Pamięć flash – 256 MB
* Wielkość bufora pakietów - 1.5 MB
* Obsługa:
* 256 aktywnych sieci VLAN
* 15000 adresów MAC
* 16 statycznych tras IPv4
* 16 statycznych tras IPv6
* 64 interfejsów SVI L3
* Obsługa MTU-L3 9198B
* Obsługa ramek Ethernet Jumbo 10240B
* 1024 grupy IGMP
* 6 połączeń zagregowanych typu „port channel”
* 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
* Ilość wpisów w listach kontroli dostępu Security ACL – 600
* ilość wpisów w listach kontroli dostępu QoS ACL – 600

6. Porty dostępowe przełącznika posiadają zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

7. Obsługa protokołu NTP

8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

9. Przełącznik wspierający 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 64 instancji protokołu STP

10. Obsługa protokołu LLDP i LLDP-MED

11. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

12. Urządzenie wspierające połączenia link aggregation zgodnie z IEEE 802.3ad

13. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

14. Możliwość uruchomienia funkcji serwera DHCP

15. Mechanizmy związane z bezpieczeństwem sieci:

* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwiający 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 jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication),
* 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),
* Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
* Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
* Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP),
* Funkcja Private VLAN,

16. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

* sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
* bezpieczna sekwencja uruchamiania,
* sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

17. Mechanizmy związane z zapewnieniem jakości usług w sieci:

* Implementacja 4 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 z możliwością skonfigurowania minimum 64 różnych ograniczeń,
* 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. Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6,

19. Przełącznik umożliwiający lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących,

20. Przełącznik posiadający wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),

21. Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow,

22. Zarządzanie

* Port konsoli,
* Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika,
* 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, https, syslog,
* Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia,
* Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;

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

24. Przewód konsolowy USB-RJ45 do zarządzania urządzeniem

25. Urządzenie objęte gwarancją i wsparciem technicznym producenta przez minimum 12 miesięcy od dnia podpisania protokołu odbioru dostawy.

\*Uwaga, wymagane jest uzupełnienie tabeli

**Zadanie 3**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** | **\*** |
| **Producent:** | **\*** |
| **Typ/model/kod producenta:** | **\*** |
| **Przełącznik 24 porty GE – L3 z licencjami – typ 2 – 4 szt.** | |

1. 24 porty 10/100/1000BaseT RJ-45 + uplink 4x1G SFP

3. Porty SFP możliwe do obsadzenia następującymi rodzajami wkładek:

3.1 Gigabit Ethernet 1000Base-T,

3.2 Gigabit Ethernet 1000Base-SX,

3.3 Gigabit Ethernet 1000Base-LX/LH,

3.4 Gigabit Ethernet 1000Base-EX,

3.5 Gigabit Ethernet 1000Base-ZX,

3.6 Gigabit Ethernet 1000Base-BX-D/U

4. Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności:

* 1. Przepustowość w ramach stosu - 320Gb/s,
  2. 8 urządzeń w stosie,
  3. Zarządzanie poprzez jeden adres IP,
  4. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad,
  5. Wsparcie dla mechanizmu Stateful Switchover (SSO) dla urządzeń połączonych w stos, który polega na ustanowieniu jednego z urządzeń w stosie jako urządzenia aktywnego (active) a drugiego jako urządzenia zapasowego (standby) wraz z pełną synchronizacją informacji pomiędzy tymi urządzeniami w celu zminimalizowania przerwy podczas przełączania ruchu (dla protokołów warstwy 2),

5. Zasilanie i chłodzenie:

* 1. Redundantne i wymienne moduły wentylatorów,
  2. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap),
  3. Przełącznik wspierający IEEE 802.3az EEE (redukcja zużycia energii dla portów w stanie bezczynności),

6. Parametry wydajnościowe:

6.1 Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów - również dla pakietów 64-bajtowych (przełącznik line-rate):

· Przepustowość przełącznika (switching capacity):

56 Gb/s (bez podłączenia do stosu), 376 Gb/s (z podłączeniem do stosu)

· Prędkość przesyłania (forwarding rate):

41.66 Mpps (bez podłączenia do stosu), 279.76 Mpps (z podłączeniem do stosu)

6.2 Bufor pakietów – 16MB

6.3 Pamięć DRAM – 8GB

6.4 Pamięć flash – 16GB

6.5 Obsługa:

· 1000 aktywnych sieci VLAN

· 32000 adresów MAC

· 8000 tras IPv4

· 4000 tras IPv6

· Ilość wpisów w listach kontroli dostępu Security ACL – 5000

· ilość wpisów w listach kontroli dostępu QoS ACL – 5000

· 1000 interfejsów SVI L3

· 128 interfejsów L3

· Jumbo frame 9198B

· 128 połączeń zagregowanych typu „port channel”

· 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP

7. Obsługa protokołu NTP

8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

9. Przełącznik wspierający następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

* 1. IEEE 802.1w Rapid Spanning Tree
  2. Per-VLAN Rapid Spanning Tree (PVRST+)
  3. IEEE 802.1s Multi-Instance Spanning Tree
  4. Obsługa 128 instancji protokołu STP
  5. Wsparcie dla protokołu REP (Resilient Ethernet Protocol)
  6. Redundancja połączeń uplink bez używania protokołu spanning-tree lub funkcji portchannel umożliwiająca aktywację zapasowego łącza uplink po wykryciu awarii łącza podstawowego wraz z możliwością wskazania, dla których sieci VLAN pierwszy uplink jest łączem podstawowym a drugi uplink zapasowym a dla których przypisanie jest odwrotne. Realizacja funkcji automatycznego powrotu do ustawień sprzed awarii (preempt) po przywrócenia aktywności liku podstawowego

10. Obsługa protokołu LLDP (IEEE 802.1ab) i LLDP-MED

11. Realizacja funkcji 802.1Q tunneling (QinQ) wraz z obsługą tzw. selektywnego QinQ polegającego na możliwości zamapowania jednego lub kilku klienckich VLAN ID (C-VLAN ID) do VLAN ID (S-VLAN IS) używanego w sieci transportowej (operatora usługi QinQ)

12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

13. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

14. Możliwość uruchomienia funkcji serwera DHCP

15. Mechanizmy związane z bezpieczeństwem sieci:

15.1 Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwiający zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level),

15.2 Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,

15.3 Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,

15.4 Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,

15.5 Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,

15.6 Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,

15.7 Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,

15.8 Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,

15.9 Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),

15.10 Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,

15.11 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),

15.12 Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,

15.13 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);

15.14 Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch) kluczami o długości 128-bitów (gcm-aes-128),

15.15 Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing),

15.16 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). Realizacja dynamicznych sieci prywatnych VLAN tj. możliwość przypisania portu przełącznika do danej prywatnej sieci VLAN w wyniku uwierzytelnienia podłączonej stacji lub użytkownika w systemie RADIUS,

15.17 Obsługa RADSEC czyli Radius over TLS dla zabezpieczenia komunikacji Radius w sieci,

16. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

* 1. sprawdzanie autentyczności oprogramowania (w tym firmware, BIOS i system operacyjny urządzenia) przed uruchomieniem urządzenia,
  2. bezpieczna sekwencja uruchamiania,
  3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

17. Mechanizmy związane z zapewnieniem jakości usług w sieci:

* 1. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
  2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
  3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
  4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
  5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting),
  6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
  7. 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. Obsługa protokołów i mechanizmów routingu:

* 1. Routing statyczny dla IPv4 i IPv6,
  2. Routing dynamiczny – RIP, OSPF do 1000 routes PIM Stub do 1000 routes
  3. Policy-based routing (PBR),
  4. Obsługa protokołu redundancji bramy (VRRP) z obsługą 256 grup,
  5. Obsługa 10 tuneli GRE (Generic Routing Encapsulation);

19. Przełącznik umożliwiający 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,

20. Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

21. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),

22. Funkcjonalność sondy IP SLA Responder,

23. Wsparcie dla protokołu OpenFlow 1.3

24. Funkcjonalność Time Domain Reflectometer (TDR) umożliwiająca wykonanie testu kabla UTP podłączonego do portu miedzianego GigabitEthernet (1Gb/s) oraz wykrycie uszkodzonej pary,

25. Zarządzanie

* 1. Port konsoli,
  2. Dedykowany port Ethernet do zarządzania out-of-band,
  3. 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 umożliwiający kontrolę dostępu do konsoli poprzez mechanizm lokalnego konta logowania lub mechanizm AAA,
  4. 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,
  5. Obsługa protokołów SNMPv3, SSHv2, SCP, sftp (SSH File Transfer Protocol), https, syslog,
  6. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów,
  7. Wsparcie dla protokoły RESTCONF,
  8. Wsparcie dla protokołu gNMI,
  9. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych,
  10. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą,
  11. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB;
  12. Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci klucza USB 3.0 o pojemności 240GB;
  13. 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,
  14. Wbudowany graficzny interfejs zarządzania przełącznikiem umożliwiający:

a. Monitoring pracy przełącznika w zakresie:

A. Użycie CPU, użycie pamięci, temperatura pracy,

B. Podstawowe informacje systemowe: nazwa urządzenia, rodzaj sprzętu, czas pracy, czas systemowy, wersja oprogramowania, data i czas ostatniej zmiany konfiguracji, numer seryjny,

C. Obraz wykorzystania poszczególnych portów w zakresie: aktywny / nieaktywny, prędkość pracy,

D. Informacji o urządzeniach sąsiednich podłączonych do przełącznika (w tym nazwa sąsiada, lokalny port przez który jest podłączony sąsiad, zdalny port przy pomocy którego łączy się do przełącznika sąsiad, typ urządzania sąsiada np. przełącznik, router)

E. Statystyki ruchu (Rx/Tx) na poszczególnych portach L2 oraz informacja o typie portu (trunk, access) oraz przypisanej sieci VLAN, liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,

F. Statystyki ruchu (Rx/Tx) na poszczególnych portach L3 (SVI, vlan), liczniki błędów oraz informacja o dacie ostatniego restartu liczników, liczniki ruchu braodcast oraz multicast,

G. Informacje o ruchu aplikacyjnym przesyłanym przez przełącznik,

H. Protokół REP (Resilient Ethernet Protocol),

I. Protokół STP (Spanning Tree Protocol),

J. Lista klientów, którzy uzyskali adres IP poprzez protokół DHCP z serwera DHCP uruchomionego w przełączniku (w tym informacja o adresie IP, identyfikatorze klienta, czasie wygaśnięcia dzierżawy),

b. Konfigurację przełącznika w zakresie:

A. Konfiguracja interfejsów:

· Fizycznych:

- opis interfejsu, prędkość, tryb racy HDX/FDX/auto, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,

- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, parametry protokołu DHCP Relay (adres IP serwera DHCP),

- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN, ograniczenie ilości adresów MAC które mogą być obsługiwane na porcie, statyczne przypisanie adresów MAC do portu (statyczna wpisy do tablicy MAC przełącznika), konfiguracja 802.1x,

- przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

· Logicznych typu „port channel”:

- opis interfejsu, status administracyjny (włączony / wyłączony), włączenie lub wyłączenie trybu L2/L3,

- w trybie L3: sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska,

- w trybie L2: typ dostępowy lub trunk, przypisana sieć VLAN dla portu dostępowego, natywna sieć VLAN,

- przypisanie listy kontroli dostępu w kierunku „do” oraz „z” urządzenia, przypisanie polityki QoS, konfiguracja poziomów dla kontroli sztormów braodcastowych, multicastowych i unicastowych)

· Wirtualnych typu SVI:

- opis interfejsu, status administracyjny (włączony / wyłączony), MTU, sposób przypisania adresu (statycznie lub dynamicznie), dla trybu statycznego adres IP / maska, przypisanie listy kontroli dostępu w kierunku „do” oraz „z”, parametry protokołu DHCP Relay (adres IP serwera DHCP)

· Tworzenie i konfiguracja sieci VLAN: ID, nazwa, stan aktywna/nieaktywna, aktywacja/dezaktywacja, IGMP Snooping, porty dostępowe należące do danej sieci VLAN,

· Przypisane do portów wzorców konfiguracyjnych zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, radiowy punkt dostępowy WiFi, stacja sieciowa, router itp.),

· Konfiguracja mechanizmów SPAN i RSPAN,

· Konfiguracja protokołu STP,

· Konfiguracja protokołu REP,

· Konfiguracja routingu statycznego i dynamicznego,

· Uruchamianie i konfiguracja protokołów RADIUS i TACAS oraz uruchomienie i konfiguracja uwierzytelnienia dla poszczególnych portów,

· Tworzenie i przypisanie list kontroli dostępu ACL,

· Konfiguracja mechanizmów rozpoznawania i analizy ruchu aplikacyjnego,

· Konfiguracja i uruchomienie NetFlow,

· Konfiguracja polityk QoS,

· Administracja przełącznika w zakresie:

· Zdalne uruchamianie komend linii poleceń,

· Nazwa przełącznika,

· Tryb pracy L2/L3,

· Adres IP przełącznika do celów zarządzania zdalnego,

· Konfiguracja serwera DHCP,

· Konfiguracja DNS,

· Czas systemowy w tym protokół NTP,

· Konta administracyjne,

· Upgrade oprogramowania,

· Backup konfiguracji,

· Zdalny restart urządzenia,

· Konfiguracja i dostęp przez SNMP,

· Diagnostyka urządzenia:

· Narzędzie PING i TRACEROUTE,

· Przeglądanie logów systemowych,

· Przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego,

26. Parametry fizyczne:

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

27. Możliwość próbkowania (bez samplowania) i eksportu statystyk ruchu do zewnętrznych kolektorów danych ze wsparciem sprzętowym dla protokołu NetFlow – obsługa 64000 strumieni (flow),

28. 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,

29. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie,

30. Izolowane środowisko oparte o Linuxa (GuestShell) dostępne bezpośrednio na przełączniku z możliwością tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku,

31. Wsparcie dla protokołu LISP zgodnie z RFC 6830,

32. Urządzenie realizuje następujące funkcjonalności z zakresu MPLS:

* 1. L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 256 połączeń wirtualnych VC,
  2. L2VPN - Virtual Private LAN Services (VPLS) - obsługa 128 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji,
  3. L3 VPN - MPLS Virtual Private Network (VPN) – obsługa 7000 tras routingowych L3 VPN,
  4. Multicast VPN (MVPN),
  5. Inter AS Option A i B,
  6. EoMPLS wraz z obsługa MACSec (MACsec over EoMPLS),
  7. MPLS over GRE,
  8. MPLS Traffic Engineering

33. Obsługa 256 wirtualnych instancji routingu (VRF),

34. Obsługa zaawansowanych protokołów routingu

* 1. IS-IS i BGP dla IPv4 i IPv6,
  2. OSPF,
  3. EIGRP (rfc7868),
  4. Routing multicastów - PIM-SM, PIM-SSM, PIM-Bidir,
  5. Multicast Source Discovery Protocol (MSDP),

35. Obsługa protokołu BFD (Bidirectional Forwarding Detection) umożliwiającego szybkie wykrywanie awarii połączeń w sieci dla potrzeb protokołów routingu, obsługa 100 sesji BFD,

36. Realizacja funkcjonalności translacji adresów IP NAT (Network Address Translation) z obsługą do 5000 translacji,

37. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) kluczami o długości 256-bitów (gcm-aes-256). Wsparcie dla uruchomienia MACsec na portach tworzących połączenia zaagregowane L2 i L3,

38. Możliwość enkapsulacji ruchu w pakiety VXLAN,

39. Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów Edge/VTEP,

40. Możliwość tworzenia bezpośrednio na przełączniku polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) z możliwością przypisywania znaczników:

* 1. Statycznie w oparciu o port do którego podłączona jest stacja,
  2. Statycznie w oparciu o VLAN, w którym pracuje stacja,
  3. Statycznie w oparciu o adres IP stacji,
  4. Dynamicznie w oparciu o autoryzację użytkownika / stacji przy pomocy 802.1X;

41. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,

42. 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,

43. 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,

44. Wsparcie dla mechanizmu NonStop Forwarding (NSF), działającego w oparciu o mechanizm SSO, w celu zminimalizowania przerw w transmisji ruchu (dla protokołów warstwy 3) w trakcie awarii,

45. Funkcjonalność bramy dla usług mDNS,

46. 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),

47. Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7),

48. Możliwość eksportu dodatkowych pół w ramach statystyk NetFlow – w tym IDP (Initial Data Packet) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa),

49. Wbudowany analizator pakietów,

50. System operacyjny umożliwiający wgrywanie poprawek bez konieczności restartowania platformy,

51. Możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 50 AP oraz 1000 klientów bezprzewodowych w sieci SDN Network Fabric. Wykorzystanie przełącznika jako kontrolera WiFi wymaga dodatowych licencji do obsługi AP, które nie są wymagane do dostarczenia,

52. Urządzenie umożliwiający uruchamianie dodatkowych aplikacji w kontenerach Docker,

53. Integracja z zewnętrzną usługą bezpieczeństwa polegającą na przechwytywaniu i sprawdzaniu zapytań DNS (DNS Query) przesyłanych przez przełącznik pod kątem bezpieczeństwa i reputacji domen, o które kierowane są zapytania,

54. Wsparcie dla IEEE 802.1BA Audio Video Bridging (AVB).

55. Wyposażenie urządzenia:

* Urządzenie powinno być wyposażone w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat
* Przewód konsolowy USB-RJ45 do zarządzania urządzeniem
* Urządzenie objęte gwarancją i wsparciem technicznym producenta przez okres minimum 12 miesięcy od dnia podpisania protokołu odbioru dostawy.

\*UWAGA, wymagane jest uzupełnienie tabeli

**Zadanie 4**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** | **\*** |
| **Producent:** | **\*** |
| **Typ/model/kod producenta:** | **\*** |
| **Router z licencjami i akcesoriami - terminal serwer typ 2 – 1 szt.** | |

1. **Przedmiot zamówienia**

Przedmiotem zamówienia jest:

* 1. Dostawa 1 urządzenia, obejmująca sprzedaż̇ i dostarczenie przez Wykonawcę̨ do Lokalizacji Zamawiającego Urządzeń wraz z dokumentacją i Oprogramowaniem;
  2. Urządzenia będą̨ objęte wsparciem technicznym na Oprogramowanie przez okres 36 miesięcy od dnia podpisania protokołu odbioru dostawy.

1. **Wymagania Ogólne**
   1. Wykonawca wraz z Urządzeniami dostarczy zestaw montażowy rack tj. wszystkie niezbędne elementy konieczne do ich montażu w Lokalizacjach Zamawiającego, w szczególności: śrubki, nakrętki koszykowe, kable zasilające, szyny montażowe, itp.
   2. Urządzenia muszą pochodzić od tego samego producenta oraz być fabrycznie nowe, aktualnie obecne w linii produktowej producenta i jednocześnie nie mogą̨ znajdować się̨ na liście „end- of-sale”, „end-of-life” oraz „end-of-support” producenta.
   3. Urządzenia muszą posiadać najnowszą dostępną stabilną wersję Oprogramowania.
   4. Nie dopuszcza się oferowania urządzeń, dla których producent nie udostępnia już najnowszej wersji oprogramowania / systemu operacyjnego.
2. **Szczegółowe wymagania dla każdego z Urządzeń**
   1. Musi posiadać co najmniej 4 interfejsów 1GE, z czego dwa powinny umożliwiać wykorzystanie wkładki optycznej SFP. Jeśli oferowane urządzenie posiada 4 wbudowane porty RJ-45, wymagane jest doposażenie o dodatkowy moduł z 2 portami optycznymi SFP.
   2. Urządzenie musi umożliwiać rozszerzenie o moduł łączności poprzez sieć komórkową przynajmniej w standardzie LTE kategorii 6. Moduł powinien pozwalać na przełączania między co najmniej dwoma różnymi operatorami sieci komórkowej.
   3. Komponent sprzętowy zawierający sprzętowy certyfikat X.509v3 oraz łańcuch zaufania, pozwalający realizować bezpieczne uwierzytelnienie urządzenia – w tym również proces automatycznego i bezpiecznie uwierzytelnionego dodania urządzenia do sieci bez konieczności wpisywania haseł jednorazowych, ani logowania się do urządzenia za pomocą WifI, linii poleceń.
   4. Urządzenie musi mieć możliwość rozszerzenia funkcjonalności o porty telefonii analogowej FXS do podłączania telefonów jako wbudowane w urządzenie lub w ramach modułów rozszerzenia. Oczekuje się możliwości rozszerzenia o minimum 4 porty FXS.
   5. Urządzenie musi mieć możliwość rozszerzenia o obsługę transkodowania strumieni głosowych przynajmniej dla 200 kanałów z sesjami G.711.
   6. Musi być wyposażone w identyfikator RFID i mieć możliwość umieszczenia etykiety z kodem QR.
   7. Musi być wyposażone w co najmniej 4 GB pamięci RAM.
   8. Musi umożliwiać na rozbudowę pamięci RAM do co najmniej 32GB RAM.
   9. Musi być wyposażone w pamięć o pojemności co najmniej 8 GB do przechowywania obrazów systemu operacyjnego, konfiguracji oraz logów systemowych. Musi umożliwiać na rozbudowę pamięci do co najmniej 32GB.
   10. Musi obsługiwać co najmniej 800 000 prefiksów w tablicach routingu IPv4/IPv6 i umożliwiać na rozbudowę przez odpowiednie moduły – do co najmniej 2 500 000 prefiksów IPv4/IPv6.
   11. Musi oferować sumaryczną wydajność dla pakietów 1400B na poziomie przynajmniej 3Gbps dla ruchu IPv4;
   12. Musi oferować sumaryczną wydajność dla pakietów szyfrowanych 1400B na poziomie przynajmniej 500 Mbps dla ruchu IPv4;
   13. Musi być przystosowane do montażu w szafie 19”, obudowa wykonana z metalu;
   14. Musi posiadać zasilacz przystosowany do zasilania prądem naprzemiennym 230V.
3. **Funkcje Oprogramowania**
   1. Musi obsługiwać routing dynamiczny: RIP, OSPF, ISIS, EIGRP, BGP dla IPv4 i IPv6;
   2. Urządzenie mieć możliwość rozszerzenia funkcjonalności o wsparcie dla MPLS i MPLS VPN (L2: VPLS, VPWS i L3: VPNv4, VPNv6, mVPN);
   3. Musi być w stanie obsłużyć co najmniej 1000 instancji VRF (Virtual Route Forwarding);
   4. Urządzenie mieć możliwość rozszerzenia funkcjonalności o podłączenia wewnętrznym logicznym interfejsem wirtualny router (VRF) z globalną tablicą routingu.
   5. Musi posiadać ochronę̨ warstwy zarządzającej (Control Plane Policing);
   6. Musi obsługiwać conajmniej 4000 ACL (Access Control Lists) z 20 000 wpisów ACE (Access Control Entries);
   7. Musi wspierać multicast w szczególności: PIM sparse/SSM/Bi-directional, IGMP, MLDv2;
   8. Musi obsługiwać RPF (Reverse Path Forwarding);
   9. Musi obsługiwać zarzadzanie ruchem (QoS):
      1. Minimum 16000 kolejek per system
      2. Hierarchiczne polityki QoS
      3. 3 poziomy hierarchii;
      4. dwie kolejki priorytetowe LLQ per polityka.
   10. Urządzenie mieć możliwość rozszerzenia funkcjonalności o możliwość definicji własnych sygnatur aplikacji, na bazie których nastąpi klasyfikacja ruchu do kolejki QoS.
   11. Musi obsługiwać funkcjonalność Sflow lub odpowiednik (J-Flow, NetFlow);
   12. Musi posiadać funkcjonalność VRRP lub odpowiednika;
   13. Musi umożliwiać zarzadzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3;
   14. Musi posiadać wsparcie dla systemów AAA (RADIUS, TACACS);
   15. Urządzenie musi posiadać możliwość pobrania konfiguracji do zewnętrznego komputera typu PC, w formie tekstowej. Konfiguracja po dokonaniu edycji poza urządzeniem może być ponownie zaimportowana do Urządzenia i uruchomiona;
   16. Urządzenie musi posiadać możliwość wyszukiwania fragmentów konfiguracji z linii poleceń Urządzenia, dzięki stosowaniu wyrażeń-filtrów;
   17. Urządzenie powinno wspierać standardy szyfrowania ruchu – IPSec z wykorzystaniem co najmniej AES-256 w trybie CBC lub GCM, HMAC-SHA1, ECDSA (256/384 bit), SHA-1 i SHA-2.
4. **Wyposażenia urządzenia:**
   1. Musi być wyposażony w licencję umożliwiającą skorzystanie z przepustowości
      1. 25/25Mbps (sumarycznie 50Mbps) dla ruchu szyfrowanego.
   2. Karta rozszerzeń na 16 połączeń asynchronicznych w komplecie z dwoma przewodami każdy zakończony wtykiem 8 x RJ45
   3. Przewód konsolowy USB-RJ45 do zarządzania urządzeniem
   4. Urządzenie objęte gwarancją i wsparciem technicznym producenta przez okres minimum 12 miesięcy od dnia podpisania protokołu odbioru dostawy.

\*Uwaga, wymagane jest uzupełnienie tabeli

**Zadanie 5**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** | **\*** |
| **Producent:** | **\*** |
| **Typ/model/kod producenta:** | **\*** |
| **Przełącznik 48 portów GE - L2 - typ 3 – 1 szt.** | |

1. Typ i liczba portów: 48 portów 10/100/1000BaseT RJ-45 + uplink 4x1G SFP

2. Porty SFP możliwe do obsadzenia następującymi rodzajami wkładek:

* Gigabit Ethernet 1000Base-SX,
* Gigabit Ethernet 1000Base-LX/LH,

3. Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi,

4. Zasilanie i chłodzenie:

* Urządzenie wyposażone jest w wbudowany zasilacz AC230V,

5. Parametry wydajnościowe:

* Przepustowość przełącznika (switching bandwidth):
  + 104 Gb/s (full duplex),
* Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3:
  + 77.38 Mpps,
* Pamięć DRAM – 512 MB
* Pamięć flash – 256 MB
* Wielkość bufora pakietów - 1.5 MB
* Obsługa:
* 256 aktywnych sieci VLAN
* 15000 adresów MAC
* 16 statycznych tras IPv4
* 16 statycznych tras IPv6
* 64 interfejsów SVI L3
* Obsługa MTU-L3 9198B
* Obsługa ramek Ethernet Jumbo 10240B
* 1024 grupy IGMP
* 6 połączeń zagregowanych typu „port channel”
* 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
* Ilość wpisów w listach kontroli dostępu Security ACL – 600
* ilość wpisów w listach kontroli dostępu QoS ACL – 600

7. Porty dostępowe przełącznika posiadające zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

8. Obsługa protokołu NTP

9. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping

10. Przełącznik wspierające 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 64 instancji protokołu STP

11. Obsługa protokołu LLDP i LLDP-MED

12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC

13. Urządzenie wspierające połączenia link aggregation zgodnie z IEEE 802.3ad

14. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego

15. Możliwość uruchomienia funkcji serwera DHCP

16. Mechanizmy związane z bezpieczeństwem sieci:

* 1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwiające zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
  2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
  3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
  4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
  5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
  6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
  7. Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication),
  8. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
  9. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
  10. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
  11. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
  12. Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP),
  13. Funkcja Private VLAN,

17. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:

* 1. sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
  2. bezpieczna sekwencja uruchamiania,
  3. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.

18. Mechanizmy związane z zapewnieniem jakości usług w sieci:

* 1. Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
  2. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
  3. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
  4. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
  5. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń,
  6. Kontrola sztormów dla ruchu broadcast/multicast/unicast,
  7. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;

19. Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6,

20. Przełącznik umożliwiające lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących,

21. Przełącznik posiadające wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),

22. Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow,

22. Zarządzanie:

* 1. Port konsoli,
  2. Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika,
  3. 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,
  4. Obsługa protokołów SNMPv3, SSHv2, https, syslog,
  5. Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia,
  6. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;

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

24. Przewód konsolowy USB-RJ45 do zarządzania urządzeniem

25. Urządzenie objęte gwarancją i wsparciem technicznym producenta przez okres minimum 12 miesięcy od dnia podpisania protokołu odbioru dostawy.

\*Uwaga, wymagane jest uzupełnienie tabeli

**Zadanie 6**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** | **\*** |
| **Producent:** | **\*** |
| **Typ/model/kod producenta:** | **\*** |
| **Firewalll z licencjami i systemem zarządzającym – 2 szt** | |

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall)
3. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band
4. Urządzenie jest zasilanie prądem przemiennym 230V
5. Możliwość montażu w szafie rack 19” (dołączone niezbędne elementy montażowe)
6. Urządzenie wyposażone w 8 wbudowanych portów GbE RJ45 w tym 2 porty PoE+
7. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – 60 interfejsów VLAN
8. Interfejsy fizyczne mogą pracować jak interfejsy przełącznika sieciowego ze sprzętowym wsparciem dla funkcjonalności L2
9. Urządzenie wyposażone w port USB 3.0
10. Wysokość urządzenia 1RU
11. Przepustowość urządzenia dla uruchomionych modułów firewall’a oraz kontroli aplikacji (AVC) na poziomie 650 Mbps dla pakietów wielkości 1024B
12. Urządzenie osiąga powyższe parametry wydajnościowe również wraz z uruchomionym silnikiem IPS.
13. 100 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawiania co najmniej 6 000 nowych połączeń na sekundę
14. Możliwość połączeń VPN do 75 urządzeń z maksymalną sumaryczną przepustowością 300 Mbps dla pakietów 1024B TCP
15. Przepustowość dekrypcji ruchu szyftowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048B) wynosi przynajmniej 150 Mbps
16. Urządzenie nie posiadające ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
17. Możliwość uruchomienia urządzenia w trybie firewall’a L2 oraz L3
18. Urządzenie obsługuje routing statyczny oraz dynamiczny: RIP, OSPF, OSPFv3, BGP
19. Możliwość monitorowania dostępności „next hop” w trasach statycznych i automatycznego wyłączania trasy, gdy jest niedostępny.
20. Urządzenie obsługujące ruch multicastowy oraz protokoły IGMP, PIM-SM oraz bidirectional PIM
21. Urządzenie posiadające możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory
22. Urządzenie obsługujące funkcjonalność Network Address Translation (NAT oraz PAT)
23. Urządzenie mogące pracować jako serwer DHCP lub DHCP relay oraz zapewnia usługę DDNS
24. Urządzenie może pracować w układzie wysokiej dostępności (HA) active/standby
25. Urządzanie zapewniające możliwość obsługi użytkowników zdalnych VPN (RA VPN)
26. Urządzenie zapewniające możliwość konfiguracji połączeń VPN typu Site-to-Site w następujących topologiach:
    1. Point to Point
    2. Hub and Spoke
    3. Full Mesh
27. Urządzenie zapewniające możliwość ograniczenia pasma w konkretnym kierunku – upload i download dla:
    1. Źródłowych i docelowych stref NGFW
    2. Źródłowych i docelowych adresów IP oraz portów
    3. Aplikacji
    4. Użytkowników
    5. URLi zdefiniowanych przez administratora
28. System posiadające możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System umożliwiający stworzenie kontekst z wykorzystaniem co najmniej poniższych parametrów:
    1. Wiedza o użytkownikach – uwierzytelnienie
    2. Wiedza o urządzeniach – pasywne skanowanie ruchu
    3. Wiedza o urządzeniach mobilnych, load balancerach, urządzeniach NAT
    4. Wiedza o aplikacjach wykorzystywanych po stronie klienta
29. System posiadający otwarte API dla współpracy z systemami zewnętrznymi
30. Rozwiązanie współpracujący z systemami SIEM
31. System posiada wbudowany moduł wykrywania aplikacji AVC, który zapewniający
    1. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji
    2. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług
    3. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach
32. Rozwiązanie umożliwiający integrację z chmurową konsolą korelacji informacji o zagrożeniach z różnych rozwiązań bezpieczeństwa tego samego producenta.
33. Urządzenie mogące być zarządzane lokalnie lub przez scentralizowaną konsolę zarządzającą
34. System umożliwiające zdefiniowanie różnych wartości czasu wygaśnięcia sesji dla takich protokołów jak: ARP, SIP, H.323, H225, ICMP, UDP oraz dla sesji translacji PAT i sesji pół-otwartych.
35. System umożliwiający zdefiniowanie następujących podstawowych zabezpieczeń dla połączeń:
    1. Randomizacja TCP sequence number
    2. Ograniczenie ilości wszystkich połączeń globalnie oraz do jednego hosta
    3. Ograniczenie ilości połączeń pół-otwartych globalnie oraz do jednego hosta
    4. Detekcja wygasłych połączeń, poprzez sprawdzanie czy dwie strony sesji są nadal aktywne
36. Urządzenie umożliwiające wybór następujących metod kompilacji reguł polityki dostępu w przypadku użycia obiektów (np. grupy adresów IP, portów):
    1. Rozłożenie jednej skonfigurowanej reguły na reguły szczegółowe będące wszystkimi możliwymi kombinacjami wszystkich elementów zawartych w obiektach w celu monitorowania każdej z tych reguł z osobna (np. ilość dopasowani połączeń hit-counts) kosztem większego wykorzystania pamięci
    2. Dopasowanie ruchu do głównej reguły na podstawie zdefiniowanych obiektów bez tworzenia wszystkich możliwych kombinacji obiektów w celu zmniejszenia wykorzystania pamięci przez szczegółowe reguły.
37. Urządzenie zapewnia możliwość przypisania do reguł czasu jej aktywności. Istnieje możliwość zdefiniowania czasu całkowitego oraz zaplanowania interwałów czasowych.

Wyposażenie:

* Licencja na okres 3 lata na URL filtering, AMP, IPS
* Licencja na system zarządzania na okres 3 lat
* Przewód konsolowy USB-RJ45 do zarządzania urządzeniem
* Urządzenie objęte gwarancją i wsparciem technicznym producenta przez okres minimum 12 miesięcy od dnia podpisania protokołu odbioru dostawy.

\*Uwaga, wymagane jest uzupełnienie tabeli

**Zadanie nr 7 – Szafa serwerowa typu RACK**

|  |  |  |
| --- | --- | --- |
| **Nazwa oferowanego urządzenia:** | | **\*** |
| **Producent:** | | **\*** |
| **Typ/model/kod producenta:** | | **\*** |
| **Szafa serwerowa – 1 szt.** | | |
| **parametr** | **wymagania** | |
| **Wysokość użytkowa** | 42U | |
| **Stopień szczelności IP** | 20 |  |
| **Rozbudowany system konfiguracji:** | możliwość zestawienia szaf w zespoły | |
| możliwość ustawiania szafy na stopkach, kółkach i cokołach | |
| doprowadzenie kabli do szafy możliwe z każdej strony | |
| **Maksymalny kąt otwarcia drzwi** | 180 stopni | |
| **Zakres dostawy** | * szkielet (płyta dolna, płyta górna, 4 słupy) * przód: drzwi perforowane typu "plaster miodu" z zamkiem trzypunktowym * osłony boczne pełne z zamkami jednopunktowymi * drzwi tylne: perforowane typu "plaster miodu" z zamkiem trzypunktowym * dwie pary belek nośnych STANDARD w rozstawie 19" * listwa i linki uziemienia * stopki regulacyjne * kółka skrętne z blokadą x2 * kółka skrętne bez blokady x2 * belki wzmacniające do kółek | |
| **Kolor** | RAL 9005 (czarny), malowanie farbą proszkową o grubej strukturze | |
| **Głębokość szafy** | gł. 1000 mm | |
| **Szerokość szafy** | szer. 800 mm | |
| **Wysokość całkowita** | wys. 1988 mm | |
| **Dopuszczalne obciążenie** | * stopki – nie mniej niż 1360 kg * kółka 300 - 500 kg * cokół nie mniej niż - 1360 kg | |
| **Inne** | * Wszystkie otwory w płycie górnej i dolnej szafy fabrycznie zakryte wyłamywanymi zaślepkami   Szafa dostarczona na kółkach | |
| **Wyposażenie dodatkowe** | Zarządzana (RJ45) listwa zasilająca 8 portowa RACK PDU, SWITCHED, 1U, 12A/208V, 10A/230V, (8)C13 z kompletem 8 przewodów zasilających C13/C14– 2 szt | |
| **Gwarancja producenta** | Minimum 24 miesiące |  |

**Zadanie 8**

|  |  |
| --- | --- |
| **Nazwa oferowanego urządzenia:** | **\*** |
| **Producent:** | **\*** |
| **Typ/model/kod producenta:** | **\*** |
| **System zdalnego dostępu z licencjami – 1 szt.** | |

**Specyfikacja techniczna**

Usługa oparta o chmurę i lokalnie wdrożone kontrolery, która pozwala na tworzenie rozbudowanych laboratoriów opartych o fizyczne i wirtualne urządzenia wraz z pełną obsługą zarządzania nimi za pośrednictwem aplikacji web.

W ten sposób przygotowane środowisko ma zostać wykorzystane zarówno w procesie dydaktycznym, jak i w przypadkach testowania nowych rozwiązań czy prowadzenia działań badawczo-rozwojowych.

Dostęp użytkowników do poszczególnych składowych systemu ma być realizowany zarówno w sposób swobodny w oparciu o ich rejestrację, jak i akcydentalny bazując na rozbudowanym mechanizmie generacji czasowych kluczy jednorazowych.

Rozwiązanie po stronie klienta korzystającego w sposób zdalny do zrealizowania pełnego dostępu w wykorzystaniem przeglądarki obsługującej HTML5.

Komunikacja do poszczególnych urządzeń w ramach laboratorium ma odbywać się z wykorzystaniem protokołów Telnet, SSH, RDP i RBF (VNC).

**Architektura**

Kompletne rozwiązanie musi składać się z szeregu elementów:

- instancji, zarówno fizycznych jak i wirtualnych maszyn

- urządzeń składających się na płaszczyznę kontrolną zbudowaną z użyciem managera opartego o aplikację webową

- kontrolerów realizujących dostęp do składowych laboratorium.

Płaszczyzna komunikacyjna musi składać się z webowej aplikacji klienckiej i obsługi komunikacji z poszczególnymi elementami laboratorium w ramach kontrolera.

Cała konfiguracja logiczna laboratorium musi być przechowywana po stronie menedżera. Zarówno równoważenie obciążenia jak i migracja pomiędzy kontrolerami musi być możliwa do zrealizowania w bezproblemowy sposób.

Kontroler w ramach sieci laboratoryjnej zajmującej się umożliwieniem dostępu do poszczególnych jego składników oraz wykonywaniem zadań związanych zarządzaniem nimi przekazanych z poziomu menedżera.

**Skalowalność**

System musi pozwalać na łatwe skalowanie rozwiązania i obsługę dowolnej liczby klientów. Maksymalna liczba obsługiwanych jednocześnie zestawów i urządzeń będących ich składowymi powinna być zależna od liczby wdrożonych kontrolerów i zasobów w ramach infrastruktury oraz wybranego poziomu licencji. W zależności od modelu licencyjnego powinno być możliwe łatwe dostosowywanie środowiska do swoich potrzeb. Licencja powinna ograniczać liczbę aktywnych jednocześnie urządzeń i zestawów, ale pozwalać na posiadanie szeregu gotowych konfiguracji aktualnie nieaktywnych.

W przypadku kontrolera możliwość jednoczesnej obsługi komunikacji z urządzeniami w ramach zestawu powinna zależna od użytego protokołu dostępowego i wariantu obsługi połączenia.

**Manager**

Manager musi być realizowany z wykorzystaniem aplikacji webowej uruchomionej w izolowanej instancji serwera web dedykowanego dla klienta, zapewniając pełną izolację obsługi. Manager musi mieć skojarzoną własną nazwę domenową, a dostęp do aplikacji powinien być realizowany tylko za pośrednictwem protokołu HTTPS.

Użytkownicy w ramach instancji managera muszą być zarządzani niezależnie przez administratora, a usługodawca powinien zapewnić backupy konfiguracji w cyklu dobowym oraz aktualizację oprogramowania do wersji najnowszej.

Użytkownik posiadający status administratora musi mieć, poza kompletną funkcjonalnością dostępną innym zarejestrowanym użytkownikom również możliwość zarządzania konfiguracjami laboratoriów.

Poza możliwością zarządzania licencjami, kontrolerami i użytkownikami musi być dostępny szereg opcji pozwalających na kształtowanie laboratorium i dostępu do niego na szereg sposobów.

**Laboratorium**

W logicznym modelu laboratorium musi być zbiorem przypisanych zestawów zawierających urządzenia. Z laboratorium związane jest najczęściej konkretne zadanie, które może być dostępne w postaci opisu w formacie *markdown* lub dołączonego dokumentu *pdf*.

**Zestaw**

Musi być logicznym zbiorem urządzeń. Każdy zestaw powinien móc zostać przypisany do jednego, lub kilku, laboratoriów. Rezerwacja zestawu mimo, że realizowana ze wskazaniem na konkretne laboratorium, przypisuje na wyłączność urządzenia w nim zawarte konkretnemu użytkownikowi. Dostęp do urządzeń może być konfigurowany na poziomie zestawu, podobnie jak lokalna nazwa inna niż standardowa nazwa urządzenia.

W ramach zestawu musi być możliwe stworzenie opisu połączeń, który posłuży do wygenerowania dynamicznie mapy zestawu w ramach laboratorium.

**Urządzenia**

Urządzenie musi być logiczną instancją, z którą skojarzona jest jego nazwa i klasa. Dla każdego urządzenia musi być możliwe skonfigurowanie dowolnej liczby globalnych dostępów w oparciu o protokoły Telnet, SSH, RDP i RBF włącznie ze zdefiniowaniem parametrów w postaci adresów oraz portów dla dostępu jak i autentykacji. Dostępy mogą być też definiowane lokalnie dla każdego z zestawów je zawierających.

**Klasy urządzeń**

Urządzenia powinny być skojarzone z klasami, co ułatwia ich wizualną identyfikację. Klasy powinny być dowolnie dodawane i modyfikowane, tak aby dostosować ich listę do faktycznych składników laboratorium.

**Uprawnienia użytkowników**

Użytkownicy mogą mieć nadane uprawnienia do korzystania z poszczególnych zestawów z poziomu zarządzania nimi jak i każdego zestawu osobno. Musi być też możliwe dodanie, lub usunięcie użytkownika z grona administratorów oraz reset hasła.

**Zarządzanie zasilaniem**

Menedżer za pośrednictwem kontrolera powinien móc w ramach sieci laboratoryjnej komunikować się z listwami zasilającymi w celu zmiany stanu poszczególnych gniazd.

**Kontroler**

Kontroler musi być stworzony i konfigurowany w oparciu o najnowszą dystrybucję Ubuntu LTS przy użyciu dedykowanej aplikacji. Ze względu na konfigurację laboratorium przechowywaną w ramach menedżera jego wdrożenie lub wymiana nie może wiązać się z żadnymi dodatkowymi operacjami poza przygotowaniem i rejestracją w systemie zarządzania.

Kontroler, ze względu na sposób jego wdrażania, musi być zarówno fizycznym serwerem, instancją działającą w ramach środowiska wirtualnego, czy też instancją w ramach chmury obliczeniowej operatora.

Kontroler, lub kontrolery, muszą pozwalać na dostęp do poszczególnych składowych zestawów za pośrednictwem protokołu obsługiwanego przez webową aplikację kliencką i bazującego na HTTP i/lub Websocket. Musi być możliwe włączenie na poziomie kontrolera mechanizmu obsługi protokołów dostępowych do urządzeń w postaci RFB, RDP, Telnet i SSH i korzystanie z niezależnych aplikacji klienckich. Komunikacja taka może być ograniczona czasowo poprzez rezerwację i dynamicznie zestawiana z poziomu managera.

Kontroler musi pozwalać na dostęp do urządzeń składających się na zestawy w ramach sieci prywatnej, której jest częścią bez konieczności realizacji żadnego zewnętrznego tłumaczenia adresów czy routingu. Dopuszczalne jest posiadanie na kontrolerze portu z adresem publicznym lub minimalnie, translacji na adres publiczny i port 443.

Scenariusz obsługi dostępu klienckiego do instancji maszyn z użyciem alternatywnych aplikacji może wymagać przypisanego adresu publicznego i braku filtrowania ruchu dla wszystkich portów.

**Aplikacja kliencka**

Zarówno klient jak i administrator systemu mogą korzystać z tego samego punktu logowania, którym jest dedykowana instancja serwera menedżera. W przypadku logowania użytkownika, który nie ma nadanego statusu administratora dostępna dla niego będzie tylko możliwość zapoznania się z laboratoriami w ofercie, zarezerwowanie dostępu do zestawów, które ma przypisane i połączenie z infrastrukturą laboratorium w ramach rezerwacji.

|  |  |  |
| --- | --- | --- |
| Składowa | Cecha |  |
| Licencja | Rozmiar | Licencja musi obejmować aktualizację oprogramowania managera, klienta i dostęp do nowych wersji oprogramowania kontrolera. Wymagane jest dostarczenie licencji na:  1 kontroler  16 aktywnych zestawów  128 aktywnych urządzeń  Wymagane wdrożenie, instalacja, przeszkolenie dwóch osób z zakresu obsługi systemu zdalnego dostępu z certyfikatem |
| Czas licencji | Licencja na 3 lata z możliwością przedłużenia licencji na analogiczny okres czasu. |
| Manager | Lokalizacja | Aplikacja web w chmurze publicznego operatora z dedykowaną nazwą domenową lub własną nazwą (wymagana własna konfiguracja serwerów DNS i ewentualna zmiana ich konfiguracji w przypadku modyfikacji adresu IP managera). |
| Protokół dostępu | HTTPS. Generacja i zarządzanie certyfikatem dla poddomeny po stronie operatora usługi. |
| Autentykacja | Za pośrednictwem identyfikatora i hasła. Możliwość włączenia autentykacji wieloskładnikowej. |
| Zakres działania | * Zarządzanie licencjami i obsługiwanymi kontrolerami, * Zarządzanie konfiguracją dla elementów składowych środowiska laboratorium sieciowego w postaci klas urządzeń, urządzeń, zestawów i laboratoriów, * Zarządzaniem dostępem do poszczególnych urządzeń, * Zarządzanie użytkownikami i ich prawami dostępu, * Monitorowanie i zarządzanie dostępem do laboratorium, * Generowanie kluczy jednorazowego dostępu do laboratorium dla użytkowników akcydentalnych, * Zarządzanie zasilaniem laboratorium, * Monitorowaniem działania kontrolerów. |
| Kontroler | Lokalizacja | Po stronie klienta.  Instancja działająca jako system w ramach maszyny fizycznej lub wirtualnej w ramach środowiska zwirtualizowanego lokalnego centrum danych lub chmury. |
| Protokół dostępu | HTTPS w ramach RestAPI w płaszczyźnie kontrolnej z poziomu managera.  HTTPS/Websock w ramach połączenia z poziomu maszyny klienckiej z przeglądarki, zarządzane poprzez manager.  RFB, RDP, Telnet i SSH w trybie dostępu z alternatywnego klienta zarządzanego przez manager (wymagane dodatkowe warunki spełnione przez konfigurację dostępu do kontrolera).  Opcjonalny dostęp poprzez SSH w celu konfiguracji i zarządzania.  HTTPS. Generacja i zarządzanie certyfikatem po stronie operatora usługi. |
| Autentykacja | Poza dostępem administracyjnym SSH możliwy tylko za pośrednictwem czasowych tokenów generowanych dla klienta i zarządzanych przez manager. |
| Zakres działania | Zapewnienie dostępu do składowych laboratorium sieciowego. |
| Klient | Lokalizacja | Aplikacja web w chmurze publicznego operatora z dedykowaną nazwą domenową lub własną nazwą (wymagana własna konfiguracja serwerów DNS i ewentualna zmiana ich konfiguracji w przypadku modyfikacji adresu IP managera). Adres zgodny z adresem managera. |
| Protokół dostępu | HTTPS. Generacja i zarządzanie certyfikatem po stronie operatora usługi. |
| Autentykacja | Za pośrednictwem identyfikatora i hasła. Możliwość włączenia autentykacji wieloskładnikowej.  Klucz jednorazowego dostępu. |
| Zakres działania | Możliwość przeglądania i rezerwacji dostępu do zestawów laboratoriów sieciowych zgodnie z nadanymi prawami dostępu lub parametrami skojarzonymi z kluczem jednorazowego dostępu.  Dostęp do urządzeń wirtualnych i fizycznych dostępnych w ramach zestawów z poziomu przeglądarki web.  Przekazanie parametrów dostępu w przypadku wdrożenia komunikacji z użyciem protokołów RFB, RDP, Telnet i SSH w trybie dostępu z alternatywnego (wymagane dodatkowe warunki spełnione przez konfigurację dostępu do kontrolera). |

\*Uwaga, wymagane jest uzupełnienie tabeli

Wykonawca zobowiązany jest do podania nazwy oferowanego urządzenia, producenta, typu/modelu /kodu producenta. Podane dane oraz uzupełniona kolumna pn: Parametry oferowane muszą pozwolić Zamawiającemu na jednoznaczną identyfikację oferowanego produktu.

Każdorazowo gdy Zamawiający używa nazwy własnej, certyfikatu, standardu lub normy należy przez to rozumieć treść danego parametru łącznie ze sformułowaniem 'lub równoważny".

**DOKUMENT NALEŻY PODPISAĆ KWALIFIKOWANYM PODPISEM ELEKTRONICZNYM.**