Załącznik nr 1

**Opis przedmiotu zamówienia – Dostawa, instalacja i konfiguracja sprzętu sieciowego w OKRL Poznań**

Spis treści

[1. Wymagania ogólne [Sprzęt, licencje, wsparcie techniczne producenta] 3](#_Toc76542898)

[2. Wymagania instalacji i uruchomienia [instalacja, konfiguracja] 5](#_Toc76542899)

[3. Wymagania w zakresie świadczenia usług wsparcia 6](#_Toc76542900)

[4. Podział projektu na etapy 7](#_Toc76542901)

[5. Wykaz urządzeń 7](#_Toc76542902)

[6. Wykaz komponentów 8](#_Toc76542903)

[7. LF1G - Urządzenie typu leaf 1G z portami dostępowymi 48x 1000BASE-T 11](#_Toc76542904)

[8. LF25G - Urządzenie typu leaf z portami dostępowymi 48x 10/25G dla wkładek SFP+ 14](#_Toc76542905)

[9. SPLF - Urządzenie typu spine/leaf z portami 64x 40/100G 17](#_Toc76542906)

[10. FCZNA - Funkcjonalność komponentu zarządzającego i automatyzującego utrzymanie sieci 20](#_Toc76542907)

[10.1 Centralny Komponent Zarządzający 21](#_Toc76542908)

[10.2 Centralny System Analityczny 23](#_Toc76542909)

[11. FWVPN - Urządzenie klasy firewall umożliwiające koncentrację połączeń VPN 26](#_Toc76542910)

[12. RSKD - Rozbudowa systemu uwierzytelniania dostępu do sieci LAN/WLAN/VPN 33](#_Toc76542911)

[13. POBM – Przełącznik typ 1 45](#_Toc76542912)

[14. PAG – Przełącznik typ 2 48](#_Toc76542913)

[15. RTR - Router 53](#_Toc76542914)

[16. FWPA – Next Generation Firewall 57](#_Toc76542915)

# Wymagania ogólne [Sprzęt, licencje, wsparcie techniczne producenta]

1. Dostarczane urządzenia będą nowe i będą pochodzić z bieżącej produkcji, a jednocześnie nie będą urządzeniami, które mogły być używane w innych projektach i poddane procesowi odnowienia. Wymagane jest dostarczenie wraz ze sprzętem pisemnego potwierdzenia wydanego przez producenta lub przedstawicielstwo producenta sprzętu, poświadczającego datę produkcji sprzętu. Sprzęt musi być wyprodukowany nie wcześniej niż sześć miesięcy od daty podpisania umowy z dostawcą.
2. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający, że oprogramowanie zawarte w dostarczonym sprzęcie jest licencjonowane na Zamawiającego.
3. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający zarejestrowanie kontraktu serwisowego na dostarczone urządzenia i oprogramowanie. Serwis gwarancyjny musi obejmować prawo do aktualizacji wersji oprogramowania systemowego urządzeń. Wykonawca zapewni Zamawiającemu dostęp do:
   1. - nowych wersji oprogramowania
   2. - narzędzi konfiguracyjnych i dokumentacji technicznej
   3. - pomocy technicznej producentów
   4. - prawo bezpośredniego zgłaszania przez Zamawiającego usterek i awarii sprzętu do Producenta.
4. Ze względu na pożądaną pełną kompatybilność oraz zabezpieczenie uprawnień gwarancyjnych Zamawiającego, dostarczane w ramach Zamówienia rozwiązania (urządzenia oraz karty i moduły do nich) mają pochodzić od jednego producenta, chyba że wymagania szczegółowe stanowią inaczej. W przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia ich producentów o pełnej wzajemnej kompatybilności oraz oświadczenia o współpracy autoryzowanych placówek serwisowych producentów w zakresie usuwania problemów powstających na styku rozwiązań.
5. Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
6. Wykonawca na żądanie Zamawiającego będzie wykonywał w cyklu kwartalnym aktualizację oprogramowania systemowego (w ramach zakupionej przez Zamawiającego wersji funkcjonalnej) urządzeń wyspecyfikowanych w wykazie urządzeń w punkcie 3, w godzinach wskazanych przez Zamawiającego, w siedzibie Zamawiającego. W przypadku dokonania uaktualnienia oprogramowania przez Wykonawcę, Wykonawca zobowiązany będzie w terminie 14 dni do dostarczenia aktualnej licencji potwierdzonej przez producenta serwisowanego sprzętu lub jego oficjalnego przedstawiciela wystawionej na Zamawiającego.
7. Wszystkie wymagania przedstawione w niniejszym dokumencie muszą zostać spełnione w aktualnie dostępnych komercyjnie rozwiązaniach oprogramowania i sprzętu. Nie dopuszcza się możliwości, że wykonawca określi przyszłą wersję oprogramowania lub sprzętu, która będzie spełniać daną wyspecyfikowaną funkcjonalność.
8. Wymagane jest dostarczenie, wraz z dostawą urządzeń, szczegółowej dokumentacji technicznej producenta oferowanych produktów potwierdzającej spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia (Zamawiający dopuszcza w tym przypadku możliwość złożenia dokumentacji w języku angielskim).
9. W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:
10. - zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), oraz zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi
11. - inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych.
12. Jeżeli inspekcja, o której mowa powyżej wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 30% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Strony w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych.
13. Zamawiający wymaga wskazania numerów katalogowych urządzeń i oprogramowania (tzw. Part number), przy czym, przez numer katalogowy Zamawiający rozumie oznaczenie standardowo wykorzystywane przez producentów oferowanych urządzeń występujących w oficjalnych cennikach i katalogach produktów, określające skonkretyzowane urządzenie, pozwalające ustalić jego konfiguracje oraz cenę katalogową. Zamawiający nie dopuszcza posłużenia się „numerami katalogowymi“ stanowiącymi oznaczenie producenta zmodyfikowane przez Wykonawcę. W związku z tym Zamawiający wymaga na etapie składania ofert dostarczenia szczegółowej dokumentacji technicznej producenta oferowanych produktów potwierdzającej spełnianie wymagań technicznych urządzeń oraz oprogramowania będących przedmiotem zamówienia (Zamawiający dopuszcza w tym przypadku możliwość złożenia dokumentacji w języku angielskim).
14. Całość dostarczonego sprzętu oraz oprogramowania musi być objęta gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależne od statusu partnerskiego Wykonawcy.
15. Dostarczany sprzęt musi być objęty 48-miesięcznym (4 lata) serwisem liczonym:
    1. od dnia podpisania protokołu odbioru Etapu 1 potwierdzającego dostawę i wdrożenie dla tego etapu,
    2. oraz oddzielnie liczony od dnia odbioru Etapu 2 potwierdzającego dostawę i wdrożenie dla tego etapu.

Opartym na bezpośrednim serwisie producenta urządzenia świadczonym w reżimie 8x5xNBD (8h, 5 dni w tygodniu, naprawa w następnym dniu roboczym). Wraz z serwisem musi być dostarczony dostęp bezpośredni do stron producenta w celu pobrania najnowszego oprogramowania lub poprawek (ang. patch) do zaproponowanych urządzeń, zgłaszania problemów serwisowych oraz bezpośredni dostęp Zamawiającego do TAC (Technical Assistance Center) producenta urządzenia.

1. Wykonawca dostarczy w terminie do 30 dni od podpisania protokołu odbioru końcowego, dokument potwierdzający zarejestrowanie kontraktu serwisowego, wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela, w którym określone zostaną daty trwania serwisu oraz rodzaj serwisu.
2. Wszystkie wymagania przedstawione w Opisie Przedmiotu Zamówienia muszą zostać spełnione w aktualnie dostępnych komercyjnie rozwiązaniach Oprogramowania i Urządzeń. Nie dopuszcza się możliwości, że Wykonawca określi przyszłą wersję Oprogramowania lub Urządzeń, która będzie spełniać daną wyspecyfikowaną funkcjonalność. Dodatkowo wymaga się aby dostarczane Urządzenia posiadały stabilne wersje oprogramowania. Oznacza to, iż rozwiązanie (Urządzenie + oprogramowanie) musi być dostępne na rynku nie krócej niż 3 miesiące przed datą ogłoszenia postępowania przetargowego.

# Wymagania instalacji i uruchomienia [instalacja, konfiguracja]

1. Skierowanie przynajmniej jednego inżyniera producenta z najwyższym możliwym certyfikatem technicznym w dziedzinie network datacenter do uczestniczenia w konsultacjach technicznych i wdrożeniu w wymiarze pełnych 5 dni roboczych.
2. Opracowanie w konsultacji z Zamawiającym projektu technicznego wdrożenia obejmującego wszystkie elementy składowe w punkcie 4 & 5.
3. Fizyczna instalacja dostarczonego sprzętu w szafach rack
4. Podłączenie sprzętu do zasilania z najwyższą starannością i estetyką.
5. Wykonanie połączeń sieciowych z najwyższa starannością i estetyką
6. Skonfigurowanie i wdrożenie dostarczonego sprzętu zgodnie z projektem technicznym.
7. Wykonanie testów akceptacyjnych wdrożonego rozwiązania, potwierdzających poprawność działania mechanizmów wyspecyfikowanych w projekcie technicznym.
8. Opracowanie dokumentacji powykonawczej wdrożonego rozwiązania w języku polskim.

# Wymagania w zakresie świadczenia usług wsparcia przez Wykonawcę

1. Okres świadczenia usług wsparcia – 12 miesięcy od momentu skończenia wdrożenia
2. Niezależnie od serwisu gwarancyjnego u producenta, usługa serwisowa musi być świadczona przez Wykonawcę w miejscu instalacji sprzętu.
3. Serwis musi być świadczony na terenie Polski przez 24 godziny na dobę przez 7 dni w tygodniu. Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon, e-mail lub WWW.
4. Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań.
5. Zaproponowane pakiety serwisowe muszą zapewniać bezpośrednie zgłoszenie awarii sprzętu do producenta sprzętu (a nie tylko u Wykonawcy) przez cały okres trwania gwarancji.
6. Zamawiający w zaproponowanych pakietach serwisowych producenta musi otrzymać dostęp do pomocy technicznej Producenta (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań.
7. W okresie obowiązywania umowy Wykonawca dostarczy Zamawiającemu, przed upływem terminu ważności dokumentów opisanych powyżej, dokumenty wystawione na kolejne 12 miesięcy.
8. Miesięczny limit roboczogodzin dla usług wsparcia to 16 godzin, czas pracy rozliczany jest za każde rozpoczęte 30 minut.
9. Obsługa zgłoszonych Awarii i Usterek infrastruktury sieciowej wdrożonej wg opisu w punkcie 2., z czasem reakcji nie dłuższym niż 4 godziny w przypadku Awarii i 8 godzin w przypadku Usterki, przy czym:
   1. Awaria - pojęcie oznacza nieprawidłowe działanie infrastruktury IT, powodujące wstrzymanie działania systemów IT i/lub działalności produkcyjnej Zamawiającego.
   2. Usterka - pojęcie oznacza nieprawidłowe działanie infrastruktury IT, nie powodujące wstrzymania działania systemów IT i/lub działalności produkcyjnej Zamawiającego (np. spowalniające pracę).
   3. Czas reakcji - pojęcie oznacza czas od zgłoszenia Awarii lub Usterki do rozpoczęcia działań Wykonawcy zmierzających do jej usunięcia.
   4. Usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zgłoszenia usterki (zgłoszenie musi nastąpić do godziny 15).
10. Przegląd logów systemowych na nadzorowanych urządzeniach/systemach.
11. Wprowadzanie zmian w konfiguracji nadzorowanych urządzeń i systemów, zgodnie z potrzebami Zamawiającego.
12. W terminie 3 miesięcy od wdrożenia, skierowanie przynajmniej jednego inżyniera producenta z najwyższym możliwym certyfikatem technicznym w dziedzinie network datacenter do uczestniczenia w 5 dniowym spotkaniu w stylu (Q- Question & A – Answer) zorganizowanym w biurze Zamawiającego.

# Podział projektu na etapy

1. Projekt zamówienia ze względu na wymagania zamawiającego jest podzielony na dwa etapy dostaw i wdrożenia, dla każdego etapu jak poniżej:
   1. **Etap 1** (dostawy i wdrożenia)
      1. Zakończenie etapu nie może nastąpić później niż do 31 Marca 2022r.
   2. **Etap 2** (dostawy i wdrożenia)
      1. Rozpoczęcie etapu nie może nastąpić wcześniej niż 1 Września 2022r.
      2. Zakończenie etapu nie może nastąpić wcześniej niż 2 Stycznia 2023r.
      3. Zakończenie etapu nie może nastąpić później niż do 15 Stycznia 2023r.
2. Zakończenie projektu dla każdego z etapów rozumiane jest jako dostarczenie sprzętu (Punkt 1), wdrożenie i konfiguracja (Punkt2) oraz rozpoczęcie usług wsparcia (Punkt 3).

# Wykaz urządzeń

Nazwy skrótowe urządzeń w kolumnie pierwszej na potrzeby opisu zamówienia.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nazwa** | **Opis** | **Liczba Sztuk [Etap 1]** | **Liczba Sztuk [Etap 2]** | | **Suma [Etap1 + Etap2]** |
| LF1G | Urządzenie typu leaf 1G z portami dostępowymi  48x 1000BASE-T | 10 | 80 | | 90 |
| LF25G | Urządzenie typu leaf z portami dostępowymi 48x 10/25G dla wkładek SFP+ / SFP28 | 16 | 28 | | 44 |
| SPLF | Urządzenie typu spine/leaf z portami 64x 40/100G | 4 | 0 | | 4 |
| FCZNA | Funkcjonalność komponentu zarządzającego  i automatyzującego utrzymanie sieci | Zgodnie z opisem funkcjonalności | 0 | | Zgodnie z opisem funkcjonalności |
| FWVPN | Firewall/koncentrator VPN | 2 | 0 | | 2 |
| RSKD | Rozbudowa systemu uwierzytelnienia dostępu do sieci LAN/WLAN/VPN | Zgodnie z opisem | 0 | |  |
| POBM | Przełącznik typ 1 | 12 | 18 | | 30 |
| PAG | Przełącznik typ 2 | 4 | 0 | | 4 |
| RTR | Router typ 1 | 2 | 0 | | 2 |
| FWPA | Next Generation Firewall | 2 | 0 | 2 |

Tabela 1

Urządzenia wyposażone są w odpowiednie licencje zgodnie z opisem funkcjonalnościowym. Czas trwania niezbędnych licencji subskrypcyjnych oraz wsparcia producenta wynosi 48 miesięcy.

# Wykaz komponentów

|  |  |  |  |
| --- | --- | --- | --- |
| **Opis** | **Liczba Sztuk [Etap 1]** | **Liczba Sztuk [Etap 2]** | **Suma [Etap1 + Etap2]** |
| Aktywny kabel optyczny SFP28 o długości 10m, prędkość transmisji 25Gbps. Temperatura pracy 0 – 70 stopni Celsjusza. Moduł pochodzi od tego samego producenta co urządzenia LF1G i jest z nimi w pełni kompatybilny. | 20 | 160 | 180 |
| Moduł optyczny SFP28 SMF, prędkość transmisji 10/25Gbps o zasięgu pracy 10Km (G.652) zakończony konektorem LC. Temperatura pracy 0 – 70 stopni Celsjusza. Moduł pochodzi od tego samego producenta co urządzenia LF25G i jest z nimi w pełni kompatybilny. | 160 | 280 | 440 |
| Kabel DAC SFP28 o długości 3m, prędkości transmisji 25Gbps. Temperatura pracy 0 – 70 stopni Celsjusza. Kabel pochodzi od tego samego producenta co urządzenia LF25G i jest z nimi w pełni kompatybilny. | 96 | 168 | 264 |
| Aktywny kabel optyczny SFP28 o długości 5m, prędkość transmisji 25Gbps. Temperatura pracy 0 – 70 stopni Celsjusza. Kabel pochodzi od tego samego producenta co urządzenia LF25G i jest z nimi w pełni kompatybilny. | 256 | 448 | 704 |
| Aktywny kabel optyczny SFP28 o długości 10m, prędkość transmisji 25Gbps. Temperatura pracy 0 – 70 stopni Celsjusza. Kabel pochodzi od tego samego producenta co urządzenia LF25G i jest z nimi w pełni kompatybilny. | 256 | 448 | 704 |
| Moduł optyczny QSFP, prędkość transmisji 100Gb o zasięgu pracy 500m SMF (G.652) zakończony konektorem LC. Moduł ma możliwość pracy z modułem QSFP 40Gb przy użyciu specjalnych przewodów „breakout cables”. Moduł pochodzi od tego samego producenta co urządzenia SPLF i jest w z nimi w pełni kompatybilny. | 32 | 56 | 88 |
| Moduł optyczny QSFP, prędkość transmisji 100Gb o zasięgu pracy 500m SMF (G.652) zakończony konektorem LC. Moduł ma możliwość pracy z modułem QSFP 40Gb przy użyciu specjalnych przewodów „breakout cables”. Moduł pochodzi od tego samego producenta co urządzenia LF25G i jest w z nimi w pełni kompatybilny. | 32 | 56 | 88 |
| Moduł optyczny SFP+ SMF o prędkości transmisji 10Gbps i zasięgu pracy do 10km. Temperatura pracy 0 – 70 stopni Celsjusza. Moduł pochodzi od tego samego producenta co urządzenia FWVPN i jest z nimi w pełni kompatybilny. | 6 | 0 | 6 |
| Moduł optyczny SFP o prędkości transmisji 1Gbps i zasięgu pracy 550m dla włókna wielomodowego i 10km dla włókna jedno modowego. Temperatura pracy od -5 do 85 stopni Celsjusza. Moduł pochodzi od tego samego producenta co urządzenia POBM i jest z nimi w pełni kompatybilny. | 24 | 36 | 60 |
| Moduł optyczny SFP o prędkości transmisji 1Gbps i zasięgu pracy 550m dla włókna wielomodowego i 10km dla włókna jedno modowego. Temperatura pracy od -5 do 85 stopni Celsjusza. Moduł pochodzi od tego samego producenta co urządzenia PAG i jest z nimi w pełni kompatybilny. | 24 | 36 | 60 |
| Moduł optyczny QSFP, prędkość transmisji 100Gb o zasięgu pracy 500m SMF (G.652) zakończony konektorem LC. Moduł ma możliwość pracy z modułem QSFP 40Gb przy użyciu specjalnych przewodów „breakout cables”. Moduł pochodzi od tego samego producenta co urządzenia PAG i jest w z nimi w pełni kompatybilny. | 8 | 0 | 8 |
| Moduł optyczny SFP o prędkości transmisji 1Gbps i zasięgu pracy 550m dla włókna wielomodowego i 10km dla włókna jednmodowego. Temperatura pracy od -5 do 85 stopni Celsjusza. Moduł pochodzi od tego samego producenta co urządzenia RTR i jest z nimi w pełni kompatybilny. | 16 | 0 | 16 |
| Moduł optyczny SFP+ SMF o prędkości transmisji 10Gbps i zasięgu pracy do 10km. Temperatura pracy 0 – 70 stopni Celsjusza. Moduł pochodzi od tego samego producenta co urządzenia RTR i jest z nimi w pełni kompatybilny. | 16 | 0 | 16 |
| Kabel miedziany kategorii 6A lub wyższej nie-ekranowany o długości 10m | 40 | 0 | 40 |
| Kabel miedziany kategorii 6A lub wyższej nie-ekranowany o długości 5m | 40 | 0 | 40 |
| Kabel miedziany kategorii 6A lub wyższej nie-ekranowany o długości 3m | 80 | 0 | 80 |
| Kabel miedziany kategorii 6A lub wyższej nie-ekranowany o długości 2m | 80 | 0 | 80 |
| Kabel miedziany kategorii 6A lub wyższej nie-ekranowany o długości 1m | 80 | 0 | 80 |
| Kabel miedziany kategorii 6A lub wyższej nie-ekranowany o długości 0,5 m | 80 | 0 | 80 |
| Kabel miedziany kategorii 6A lub wyższej nie-ekranowany o długości 0,25 m | 80 | 0 | 80 |

Tabela 2

# LF1G **-** Urządzenie typu leaf 1G z portami dostępowymi 48x 1000BASE-T

1. Przełącznik posiada:
   1. 48 portów 1000BaseT
   2. 6 portów uplink, w tym min. 2 porty 40/100GE definiowane za pomocą wkładek QSFP28, przy czym każdy z tych portów QSFP28 posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode lub single-mode.
   3. Prędkość przełączania 696Gbps
   4. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
2. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
   1. Trunking IEEE 802.1Q VLAN;
   2. Wsparcie dla 3000 sieci VLAN;
   3. Wsparcie sprzętowe dla 90 tysięcy adresów MAC
   4. IEEE 802.1w Rapid Spanning Tree (RST)
   5. IEEE 802.1s Multiple Spanning Tree (MST)
   6. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
   7. Internet Group Management Protocol (IGMP) Versions 2, 3;
   8. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad
   10. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
   11. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   12. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
3. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
   1. Sprzętowe przełączanie pakietów w warstwie L3
   2. Routing w oparciu o trasy statyczne
   3. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
   4. Policy Based Routing (PBR)
   5. VRRP
   6. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6
   7. Wsparcie sprzętowe dla minimum 750tyś prefixów LPM oraz 750tyś wpisów hosta w tablicy routingu IP
   8. Wsparcie dla min. 200 VRF
   9. Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP)
   10. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
   11. Wsparcie dla IGMPv3 oraz MSDP
   12. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych
   13. Obsługa minimum 5000 wpisów dla ACL (access control list)
4. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   1. Zintegrowany, sprzętowy VXLAN Bridging/Routing
   2. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
   3. Implementacja VXLAN BGP EVPN (Ethernet VPN)
   4. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN)
5. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   1. Layer 2 IEEE 802.1p (CoS) oraz DSCP
   2. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6)
   3. Kolejkowanie bezwzględne (strict-priority)
   4. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)
   5. Ograniczanie ruchu (policing) do zadanej przepływności
   6. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
   8. Wsparcie dla RDMA, w tym RoCEv2
   9. Data Center Bridging Exchange Protocol – (DCBX)
   10. Explicit Congestion Notification – (ECN)
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   1. Obsługa list kontroli dostępu (ACL)
      1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
      2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
      3. ACL oparte o porty (PACL);
   2. DHCP Snooping
   3. ARP Inspection
   4. IP Source Guard
   5. Unicast reverse path forwarding (uRPF)
   6. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
   7. Sprzętowe wsparcie dla IEEE 802.1AE MacSec
7. Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   1. Port zarządzający 100/1000 Mbps;
   2. Port konsoli CLI;
   3. Zarządzanie In-band;
   4. SSHv2;
   5. Authentication, authorization, and accounting (AAA);
   6. RADIUS;
   7. TACACS+
   8. Syslog;
   9. SNMP v1, v2c, v3;
   10. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB.
   11. Role-Based Access Control RBAC;
   12. IEEE 802.1ab LLDP
   13. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   14. 802.1x
   15. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   16. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)
   17. Network Time Protocol (NTP);
   18. Precision Time Protocol IEEE 1588
   19. Diagnostyka procesu BOOT;
   20. Ping
   21. Traceroute
8. Narzędzia programowania i zarządzania przełącznikiem:
   1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
   2. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika
   3. Wsparcie dla kontenera LXC (Linux Container) lub Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika.
   4. Interfejs programistyczny REST API wraz z upublicznionym SDK
   5. Możliwość zainstalowania klienta Chef
   6. Możliwość zainstalowania agenta Puppet
   7. Wsparcie dla OpenStack Neutron plugin
9. Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych (kierunek „port side exhaust airflow”).
10. Obudowa o wymiarach 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
11. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem/oprogramowaniem zarządzającym. Przełącznik ma możliwość zmiany trybu pracy poprzez wymianę oprogramowania bez konieczności modyfikacji sprzętowej urządzeń.
12. Urządzenie współpracuje z systemem analityki w pełnym zakresie funkcjonalności opisywanych w punkcie „FCZNA - Funkcjonalność komponentu zarządzającego i automatyzującego utrzymanie sieci” podpunkt „Centralny System Analityczny”. Jeśli do zapewnienia opisywanej funkcjonalności niezbędne są dodatkowe licencje, należy je dostarczyć na okres 48 miesięcy.
13. Wyposażenie każdego przełącznika obejmuje:
14. 2 x aktywny kabel optyczny SFP28 o długości 10m, prędkość transmisji 25Gb.

# LF25G - Urządzenie typu leaf z portami dostępowymi 48x 10/25G dla wkładek SFP+

1. Przełącznik posiada:
   1. 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+/SFP28 wpierających kodowanie zgodnie z IEEE FC-FEC oraz RS-FEC.
   2. 6 portów 40/100GE definiowanych za pomocą wkładek QSFP28, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie100Gbps na pojedynczej parze okablowania multi-mode lub single mode.
2. Parametry wydajnościowe:
   1. Prędkość przełączania 3,6 Tbps
   2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
   1. Trunking IEEE 802.1Q VLAN;
   2. Wsparcie dla 3000 sieci VLAN;
   3. Wsparcie sprzętowe dla 90 tysięcy adresów MAC
   4. IEEE 802.1w Rapid Spanning Tree (RST)
   5. IEEE 802.1s Multiple Spanning Tree (MST)
   6. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
   7. Internet Group Management Protocol (IGMP) Versions 2, 3;
   8. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad
   10. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
   11. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   12. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
   1. Sprzętowe przełączanie pakietów w warstwie L3
   2. Routing w oparciu o trasy statyczne
   3. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
   4. Policy Based Routing (PBR)
   5. VRRP
   6. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6
   7. Wsparcie sprzętowe dla minimum 750tyś prefixów LPM oraz 750tyś wpisów hosta w tablicy routingu IP
   8. Wsparcie dla min. 200 VRF
   9. Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP)
   10. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
   11. Wsparcie dla IGMPv3 oraz MSDP
   12. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych
   13. Obsługa minimum 5000 wpisów dla ACL (access control list)
5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   1. Zintegrowany, sprzętowy VXLAN Bridging/Routing
   2. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
   3. Implementacja VXLAN BGP EVPN (Ethernet VPN)
   4. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN)
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   1. Layer 2 IEEE 802.1p (CoS) oraz DSCP
   2. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6)
   3. Kolejkowanie bezwzględne (strict-priority)
   4. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)
   5. Ograniczanie ruchu (policing) do zadanej przepływności
   6. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
   8. Wsparcie dla RDMA, w tym RoCEv2
   9. Data Center Bridging Exchange Protocol – (DCBX)
   10. Explicit Congestion Notification – (ECN)
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   1. Obsługa list kontroli dostępu (ACL)
      1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
      2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
      3. ACL oparte o porty (PACL);
   2. DHCP Snooping
   3. ARP Inspection
   4. IP Source Guard
   5. Unicast reverse path forwarding (uRPF)
   6. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
   7. Sprzętowe wsparcie dla IEEE 802.1AE MacSec
8. Przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
   1. Port zarządzający 100/1000 Mbps;
   2. Port konsoli CLI;
   3. Zarządzanie In-band;
   4. SSHv2;
   5. Authentication, authorization, and accounting (AAA);
   6. RADIUS;
   7. TACACS+
   8. Syslog;
   9. SNMP v1, v2c, v3;
   10. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB.
   11. Role-Based Access Control RBAC;
   12. IEEE 802.1ab LLDP
   13. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   14. 802.1x
   15. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   16. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)
   17. Network Time Protocol (NTP);
   18. Precision Time Protocol IEEE 1588
   19. Diagnostyka procesu BOOT;
   20. Ping
   21. Traceroute
9. Narzędzia programowania i zarządzania przełącznikiem:
   1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
   2. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika
   3. Wsparcie dla kontenera LXC (Linux Container) lub Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika.
   4. Interfejs programistyczny REST API wraz z upublicznionym SDK
   5. Możliwość zainstalowania klienta Chef
   6. Możliwość zainstalowania agenta Puppet
   7. Wsparcie dla OpenStack Neutron plugin
10. Przełącznik posiada możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów lub przełączników jest realizowane w ramach domeny fizycznej bądź stosu urządzeń (bez wykorzystania mechanizmów L2 lub L3). Porty modułu wyniesionego są udostępniane do zarządzania i monitorowania z poziomu przełącznika centralnego.
11. Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych (kierunek „port side exhaust airflow”).
12. Obudowa o wymiarach 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
13. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem/oprogramowaniem zarządzającym. Przełącznik ma możliwość zmiany trybu pracy poprzez wymianę oprogramowania bez konieczności modyfikacji sprzętowej urządzeń.
14. Urządzenie współpracuje z systemem analityki w pełnym zakresie funkcjonalności opisywanych w punkcie „FCZNA - Funkcjonalność komponentu zarządzającego i automatyzującego utrzymanie sieci” podpunkt „Centralny System Analityczny”. Jeśli do zapewnienia opisywanej funkcjonalności niezbędne są dodatkowe licencje, należy je dostarczyć na okres 48 miesięcy.
15. Wyposażenie każdego przełącznika obejmuje:
    1. 2 x moduł optyczny QSFP28 100Gb umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów jednomodowych (SM) o zasięgu pracy 500m SMF (G.652) zakończony konektorem LC
    2. 10 x moduł optyczny SFP28 wielomodowy MMF umożlwiający połączenie z wykorzystanie pojedynczej pary światłowodów MMF, prędkość transmisji 10/25Gbps o zasięgu pracy 300m (OM3) i 400m (OM4) zakończony konektorem LC.
    3. 6 x kabel DAC SFP28 o długości 3m, prędkości transmisji 25Gbps
    4. 16 x aktywny kabel optyczny SFP28 o długości 5m, prędkość transmisji 25Gbps
    5. 16 x aktywny kabel optyczny SFP28 o długości 10m, prędkość transmisji 25Gbps

# SPLF - Urządzenie typu spine/leaf z portami 64x 40/100G

1. Przełącznik posiada:
   1. min. 64 porty 40/100Gbps definiowane za pomocą wkładek QSFP28, przy czym każdy z tych portów posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m) lub single-mode. Dodatkowo wymagane jest wsparcie dla optyki SFP poprzez odpowiedni konwerter oraz breakout 2x50, 4x10, 4x25 na co najmniej połowie portów.
2. Parametry wydajnościowe:
   1. Prędkość przełączania 6.4Tbps full duplex
   2. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3
3. Przełącznik posiada następującą funkcjonalność dla warstwy L2:
   1. Trunking IEEE 802.1Q VLAN;
   2. Wsparcie dla 3000 sieci VLAN;
   3. Wsparcie sprzętowe dla 90 tysięcy adresów MAC
   4. IEEE 802.1w Rapid Spanning Tree (RST)
   5. IEEE 802.1s Multiple Spanning Tree (MST)
   6. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU)
   7. Internet Group Management Protocol (IGMP) Versions 2, 3;
   8. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach
   9. Link Aggregation Control Protocol (LACP): IEEE 802.3ad;
   10. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
   11. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN
   12. Wsparcie sprzętowe dla tunelowania QinQ i QinVNI
4. Przełącznik posiada następującą funkcjonalność dla warstwy L3:
   1. Sprzętowe przełączanie pakietów w warstwie L3
   2. Routing w oparciu o trasy statyczne
   3. Umożliwia rozbudowę poprzez licencje o funkcjonalności warstwy L3 – OSPF, BGP, IS-IS dla protokołów IPv4 oraz IPv6
   4. Policy Based Routing (PBR)
   5. VRRP
   6. Wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6
   7. Wsparcie sprzętowe dla minimum 750tyś prefixów LPM oraz 750tyś wpisów hosta w tablicy routingu IP
   8. Wsparcie dla min. 200 VRF
   9. Wybór do 32 jednoczesnych ścieżek o równej metryce (ECMP)
   10. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast)
   11. Wsparcie dla IGMPv3 oraz MSDP
   12. Wsparcie sprzętowe dla minimum 32 000 tras multicast
   13. Obsługa minimum 5000 wpisów dla ACL (access control list)
5. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
   1. Zintegrowany, sprzętowy VXLAN Bridging/Routing
   2. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast)
   3. Implementacja VXLAN BGP EVPN (Ethernet VPN)
   4. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN
6. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   1. Layer 2 IEEE 802.1p (CoS) oraz DSCP
   2. Klasyfikacja QoS w oparciu o listy ACL (Access control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6)
   3. Kolejkowanie bezwzględne (strict-priority)
   4. Kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection)
   5. Ograniczanie ruchu (policing) do zadanej przepływności
   6. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych
   7. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
   8. Wsparcie dla RDMA, w tym RoCEv2
   9. Data Center Bridging Exchange Protocol – (DCBX)
   10. Explicit Congestion Notification – (ECN)
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   1. Obsługa list kontroli dostępu (ACL)
      1. ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu;
      2. ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP);
      3. ACL oparte o porty (PACL);
   2. DHCP Snooping
   3. ARP Inspection
   4. IP Source Guard
   5. Unicast reverse path forwarding (uRPF)
   6. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
8. Urządzenie realizuje następujące funkcjonalności dotyczące zarządzania i zabezpieczenia:
   1. Port zarządzający 100/1000 Mbps;
   2. Port konsoli CLI;
   3. Zarządzanie In-band;
   4. SSHv2;
   5. Authentication, authorization, and accounting (AAA);
   6. RADIUS;
   7. TACACS
   8. Syslog;
   9. SNMP v1, v2, v3;
   10. Telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB.
   11. Role-Based Access Control RBAC;
   12. IEEE 802.1ab LLDP
   13. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback)
   14. 802.1x
   15. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing)
   16. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring)
   17. Network Time Protocol (NTP);
   18. Precision Time Protocol IEEE 1588
   19. Diagnostyka procesu BOOT;
   20. Ping
   21. Traceroute
9. Narzędzia programowania i zarzadzania przełącznikiem:
   1. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API
   2. Wbudowana powłoka Bash do zarządzania systemem Linux przełącznika
   3. Wsparcie dla kontenera LXC (Linux Container) lub Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika.
   4. Interfejs programistyczny REST API wraz z upublicznionym SDK
   5. Możliwość zainstalowania klienta Chef
   6. Możliwość zainstalowania agenta Puppet
10. Przełącznik jest wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych (kierunek „port side exhaust airflow”).
11. Obudowa o rozmiarach maksymalnie 2RU (rack unit), przeznaczona do montażu w szafie rackowej 19”.
12. Urządzenie ma możliwość pracy samodzielnej (realizując opisane powyżej funkcjonalności) oraz współpracy z komponentem/oprogramowaniem zarządzającym. Przełącznik ma możliwość zmiany trybu pracy poprzez wymianę oprogramowania bez konieczności modyfikacji sprzętowej urządzeń.
13. Wyposażenie każdego przełącznika obejmuje:
    1. 8 x moduł optyczny QSFP28 100Gb umożliwiające połączenie 100GE z wykorzystaniem pojedynczej pary światłowodów jednomodowych (SM) o zasięgu pracy 500m SMF (G.652) zakończony konektorem LC

# FCZNA - Funkcjonalność komponentu zarządzającego i automatyzującego utrzymanie sieci

Rozwiązanie składa się z redundantnych i uzupełniających się komponentów sprzętowych i programowych tworzących wspólną całość tj.:

* 1. **Centralnego Komponentu Zarządzającego** realizującego funkcjonalność zarządzania siecią fizyczną, wirtualną, kontenerową oraz warstwą logiczną i zapewniającego uruchamianie usług w oparciu o modelowanie polityk dla aplikacji.
  2. **Centralnego Systemu Analitycznego** wspierającego zarządzanie i diagnostykę, dbającego o poprawność implementacji polityk oraz zawierającego moduły audytu bezpieczeństwa.

## 10.1 Centralny Komponent Zarządzający

1. Zarządza infrastrukturą sieciową złożoną z przełączników 10/25/40/100 GigabitEthernet, zorganizowanych w dwustopniowej nieblokowalnej architekturze rdzeń-brzeg (spine-leaf) określanej jako „IP Fabric”.
2. Jest zrealizowany w oparciu o dedykowaną warstwę sprzętową i programową. Zasoby sprzętowe (CPU, pamięć, dyski, porty sieciowe) są w pełni dedykowane dla oprogramowania zarzadzającego.
3. Zrealizowany jest redundantnie (np. w formie klastra kilku instancji) zarówno w warstwie sprzętowej, jak i programowej tak, aby zapewnić spójne działanie środowiska i możliwość modyfikacji konfiguracji po ewentualnej utracie jednej z instancji.
4. Utrata wszystkich instancji klastra nie wpływa na działanie infrastruktury sieciowej w zakresie istniejącej konfiguracji (może wpływać na wprowadzanie do niej zmian).
5. Obsługuje wyłącznie ruch związany z zarządzaniem i monitorowaniem infrastruktury sieciowej (tzw. „control plane”), nie zajmuje się przełączaniem ruchu (tzw. „data plane”).
6. Umożliwia zarządzanie infrastrukturą sieciową złożoną z 2000 portów i dołączonych do niej 1000 fizycznych serwerów dwuprocesorowych w ramach dostarczanych licencji.
7. Umożliwia automatyzację konfiguracji zarządzanej sieci w oparciu o model sieciowych polityk grupowych powiązanych z aplikacjami.
8. Umożliwia wydzielanie izolowanych wirtualnych środowisk sieciowych wraz z dedykowanymi zespołami administratorów i prawami dostępu dla 100 takich środowisk (tzw. „multi-tenant”).
9. Dla izolowanych środowisk sieciowych umożliwia implementację funkcjonalności dedykowanej bramy wyjściowej L2/L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7.
10. Umożliwia tworzenie wirtualnych instancji sieciowych umożliwiających nakładanie się adresacji IP w wielu zaimplementowanych równocześnie instancjach (VRF) w liczbie 10 instancji VRF na wirtualne środowisko.
11. Umożliwia jednoczesne konfigurowanie sieci dla środowisk złożonych z:
    1. Serwerów fizycznych
    2. Serwerów wirtualnych realizowanych w oparciu o VMWare vSphere i VMware vCenter
    3. Serwerów wirtualnych realizowanych w oparciu o Microsoft HyperV
    4. Serwerów wirtualnych realizowanych w oparciu o RedHat KVM i OVS (Open vSwitch) w środowisku OpenStack
    5. Kontenerów wirtualnych realizowanych w oparciu o Kubernetes i Openshift
12. Umożliwia zintegrowanie usług zewnętrznych poprzez zapewnienie szczegółowej konfiguracji i mechanizmu przekierowania ruchu dla warstw 4-7 dla urządzeń Firewall i Loadbalancer posiadanych obecnie:
    1. Loadbalancer F5
    2. Firewall Cisco Firepower
    3. Firewall Palo Alto
13. Umożliwia wymianę informacji na temat segmentów bezpieczeństwa z posiadanym rozwiązaniem Cisco ISE (broker tożsamości).
14. Umożliwia monitorowanie i diagnostykę sieciową dla uruchamianych środowisk:
    1. Prezentację sprawności bieżącej i historycznej środowiska w formie SLA dla danego środowiska sieciowego oraz modelu polityk aplikacyjnych
    2. Prezentowanie bieżącej i historycznej statystyki ruchu dla danego środowiska sieciowego, zdefiniowanych warstw aplikacji oraz interfejsów fizycznych
    3. Pomiar ruchu na portach wejściowych i wyjściowych infrastruktury sieciowej dla środowisk uruchamianych w oparciu o model polityk aplikacyjnych
    4. Diagnostykę ścieżki (traceroute) między dowolną parą portów fizycznych bądź wirtualnych wchodzących w skład infrastruktury
    5. Monitorowanie i raportowanie ilości wykorzystanych i dostępnych zasobów wchodzących w skład infrastruktury
    6. Zbieranie, agregowanie i interpretowanie zdarzeń (events) i problemów (faults) w ramach infrastruktury sieciowej
    7. Monitorowanie ruchu poprzez kopiowanie (mirroring) ruchu dla wybranych warstw aplikacyjnych
15. Umożliwia automatyczną detekcję topologii oraz inwentarza infrastruktury sieciowej.
16. Implementuje centralne repozytorium oprogramowania (firmware) dla infrastruktury sieciowej.
17. Implementuje centralny mechanizm aktualizacji oprogramowania (firmware) dla infrastruktury sieciowej.
18. Umożliwia zachowywanie (snapshot) i odtwarzanie (rollback) dla całości konfiguracji infrastruktury sieciowej.
19. Udostępnia następujące interfejsy zarządzające:
    1. GUI (http/https)
    2. CLI (linia komend konsoli)
    3. Plugin dla OpenStack umożliwiający integrację na poziomie Neutron ML2
20. Udostępnia następujące mechanizmy programowania/API:
    1. REST API ze wsparciem dla formatu XML
    2. Możliwość konfiguracji infrastruktury bezpośrednio poprzez http, np. z wykorzystaniem Postman REST Client
    3. Python SDK
    4. Powszechnie dostępna dokumentacja dla REST API
21. Udostępnia autoryzację dostępu użytkowników w oparciu o mechanizmy:
    1. Lokalną definicję
    2. RADIUS
    3. TACACS+
    4. LDAP
22. Umożliwia synchronizację całej infrastruktury sieciowej w oparciu o protokół NTP.
23. Implementuje następujące protokoły i mechanizmy L2 na zarządzanej infrastrukturze sieciowej:
    1. Sprzętowe wsparcie dla VXLAN Bridging i VXLAN Routing w oparciu o sprzętowy VTEP
    2. Umożliwia tworzenie segmentów sieci L2 w oparciu o technologię VXLAN
    3. Definiowanie domen rozgłoszeniowych L2 z opcjonalną możliwością eliminacji ruchu rozgłoszeniowego dla mechanizmów ARP/GARP, Unknown Unicast
    4. Eliminacja ruchu rozgłoszeniowego dla mechanizmów ARP i Unknown Unicast poprzez lokalizację w oparciu o bazę adresową L2/L3
    5. Dołączanie urządzeń zewnętrznych (serwerów, modułów, przełączników) poprzez zagregowaną wiązkę połączeń LACP 802.3ad do dwóch przełączników brzegowych (multi link aggregation, virtual port channel, itp.)
    6. Pełna mobilność serwera fizycznego i wirtualnego w domenie L2
    7. Definiowanie zewnętrznych połączeń w domenie L2
    8. Mechanizm eliminacji pętli na przełącznikach brzegowych w fabric
24. Implementuje następujące protokoły i mechanizmy L3 na zarządzanej infrastrukturze sieciowej:
    1. IPv4 Unicast i Multicast;
    2. Przesyłanie IPv6 Unicast;
    3. Niezależne sieci prywatne (VRF) z duplikacją adresacji IP;
    4. Protokoły routingu eBGP, iBGP, OSPF dla IPv4 i IPv6;
    5. Routing statyczny dla IPv4 i IPv6;
    6. Przełączanie ruchu pomiędzy parą podsieci IP (SVI) realizowane sprzętowo w modelu IP Anycast w ramach fabric, tj. na każdym przełączniku brzegowym, niezależnie od ilości przełączników brzegowych w fabric;
    7. Pełna mobilność serwera fizycznego i wirtualnego w domenie L3;
    8. Interfejsy i subinterfejsy L3 (per VLAN) na portach fizycznych przełączników brzegowych;
    9. Definiowanie zewnętrznych połączeń w domenie L3;
25. Implementuje następujące mechanizmy optymalizacji ruchu: Load-balancing pakietów dostosowany do różnych warunków przesyłania (natłoku) w ramach środowiska i priorytetyzacja połączeń.
26. Umożliwia wyniesienie dowolnej pary urządzeń typu leaf do lokalizacji zdalnej przy zachowaniu przynależności do centralnej IP Fabric
27. Ze względu na istniejące okablowanie światłowodowe wymagana jest realizacja architektury IP Fabric trójwarstwowej Spine-Leaf-Leaf, w szczególności podłączenia urządzeń typu leaf LF1G do urządzeń LF25G.
28. Komunikacja pomiędzy oprogramowaniem zarządzającym a zarządzanymi urządzeniami sieciowymi odbywa się w sposób spójny dla wszystkich funkcjonalności (jeden protokół komunikacji) i w sposób zaszyfrowany.
29. Kompatybilność pomiędzy oprogramowaniem zarządzającym a urządzeniami sieciowymi jest potwierdzona dokumentacją producenta.

## 10.2 Centralny System Analityczny

1. Narzędzie lub zespół narzędzi analitycznych zawierających zestaw zaawansowanych algorytmów powiadamiania, ustalania wartości bazowych, korelacji i prognoz/trendów.
2. Narzędzie(a) mają zapewnić wgląd w zachowanie/stan sieci przy wykorzystaniu danych telemetrycznych z komponentów sieciowych i zarządzających.
3. Rozwiązanie ma pomagać w szybkim znajdowaniu przyczyn problemów, wspierać ich rozwiązywanie poprzez wizualizacje oraz rekomendacje w zakresie działań naprawczych. Wymagane jest wsparcie dla „IP Fabric” (topologii sieciowych spine-leaf).
4. Funkcjonalności w zakresie weryfikacji bieżącego stanu sieci( IP Fabric) z bazami online producenta:
   1. Analiza na bieżąco zdarzeń i logów celem identyfikacji znanych ostrzeżeń, ich wpływu na określone przełączniki urządzenia, oraz zalecenia dotyczące działań naprawczych,
   2. informacje o błędach, podatnościach (PSIRT/CVE), zaleceniach producenta, poprawkach, EOL / EOS oprogramowania i sprzętu,
   3. Anomalie w konfiguracji – informacje o przekroczeniu przez konfiguracje zweryfikowanej skali dla danego urządzenia i użytkowanej wersji oprogramowania,
   4. Informacje o problemach w procesie utwardzania (zabezpieczania) platformy, niezgodnościach w warstwie zarządzania
   5. Informacja o wpływie poprawek na dostępność systemu, np. czy aktualizacja oprogramowania będzie bezprzerwowa, czy (nowy) sprzęt może obsługiwać istniejący zestaw funkcji i skalę,
   6. Otwieranie zgłoszeń u producenta wraz ze wsparciem przygotowania i dostarczenia wymaganych logów,
   7. Wsparcie wysyłania powiadomień o powyższych problemach i rekomendacjach poprzez email i Kafka (szyna danych);
5. Analiza warstwy zarządzania (control plane) Fabryki IP z następującymi funkcjonalnościami:
   1. Zbieranie danych: zmiany konfiguracji, zdarzenia i błędy w warstwie zarządzania,
   2. Analiza celem określenia korelacji między wszystkimi zmianami, zdarzeniami i błędami,
   3. Wykrywanie anomalii: detekcja nieoczekiwanych zdarzeń, w tym tych mających wpływ na przestoje;
   4. Analiza protokołów multicast i ich stanu (PIM/IGMP oraz IGMP snooping)
   5. Co najmniej 30 dniowa retencja danych;
6. Wizualizacja wykorzystania zasobów, z podziałem na następujące kategorie
   1. Zasoby operacyjne: wyświetla pojemność zasobów, które mają charakter dynamiczny i oczekuje się ich zmiany w krótkich odstępach czasu. Przykładami są trasy LPM, adresy MAC, tablice zabezpieczeń (ACL TCAM), itp. Predykcja przekroczenia na bazie trendu,
   2. Zasoby konfiguracyjne: Wyświetla wykorzystanie pojemności zasobów zależnych od konfiguracji, takich jak liczba VRF, VLAN, (mikro)segmentów, itp.,
   3. Zasoby sprzętowe: wykorzystanie ilości portów i przepustowość,
   4. Środowiskowe (temperatura, utylizacja CPU, RAM, prędkości wentylatorów, itp.),
   5. Co najmniej 30 dniowa retencja danych;
7. Analityka przepływów w sieci (flow)– celem identyfikacji anomalii sieciowych i ich źródeł w warstwie transmisji (data plane). Wspierane anomalie/funkcjonalności:
   1. odrzucone pakiety,
   2. opóźnienia,
   3. ruchy, przemieszczenia workload (MAC flapping, itp) dla vm i bare metal wraz z ich lokalizacją,
   4. problemy z routingiem,
   5. odrzucone pakiety/ramki przez ACL,
   6. Co najmniej 7 dniowa retencja danych o wszystkich przepływach i związanych z nimi anomaliach zebranych ze wszystkich urządzeń Fabryki IP.
8. Silnik analityczny, który po analizie konfiguracji i weryfikacji stanu sieci zapewnia zabezpieczenie poprawności działania i konfiguracji w sieci opartej o architekturę IP Fabric. Przeprowadzona analiza zawiera opis zdarzenia, obiekty, których dotyczy (jak urządzenia końcowe, segment/VLAN/VRF itp.) oraz rekomendację co działań naprawczych.
9. Wspomaganie zarządzania zmianami konfiguracji i predykcji ich wpływu na usługi sieciowe
   1. Analiza wpływu dokonanych zmian w konfiguracji w określonym przedziale czasu, z wyszczególnieniem zlikwidowanych oraz nowych zdarzeń/alertów z podziałem na ważność problemu.
   2. Analiza porównawczej pomiędzy dwoma stanami sieci, np. sprzed i po oknie serwisowym ze szczegółowym wykazaniem wszystkich zmian, wskazaniem ich wpływu na poszczególne części sieci (obiekty sieciowe jak segment/VRF, itp.) oraz osób odpowiedzialnych za wdrożenie tych zmian.
   3. Przewidywanie wpływu zmiany – analiza zmiany zdefiniowanej jako plik konfiguracyjny (typu JSON/XML, itp.) w stosunku do aktualnej konfiguracji w szczególności z wyszczególnieniem zdarzeń/alertów z podziałem na nowe, zachowane, usunięte oraz na ważność problemu.
   4. Możliwość automatycznego testowania (poprawności) zmiany – punkt c) z wykorzystanie API.
   5. Weryfikacja stanu sieci - zapewnienie komunikacji i eliminacja potencjalnych awarii/luk w konfiguracji przed wystąpieniem jakiegokolwiek wpływu na produkcję, np. pętli routingowych oraz zduplikowanych sieci w tym samym VRF;
   6. Weryfikacja zgodności konfiguracji z ustalonymi regułami polityki bezpieczeństwa i polityki dostępności.
   7. Bieżąca analiza i weryfikacja dynamicznego stanu całej sieci pod kątem ustalonych reguł dotyczących: komunikacji lub jej braku, realizacji polityki ruchu i bezpieczeństwa.
   8. Generowanie alertów dla administratora w przypadku wystąpienia naruszeń, np. ACL dopuszczająca ruch pomiędzy dwoma segmentami, kiedy jest to zabronione odpowiednią regułą polityki bezpieczeństwa.
   9. Analiza problemów z łącznością dla urządzeń końcowych z klasyfikacją ich ważności;
   10. Graficzna analiza zasad polityki ruchu (z uwzględnieniem obiekty typu segment, urządzenie końcowe, VRF, tenant). Możliwość weryfikacji łączności pod kątem komunikacji oraz zasad bezpieczeństwa (ACL) i segmentacji między obiektami sieciowymi.
10. Zestaw narzędzi jest dostarczony na platformie sprzętowej rekomendowanej przez producenta, zwymiarowanej zgodnie z wymaganiami oraz odpornej na wystąpienie pojedynczej awarii (dysk, CPU, cały węzeł).
11. Kompatybilność pomiędzy oprogramowaniem zarządzającym, analitycznym a urządzeniami sieciowymi jest potwierdzona dokumentacją producenta.

# FWVPN - Urządzenie klasy firewall umożliwiające koncentrację połączeń VPN

System składa się z następujących elementów:

* 1. Dwa urządzenia typu firewall dostarczone jako dedykowane urządzenie fizyczne pracujące w trybie wysokiej dostępności wraz ze wszystkimi usługami subskrypcyjnymi na okres 48 miesięcy.

**Opis techniczny urządzeń:**

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.

1. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection
2. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band
3. Urządzenie jest zasilane prądem przemiennym 230V
4. Możliwość montażu w szafie rack 19” (dołączone niezbędne elementy montażowe)
5. Urządzenie wyposażone w 12 wbudowanych portów GbE RJ45, 4 porty Gigabit Ethernet SFP oraz jeden slot na moduły rozszerzeń umożliwiające dalszą rozbudowę o porty 10 Gigabit Ethernet SFP+ (co najmniej 8)
6. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1 000 sieci VLAN
7. Urządzenie wyposażone w port USB 2.0
8. Wysokość urządzenia 1RU
9. Urządzenie wyposażone jest w redundantny zasilacz. Zasilacze mogą być wymieniane podczas pracy urządzenia („na gorąco”)
10. Przepustowość urządzenia przy włączonej inspekcji „stateful” na poziomie 10Gbps dla pakietów o wielkości 1500 bajtów oraz 5 Gbps dla ruchu rzeczywistego (tzw. ruch multiprotocol)
11. 2 000 000 maksymalnych jednoczesnych sesji z możliwością zestawiania co najmniej 40 000 nowych połączeń na sekundę
12. Możliwość połączenia VPN do 7500 urządzeń z maksymalną sumaryczną przepustowością 1 Gbps dla pakietów 450B UDP
13. Urządzenie umożliwia wirtualizację konfiguracji oraz na odseparowanie tablic routingu poprzez podział fizycznego urządzenia na wirtualne konteksty. Urządzenie posiada dwa wbudowane konteksty oraz pozwala na rozbudowę do 30 kontekstów poprzez zakup odpowiedniej licencji.

**Opis funkcjonalny:**

1. Urządzenie działa pod kontrolą 64-bitowego dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia
2. Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
3. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory
4. Urządzenie posiada możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos
5. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
6. Urządzenie pełni funkcję koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access)
7. Urządzenie obsługuje protokoły IKEv1 i IKEv2.
8. Urządzenie obsługuje funkcję skrótu SHA-2 o długości 256, 384 i 512 bitów.
9. Urządzenie obsługuje szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
10. Urządzenie obsługuje protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH) dla grup 19,20 i 21.
11. Urządzenie obsługuje protokół DSA w przestrzeni krzywych eliptycznych (ECDSA)
12. Urządzenie zapewnia w zakresie SSL VPN weryfikację uprawnień stacji do zestawiania sesji, poprzez weryfikację jej cech, co najmniej:
    1. OS - System operacyjny
    2. IP Address Check - adres z jakiego następuje połączenie
    3. File Check - pliki w systemie.
    4. Registry Check - wpisy w rejestrze systemu Windows.
    5. Certificate Check - zainstalowane certyfikaty
13. Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN
14. Oprogramowanie klienta VPN (IPSec oraz SSL) ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows (7, XP – wersje 32 i 64-bitowe) i Linux i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC.
15. Oprogramowanie klienta VPN obsługuje protokół szyfrowania AES
16. Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połączenia klientem VPN (wyłączanie tzw. split-tunnelingu)
17. Wraz z systemem dostarczone są licencje klienta VPN w ilości sztuk 1000 w zakresie poniższych funkcjonalności:

- podstawowe funkcjonalności VPN dla komputerów oraz urządzeń mobilnych, VPN per-aplikacja dla urządzeń mobilnych

- uwierzytelnianie SAML

- zbieranie danych kontekstowych z urządzeń końcowych

- suplikant Windows IEEE 802.1x

- zgodność FIPS

- możliwość weryfikacji zgodności i głębokiej analizy stacji końcowej

1. Urządzenie ma możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI
2. Urządzenie umożliwia grupowanie VLANów w transparentnym trybie pracy firewalla z możliwością zdefiniowania co najmniej 250 takich grup co najmniej po 20 VLANów. Każda tak zdefiniowana grupa umożliwia realizację odrębnych list kontroli dostępu.
3. Urządzenie umożliwia wdrożenia w scenariuszu z routingiem asymetrycznym.
4. Urządzenie obsługuje protokół NTP dla IPv4 i IPv6 oraz obsługuje następujące algorytmy uwierzytelnienia: MD5, SHA-1, SHA-256, SHA-512.
5. Urządzenie współpracuje z serwerami CA
6. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego. Urządzenie wspiera translację adresów (NAT) dla ruchu multicastowego
7. Urządzenie wspiera mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv6 na IPv6, z IPv4 na IPv4, z IPv4 na IPv6.
8. Urządzenie umożliwia więcej niż 65535 dynamicznych translacji PAT do pojedynczego zewnętrznego adresu IP.
9. Urządzenie umożliwia konfigurację czasu ważności translacji PAT.
10. Urządzenie wykonując dynamiczne translacje PAT do puli zewnętrznych adresów IP, równomiernie korzysta ze wszystkich zdefiniowanych w puli adresów.
11. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby i active/active dla kontekstów.
12. Urządzenie realizuje synchronizację tablicy połączeń pomiędzy węzłami pracującymi w trybie wysokiej dostępności HA
13. Urządzenie zapewnia możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia
14. Urządzenie zapewnia funkcjonalność stateful failover dla ruchu VPN
15. Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli co najmniej następujących usług:
    1. Hypertext Transfer Protocol (HTTP),
    2. File Transfer Protocol (FTP),
    3. Extended Simple Mail Transfer Protocol (ESMTP),
    4. Domain Name System (DNS),
    5. Simple Network Management Protocol v 1/2/3 (SNMP),
    6. Internet Control Message Protocol (ICMP),
    7. SQL\*Net,
    8. inspekcji protokołów dla ruchu voice/video – H.323 (włącznie z H.239), SIP, MGCP, RTSP
16. Urządzenie umożliwia zaawansowaną normalizację ruchu TCP:
    1. poprawność pola TCP ACK (invalid-ack )
    2. poprawność sekwencjonowania segmentów TCP (seq-past-window)
    3. poprawność ustanawiania sesji TCP z danymi (synack-data)
    4. limitowanie czasu oczekiwania na segmenty nie w kolejności
    5. poprawność pola MSS (exceed-mss).
    6. poprawność pola długości TCP
    7. poprawność skali okna segmentów TCP non-SYN
    8. poprawność wielkości okna TCP
17. Urządzenie umożliwia zaawansowane badanie stanu każdej sesji TCP w zakresie:
    1. sprawdzania opcji TCP, usuwania opcji TCP i odrzucania segmentów z opcjami TCP
    2. poprawności pola TCP ACK
    3. poprawności sekwencjonowania segmentów TCP (seq-past-window) ze wsparciem mechanizmów akceleracji sieci WAN wprowadzających przesunięcie numerów sekwencyjnych TCP
    4. weryfikacji sumy kontrolnej segmentu TCP
    5. weryfikacji pola TCP SACK ALLOW
    6. weryfikacji wielkości okna TCP
    7. usuwania flagi URG
    8. usuwania segmentów przekraczających maksymalny rozmiar (MSS)
    9. usuwania segmentów z flagą SYN i z flagami SYN/ACK, jeśli zawierają one dane
18. Urządzenie umożliwia ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów.
19. Urządzenie umożliwia ograniczenie maksymalnej liczby równoczesnych półotwartych połączeń TCP zestawionych do hosta lub do grupy hostów.
20. Urządzenie umożliwia zresetowanie otwartego połączenia TCP, jeśli przez określony okres czasu przez połączenie nie przesyłano żadnych danych.
21. Urządzenie umożliwia inspekcję ruchu HTTP w zakresie:
22. zgodności z formalną definicją protokołu
23. ukrywania nagłówka Server w odpowiedzi HTTP
24. filtrowania dopuszczalnych metod HTTP
25. filtrowania dopuszczalnych typów MIME
26. filtrowania dopuszczalnych adresów URL
27. Urządzenie umożliwia inspekcję ruchu SMTP w zakresie:
28. zgodności z formalną definicją protokołu ESMTP
29. ukrywania wiadomości powitalnej serwera
30. filtrowania długości wydawanych komend
31. filtrowania listy odbiorców dłuższej niż określona liczba
32. filtrowania długości adresu nadawcy
33. filtrowania długości pola MIME
34. filtrowania dopuszczalnych typów MIME
35. Urządzenie umożliwia inspekcję ruchu DNS w zakresie:
36. zgodności z formalną definicją protokołu DNS
37. filtrowania długości wiadomości
38. filtrowania po typie zapytania
39. randomizowania numeru identyfikacyjnego wiadomości
40. weryfikacji zgodności numeru indentyfikacyjnego zapytania i odpowiedzi
41. blokowania innych odpowiedzi niż pierwsza (ochrona przed atakiem dns spoofing i dns poisoning)
42. Urządzenie ma możliwość blokowania aplikacji (np. peer-to-peer czy „internetowy komunikator”) wykorzystujących port 80
43. Urządzenie zapewnia obsługę i kontrolę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP
44. Urządzenie ma możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe
45. Urządzenie zapewnia wsparcie stosu protokołów IPv6 w tym:
46. dla list kontroli dostępu dla IPv6
47. możliwości filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload
48. wspiera inspekcję protokołu IPv6, pracując w trybie transparentnym
49. wspiera adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover)
50. wspiera realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6
51. Urządzenie umożliwia współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik, o wielkości przekraczającej 4KB
52. Urządzenie obsługuje routing statyczny i dynamiczny (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).
53. Urządzenie pozwala na osiągnięcie wysokiej dostępności dla protokołów routingu dynamicznego (min OSPF), tzn. trasy dynamiczne zawarte w tablicy routingu są synchronizowane z urządzenia active na urządzenie standby
54. Urządzenie obsługuje ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania list kontroli dostępu dla ruchu multicastowego.
55. Urządzenie umożliwia konfigurację w roli serwera DHCP, z możliwością rezerwacji adresu IP dla zdefiniowanego adresu MAC.
56. Urządzenie umożliwia funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay) dla IPv4 i IPv6.
57. Urządzenie umożliwia zbieranie informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL)
58. Urządzenie umożliwia konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie
59. Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu
60. Istnieje możliwość zaimplementowania list kontroli dostępu ACL na dwa sposoby:
    1. Gdy pojedyncza reguła konfiguracyjna w ACL składa się z obiektów, urządzenie tworzy tyle rzeczywistych reguł, ile jest możliwości połączeń (permutacji) pomiędzy danymi z tych obiektów i monitoruje każdy taki wpis osobno.
    2. Gdy pojedyncza reguła konfiguracyjna składa się z obiektów, urządzenie tworzy tylko jedną regułę rzeczywistą zawierającą same obiekty i monitoruje tę regułę w całości jako jeden wpis. Taki tryb pozwala na tworzenie bardzo dużych list ACL opartych w większości na obiektach bez znacznego wpływu na zajętość pamięci urządzenia.
61. Listy kontroli dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:
62. źródłowy i docelowy adres IPv4
63. źródłowy i docelowy adres IPv6
64. źródłowy i docelowy numer portu UDP
65. źródłowy i docelowy numer portu TCP
66. nazwy domenowej hosta źródłowego lub docelowego
67. nazwa użytkownika w usłudze katalogowej Microsoft Active Directory
68. nazwa grupy w usłudze katalogowej Microsoft Active Directory
69. czas
70. Urządzenie nie może posiadać żadnych zaszytych w kodzie ograniczeń na liczbę reguł dostępu jakie mogą być równocześnie wykorzystywane.
71. Urządzenie umożliwia inspekcję ruchu IPv4 z wykorzystaniem nagłówków: End of Options List, No Operation, Router Alarm.
72. Urządzenie umożliwia inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload.
73. Jeśli pakiet IPv4/IPv6 został pofragmentowany, urządzenie odtwarza oryginalny pakiet kontrolując przy tym kolejność fragmentów i ich integralność.
74. Urządzenie umożliwia skonfigurowanie maksymalnej dopuszczalnej liczby fragmentów w ramach jednego odtwarzanego pakietu.
75. Urządzenie umożliwia skonfigurowanie maksymalnego dopuszczalnego okresu czasu, w którym otrzymuje wszystkie fragmenty niezbędne do odtworzenia pakietu.
76. Urządzenie umożliwia pominięcie stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu
77. Urządzenie wspiera Proxy dla protokołu SCEP i umożliwia zautomatyzowany proces pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN
78. Urządzenie wspiera użytkownika korzystającego z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie Microsoft AD bezpośrednio, co najmniej dla obsługi sytuacji wygaśnięcia terminu ważności hasła w systemie Microsoft AD, umożliwiając zmianę przeterminowanego hasła.
79. Urządzenie obsługuje IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode. Ponadto urządzenie wspiera protokół IKEv2 (Internet Key Exchange w wersji 2) dla połączeń zdalnego dostępu VPN oraz site-to-site VPN opartych o protokół IPSec
80. Urządzenie obsługuje ramki Ethernet typu Jumbo (o rozmiarze 9216 bajtów).
81. Urządzenie obsługuje ramki XOFF zgodnie z definicją standardu 802.3x.
82. Urządzenie umożliwia konfigurację następujących mechanizmów zarządzania jakością przesyłania danych (Quality of Service):
83. Urządzenie obsługuje mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu - obsługa kolejki priorytetowej o konfigurowalnej długości per każdy interfejs urządzenia realizujący usługę firewalla– pakiety umieszczone w tej kolejce zostaną obsłużone przed innymi pakietami umieszczonymi w innych kolejkach
84. policing – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez odrzucanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps. Policing jest obsługiwany dla ruchu wchodzącego i wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.
85. shaping – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez buforowanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps konfigurowalną z granularnością co najmniej 8kbps. Zbuforowane pakiety są wysyłane w późniejszym okresie czasu, gdy sumaryczna przepustowość strumieni danych będzie niższa niż zadana wartość w bps. Shaping jest obsługiwany co najmniej dla ruchu wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.
86. Urządzenie obsługuje protokół WCCPv2.
87. Urządzenie umożliwia wykrywanie, raportowanie i filtrowanie ruchu typu "call-home" od zainfekowanych złośliwym oprogramowaniem hostów w sieci chronionej do sieci typu botnet. Proces filtrowania opiera się o globalną bazę reputacyjną adresów IP utrzymywaną przez producenta urządzenia.
88. Urządzenie umożliwia zarządzanie:
89. przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.
90. przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji
91. programowo przez interfejs API dostępny przy pomocy protokołu https
92. przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji
93. Zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.
94. Urządzenie dla protokołu SSHv2 umożliwia uwierzytelnienie w oparciu o nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.
95. Urządzenie umożliwia konfigurację maksymalnej równoczesnej liczby sesji zdalnego zarządzania.
96. Urządzenie umożliwia ograniczenia dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.
97. Urządzenie umożliwia wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.
98. Urządzenie ma możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG z możliwością szyfrowania transmisji wiadomości SYSLOG przy pomocy SSL/TLS.
99. Urządzenie wspiera eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow v9 (RFC 3954)
100. Urządzenie posiada możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS i TACACS+ oraz obsługuje mechanizmy AAA (autentykacja, autoryzacja, accounting) przy współpracy z systemem Cisco ISE.
101. Dostęp do urządzenia jest możliwy przez SSHv2
102. Urządzenie obsługuje protokół SNMP v 1/2c/3
103. Znacznik czasu w logach generowanych przez urządzenie jest zgodny z RFC5424
104. Możliwa jest edycja pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.
105. Urządzenie umożliwia zrzucenie obecnego stanu programu (coredump) dla potrzeb diagnostycznych
106. Urządzenie posiada wsparcie dla mechanizmu TCP Ping, który pozwala na wysyłanie wiadomości TCP dla rozwiązywania problemów związanych z łącznością w sieciach IP
107. Urządzenie umożliwia uwierzytelnienie i konfigurację poziomu dostępu administratora w oparciu o role (ang. Role Base Access Control) z wykorzystaniem bazy danych użytkowników zdefiniowanej lokalnie na urządzeniu lub na zewnętrznych serwerach dostępnych przy pomocy protokołów RADIUS i TACACS+.
108. Urządzenie posiada zaawansowaną instrumentację pozwalającą na uzyskanie szczegółowej informacji o obciążeniu CPU przez każdy z procesów oddzielnie, z podziałem na procesy, w interwałach czasowych 5 minut, 1 minuta i 5 sekund.
109. Wyposażenie każdego firewalla obejmuje:
     1. 3 x moduł SFP+ o prędkości 10Gb umożliwiający połączenie z wykorzystaniem pojedynczej pary światłowodów jednomodowych (SM) zakończony konektorem LC.

# RSKD - Rozbudowa systemu uwierzytelniania dostępu do sieci LAN/WLAN/VPN

System zapewnia pełne zarządzanie cyklem życiowym dostępu do zasobów sieciowych, niezależnie od miejsca uzyskiwanego dostępu. System realizuje wsparcie dla dostępu gościnnego w sieci, identyfikację stacji, rejestrację urządzeń. System może obejmować kontrolą dostęp wszystkich urządzeń podłączonych do sieci IP w tym terminali, komputerów PC, smartfonów i tabletów, telefonii IP, terminali video i innych podłączonych urządzeń.

Rozbudowa systemu obejmuje dostarczenie dwóch maszyn wirtualnych. Każda z maszyn wspiera tryb pracy w oparciu o min. 64GB RAM i 16vCPU.

Dostarczone maszyny wirtualne mają integrować się z obecnie wykorzystywanym przez Zamawiającego systemem kontroli dostępu Cisco Identity Services Engine w pełnym zakresie funkcjonalności udostępnianym przez producenta systemu oraz zgodnie z wymaganiami opisanymi w niniejszej sekcji.

**Podstawowe cechy systemu**

1. System umożliwia instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych.
2. System umożliwia elastyczną rozbudowę poprzez dodawanie licencji dla podstawowych i zaawansowanych funkcjonalności w ramach wzrostu liczby obsługiwanych stacji końcowych.
3. System umożliwia wysoką skalowalność i rozbudowę w miarę wzrostu liczby urządzeń.
4. System umożliwia instalację na maszynie wirtualnej (VM) i maszynie fizycznej, w tym na:
5. VMware wersji 8 dla ESXi 5.1 U2
6. VMware wersji 11 dla ESXi 6.x
7. hypervisorze KVM na Red Hat Enterprise Linux (RHEL) 7.0
8. Microsoft Hyper-V
9. serwerach fizycznych wspieranych przez producenta
10. System umożliwia wydzielenie określonych elementów funkcjonalnych, instalowanych jako oddzielne maszyny fizyczne lub wirtualne, w tym:
    1. Wydzielenie podsystemu zarządzania (Administration), umożliwiającego administratorowi dostęp do interfejsu graficznego (GUI) za pomocą przeglądarki web i zmianę konfiguracji systemu oraz jego monitorowanie
    2. Wydzielenie podsystemu monitoringu, logowania i rozwiązywania problemów, umożliwiającego gromadzenie wiadomości logowania z:
       1. przełączników dostępowych
       2. sesji uwierzytelniania 802.1X
       3. zdarzeń kontroli dostępu (autoryzacji)
       4. zdarzeń związanych z błędami
       5. zdarzeń związanych z alarmami systemowymi
    3. Wydzielenie serwerów usługowych realizujących funkcje:
       1. serwera RADIUS dla infrastruktury sieciowej
       2. serwera polityk uwierzytelniania i kontroli dostępu 802.1X
       3. serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego
       4. serwera profilowania stacji końcowych
11. System umożliwia realizację wysokiej dostępności elementów funkcjonalnych, w tym:
    1. zapewnienie redundancji 1:1 podsystemu zarządzania i podsystemu monitoringu
    2. zapewnienie redundancji przynajmniej N+1 dla serwerów usługowych
12. System umożliwia aktualizację oprogramowania za pomocą interfejsu graficznego z repozytoriów umieszczonych na dysku lokalnym oraz zasobach zdalnych – co najmniej przez serwer TFTP, serwer FTP/SFTP, serwer HTTP/HTTPS, udział NFS.
13. System umożliwia zarządzanie łatkami (patch management), w tym operację powrotu do poprzedniej wersji (rollback).
14. System umożliwia tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
15. System umożliwia uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników.
16. System umożliwia wymuszenie reguł złożoności haseł dla administratorów, w tym co najmniej minimalną długość hasła oraz wymuszenie hasła zawierającego małą literę, wielką literę, cyfrę, znak niealfanumeryczny. System wymusza hasło różne od trzech poprzednich haseł i jego zmianę co określoną ilość dni.
17. System umożliwia kontrolę dostępu do poszczególnych elementów menu interfejsu graficznego administratora:
    1. dostęp do interfejsu konfiguracji usług tożsamości 802.1X
    2. dostęp do interfejsu konfiguracji urządzeń sieciowych
    3. dostęp do interfejsu konfiguracji polityk
    4. dostęp do interfejsu konfiguracji kontroli dostępu gościnnego
    5. dostęp do interfejsu monitorowania, rozwiązywania problemów i raportowania
18. System umożliwia kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP.
19. System posiada możliwość podłączenia i identyfikacji urządzenia końcowego z wykorzystaniem MUD (Manufacturer Usage Description) zgodnie ze standardem IETF i RFC8520.

**Mechanizmy uwierzytelniania 802.1x:**

1. System wspiera następujące protokoły uwierzytelniania i standardy:
   1. RADIUS, zgodnie z dokumentami:
      1. RFC 2138 — Remote Authentication Dial In User Service (RADIUS)
      2. RFC 2139 — RADIUS Accounting
      3. RFC 2865 — Remote Authentication Dial In User Service (RADIUS)
      4. RFC 2866 — RADIUS Accounting
      5. RFC 2867 — RADIUS Accounting for Tunnel Protocol Support
      6. RFC 2868 — RADIUS Attributes for Tunnel Protocol Support
      7. RFC 2869 — RADIUS Extensions
   2. RADIUS Proxy dla zewnętrznego serwera RADIUS
2. System wspiera protokół Windows Active Directory, w tym następujące repozytoria AD:
   1. Microsoft Windows Active Directory 2003 32bit
   2. Microsoft Windows Active Directory 2003 R2 32bit i 64bit
   3. Microsoft Windows Active Directory 2008 32bit i 64bit
   4. Microsoft Windows Active Directory 2008 R2 64bit
   5. Microsoft Windows Active Directory 2012
   6. Microsoft Windows Active Directory 2012 R2
   7. Microsoft Windows Active Directory 2016
3. System wspiera protokół Lightweight Directory Access Protocol (LDAP)
4. System wspiera serwery Radius Token OTP, w tym co najmniej każdy serwer tokenowy RADIUS zgodny z dokumentem RFC 2865
5. System wspiera następujące protokoły uwierzytelniania:
   1. PAP/ASCII
   2. CHAP
   3. MS-CHAPv1
   4. MS-CHAPv2
   5. EAP-MD5
   6. LEAP
   7. EAP-TLS
   8. Protected Extensible Authentication Protocol (PEAP) z metodami wewnętrznymi:
      1. EAP-MS-CHAPv2
      2. EAP-GTC
      3. EAP-TLS
   9. System umożliwia konfigurację mechanizmów PEAP Session Resume, PEAP Session Timeout i Fast Reconnect
6. System wspiera implementację 802.1X z przynajmniej następującymi suplikantami:
   1. wbudowanym klientem 802.1X dla Windows 10
   2. wbudowanym klientem 802.1X dla Windows Vista
   3. wbudowanym klientem 802.1X dla Windows 7
   4. wbudowanym klientem 802.1X dla Windows 8 i 8.1
   5. Apple Mac OS X Supplicant
   6. Apple iOS Supplicant
   7. Google Android Supplicant
7. System umożliwia tworzenie polityk uwierzytelniania 802.1X opartych złożone o reguły (rule-based).
8. System umożliwia uwierzytelnianie 802.1X maszyn i użytkowników.
9. System umożliwia tworzenie polityk kontroli dostępu (authorization) 802.1X opartych o reguły.
10. System posiada lokalną bazę użytkowników. Lokalną bazę użytkowników można tworzyć per użytkownik lub dodać w postaci zbiorczego pliku w formacie CSV (lub innym edytowalnym).
11. System posiada lokalną bazę stacji końcowych. Lokalna baza stacji końcowych jest tworzona per stacja końcowa na podstawie unikalnego adresu MAC.
12. System wspiera uwierzytelnienie stacji końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
13. System wspiera zaawansowane funkcjonalności 802.1X realizowane na urządzeniach dostępowych (NAD - Network Access Devices), w tym:
    1. tryb uwierzytelniania 802.1X, w którym dozwolony jest jeden host per port
    2. tryb uwierzytelniania 802.1X, w którym dozwolonych jest wiele urządzeń per port fizyczny, ale wymagane jest uwierzytelnienie jedynie pierwszego urządzenia
    3. tryb uwierzytelniania 802.1X, w którym dozwolone jest jedno urządzenie telefonii IP w domenie głosowej (Voice VLAN) i jeden w host w domenie danych (Data VLAN) na jednym porcie fizycznym
    4. tryb uwierzytelniania 802.1X dozwalający wiele hostów na jednym porcie fizycznym
    5. mechanizm umożliwiający przeniesienie uwierzytelnionego hosta w obrębie przełącznika z jednego portu fizycznego na inny
    6. mechanizm umożliwiający poprawną obsługę sytuacji w której nowy host podłącza się do portu na którym uprzednio było uwierzytelnione urządzenie, w tym w VLANie głosowym
    7. mechanizm umożliwiający wysłanie informacji o reloadzie urządzenia (przełącznika) dostępowego do serwera AAA. Dzięki temu uwierzytelnione aktywne sesje związane z tym konkretnym urządzeniem zostaną usunięte z listy na serwerze AAA.
    8. mechanizm przypisania VLANu w procesie uwierzytelnienia i kontroli dostępu 802.1X
    9. mechanizm przypisania listy kontroli dostępu per użytkownik dla ruchu IP (ACL) w procesie uwierzytelnienia i kontroli dostępu 802.1X
    10. obsługa przypisania listy kontroli dostępu dla przekierowania ruchu web w procesie uwierzytelnienia i kontroli dostępu 802.1X, w celu realizacji uwierzytelniania za pomocą przeglądarki
    11. mechanizm 802.1x umożliwiający realizację dostępu gościnnego w dedykowanym VLANie (Guest VLAN) dla użytkowników gościnnych
    12. mechanizm 802.1x umożliwiający przypisanie urządzenia telefonii IP do dedykowanego VLANu w sytuacji, gdy serwer AAA jest niedostępny
    13. przypisanie przez serwer AAA dla uzytkownika nie jednego, lecz grupy VLANów dla użytkownika, z których przełącznik wybiera jeden, w którym jest najmniej użytkowników
    14. uwierzytelnienie 802.1X urządzenia telefonii IP znajdującego sie w VLANie głosowym
    15. współpraca mechanizmu 802.1X z urządzeniami używającymi mechanizmu Wake-on-LAN
    16. możliwość elastycznej konfiguracji kolejności metod 802.1X użytych do uwierzytelnienia stacji, w tym uwierzytelnienia względem centralnej bazy MAC, metod EAP dla 802.1X i uwierzytelnienia web
    17. możliwość uwierzytelnienia przełącznika dostępowego do dystrybucyjnego, jako stacji końcowej w celu zapobiegnięcia przed podłączeniem do sieci nieuprawnionego przełącznika
14. System wspiera uwierzytelnianie nazwą użytkownika i hasłem przez portal web, jako jedną z metod uwierzytelniania do sieci, (dotyczy m.in. w sytuacji, gdy stacja ma niepoprawnie skonfigurowane lub niedziałające oprogramowanie suplikanta 802.1X).
15. System wspiera m.in. następujące urządzenia sieciowe, jako klientów RADIUS (NAD - Network Access Device):
    1. Przełączniki Ethernet. Lista wspieranych przełączników Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania)
    2. Kontrolery sieci bezprzewodowej. Lista wspieranych kontrolerów sieci bezprzewodowej Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania)
    3. Koncentratory VPN. Lista wspieranych koncentratorów VPN Cisco oraz producentów trzecich dostępna jest na stronach Cisco (wraz z wersjami oprogramowania)
16. Możliwość rozbudowy funkcjonalności o serwer TACACS+ do administrowania urządzeniami sieciowymi bez konieczności rozbudowy sprzętowej

**Realizacja dostępu gościnnego:**

1. System umożliwia realizację dostępu gościnnego dla stacji końcowych wyposażonych w przeglądarkę internetową, w tym, między innymi dla:
   1. Microsoft Windows 10, Windows 8.1, Windows 8, Windows 7, Microsoft Windows Vista,
   2. Apple Mac OS X 10.x
   3. Apple iOS 8.0, 7.x, 6.1, 6, 5.1, 5.0.1
   4. Google Android dla 2.2 i nowszych
   5. Linux
2. System umożliwia dodawanie kont gościnnych przez wybrane osoby (sponsor).
3. System zapewnia uwierzytelnienie sponsora które musi odbywać sekwencyjnie się w oparciu o:
   1. wewnętrzną bazę użytkowników
   2. zewnętrzne repozytorium użytkowników
4. System umożliwia konfigurację uprawnień sponsora, w tym uprawnienia do:
   1. logowania się do systemu
   2. tworzenia pojedynczego konta gościnnego
   3. tworzenia wielu kont gościnnych
   4. importowania kont gościnnych z pliku CSV
   5. wysyłania wiadomości email po utworzeniu konta gościnnego
   6. wysyłania wiadomości SMS po utworzeniu konta gościnnego
   7. wyświetlenia hasła konta gościnnego
   8. wydrukowania danych konta gościnnego
   9. wyświetlenia danych stworzonych kont gościnnych
   10. zawieszenia (suspend) i reinicjacji kont gościnnych
5. System umożliwia personalizację wyglądu portalu sponsora i gościa, w tym:
   1. zmianę logo strony logowania
   2. zmianę obrazu tła strony logowania
   3. zmianę logo bannera
   4. zmianę obrazu tła bannera
   5. zmianę koloru tła strony z treścią
6. System umożliwia zmianę konfiguracji portów portalu administratora, gościa i sponsora, w tym portu HTTP i portu HTTPS
7. System umożliwia zmianę adresu URL i FQDN strony sponsora.
8. System umożliwia automatyczne kasowanie wygasłych kont gościnnych: na żądanie i okresowo co zadaną liczbę dni i o określonej godzinie. System umożliwia wyświetlenie czasu ostatniego kasowania wygasłych kont gościnnych i następnego kasowania wygasłych kont gościnnych
9. System posiada wbudowane, wspierane przez producenta wzorce językowe dla stron sponsora i gościa, co najmniej w językach polskim, angielskim, francuskim, niemieckim i hiszpańskim
10. System umożliwia stworzenie własnego wzorca językowego dla stron sponsora i gościa, w tym w języku polskim.
11. System umożliwia wymuszenie wpisania w formularz rejestracyjny następujących danych gościa w trakcie tworzenia konta przez sponsora:
    1. Imienia
    2. Nazwiska
    3. Firmy
    4. adresu e-mail
    5. numeru telefonu
    6. danych opcjonalnych (nie mniej niż 5 dodatkowych pól)
12. System umożliwia konfigurację dla użytkowników gościnnych:
    1. wyświetlenia im informacji o polityce akceptowalnego użycia sieci (AUP)
    2. zezwolenia gościom na zmianę hasła
    3. samoobsługi przez gościa, czyli możliwości utworzenia konta gościnnego bez sponsora
13. System umożliwia honorowanie ustawień locale przeglądarki internetowej dla zastosowania odpowiedniego wzorca językowego.
14. System umożliwia konfigurację maksymalnej ilości nieudanych logowań do konta gościnnego.
15. System umożliwia konfigurację maksymalnej liczby urządzeń per konto gościnne i obsługuje co najmniej 20 urządzeń per konto gościnne.
16. System umożliwia konfigurację czasu ważności hasła w dniach w przedziale zadanym w dniach.
17. System umożliwia określenie profilu czasowego dla dostępu gościnnego, czyli domyślnego czasu ważności konta gościnnego z dokładnością do daty i godziny
18. System umożliwia konfigurację polityki złożoności haseł użytkowników gościnnych:
19. System umożliwia konfigurację polityki nazwy (login) użytkownika gościnnego w tym co najmniej tworzenie nazwy użytkownika z adresu e-mail i minimalnej długości nazwy użytkownika
20. System umożliwia tworzenie portalu typu Hotspot bez konieczności uwierzytelniania się gościa nazwą użytkownika i hasłem z opcjonalną akceptacją AUP (Acceptable Use Policy) i z koniecznością podania kodu dostępu.
21. System umożliwia przypisanie do każdego portalu gościnnego niezależnego wzorca językowego, interfejsu IP, portu HTTPS i certyfikatu SSL dla FQDN.
22. System umożliwia udostępnienie danych logowania gościnnego za pomocą email przez konfigurację bramy SMTP i poprzez SMS,
23. System wspiera API dla masowych operacji CRUD (Create, Read, Update, Delete) na kontach gościnnych.

**Profilowanie urządzeń:**

1. System umożliwia dokonanie profilowania (profiling) urządzenia końcowego dołączanego do sieci i realizację zróżnicowanego dostępu na podstawie jej zidentyfikowanego typu.
2. System umożliwia wykorzystanie danych z procesu profilowania do zdefiniowania polityk bezpieczeństwa. W szczególności zapewnia możliwość stworzenia polityk np. dla wszystkich drukarek, dla wszystkich urządzeń mobilnych, dla wszystkich stacji z Windows, etc.
3. System umożliwia dokonanie profilowania stacji końcowych poprzez analizę informacji pochodzących z następujących źródeł:
   1. DHCP
   2. DHCP SPAN
   3. HTTP
   4. RADIUS
   5. DNS
   6. SNMP
   7. Network Scan (NMAP lub inne narzędzie profilowania aktywnego)
4. System umożliwia wysłanie wiadomości RADIUS CoA (Reauth, Port Bounce) zgodnych z RFC 5176, po dokonaniu profilowania urządzenia końcowego w celu zmiany profilu autoryzacji.
5. System umożliwia dodawanie sprofilowanych stacji końcowych do lokalnej bazy stacji końcowych wraz z przypisaniem do grupy.
6. System posiada dostarczony przez producenta zestaw profili urządzeń, w tym przynajmniej dla:
   1. Stacji robocznych pracujących z systemami FreeBSD, Linux, Macintosh, Microsoft Windows, Sun,
   2. Urządzeń mobilnych: Android, Apple, Blackberry
   3. Telefonów IP
   4. Drukarek sieciowych
   5. Systemów wideokonferencyjnych w tym terminali i urządzeń z nimi powiązanych
   6. Routerów
   7. Punktów dostępu bezprzewodowego
7. System umożliwia subskrypcyjne, regularne i automatyczne pobieranie nowych profili urządzeń ze strony producenta, w tym następujących informacji:
   1. reguł identyfikacji nowych i uaktualnionych profili urządzeń końcowych w sieci
   2. reguł identyfikacji nowych urządzeń końcowych w sieci na podstawie MAC OUI, publikowanych na stronie http://standards.ieee.org/develop/regauth/oui/oui.txt
8. System umożliwia włączenie funkcjonalności regularnej (z częstotliwością dobową) i automatycznej subskrypcji nowych profili urządzeń ze strony producenta o zadanej godzinie lub jej całkowite wyłączenie w dowolnym momencie.
9. System wspiera raportowanie zmian w bazie danych profili powstałych w wyniku pobrania uaktualnienia profili urządzeń końcowych ze strony producenta.

**Analiza stacji końcowej (Posture Assessment):**

1. System umożliwia pobranie bazy wiedzy reguł analizy stacji końcowej (Posture) dla wspieranych systemów Antywirusowych (AV) i Antispyware (AS) ze strony producenta.
2. System umożliwia kontrolę zachowania dla stacji końcowych, które nie posiadają zainstalowanego agenta głębokiej analizy stacji końcowej (Posture).
3. System umożliwia regularne ponawianie głębokiej analizy stacji końcowej (periodic reassessment) w przedziale od 1 do 24 godzin.
4. System umożliwia przedstawienie użytkownikowi dokumentu Polityki Akceptowalnego Użycia (AUP). Polityka AUP jest prezentowana w postaci strony web po procesie głębokiej analizy stacji. Zawartość dokumentu AUP jest konfigurowalna.
5. System umożliwia głęboką analizę stacji końcowej Windows pod kątem plików (File Condition), w tym:
   1. istnienia pliku na stacji końcowej
   2. wersji pliku na stacji końcowej (równa, wcześniejsza niż, późniejsza niż)
   3. daty utworzenia i modyfikacji pliku na stacji końcowej (równa, wcześniej niż, później niż)
6. System umożliwia głęboką analizę stacji końcowej z systemem:
   1. Windows Vista
   2. Windows 7
   3. Windows 8 i 8.1
   4. Windows 10

pod kątem wpisów w rejestrze (Registry Condition), w tym:

1. kluczy rejestru z kluczem root: HKLM, HKCC, HKCU, HKU, HKCR z zadanym podkluczem pod kątem:

- istnienia lub nieistnienia klucza

- wartości klucza rejestru

- istnienia i wartości domyślnej wartości klucza rejestru typu Number, String, Version

1. System umożliwia głęboką analizę stacji końcowej z systemem:
   1. Windows Vista
   2. Windows 7
   3. Windows 8 i 8.1
   4. Windows 10

pod kątem uruchomionych aplikacji (Application Condition), w tym nazwy uruchomionego lub nieuruchomionego procesu

1. System umożliwia tworzenie słownika prostych i złożonych warunków (Simple i Compound Condition) dla głębokiej analizy stacji końcowej za pomocą wyrażeń logicznych AND, OR, NOT, w tym z uwzględnieniem:
   1. parametrów dostępu do sieci, w tym:
      1. lokalizacji stacji końcowej
      2. nazwy użytkownika
      3. adresu IP stacji
      4. metody uwierzytelnienia
      5. statusu uwierzytelnienia
      6. repozytorium użytkowników użytych dla uwierzytelnienia
      7. atrybutów RADIUS, w tym:
      8. Calling-Station-ID
      9. Framed-IP-Address
      10. NAS-Identifier
      11. NAS-IP-Address
      12. NAS-Port-Type
      13. Service-Type
      14. User-Name
   2. Parametrów sesji, w tym:
      1. typu żądania agenta na stacji końcowej (początkowe/initial lub reassessment)
      2. architektury systemu operacyjnego na stacji końcowej (32-bit lub 64-bit)
      3. adresu URL, z którego nastąpiło przekierowanie
2. System umożliwia głęboką analizę stacji końcowej z systemem:
   1. Windows Vista
   2. Windows 7
   3. Windows 8 i 8.1
   4. Windows 10
   5. Mac OS-X

pod kątem zainstalowanych aplikacji Antywirusowych (AV Compound Condition), w tym:

1. stwierdzenia czy system AV jest obecny na stacji
2. stwierdzenia czy definicje sygnatur AV są nie starsze niż zadana ilość dni od:
3. daty ostatniego pliku definicji
4. aktualnego czasu systemowego

**Obsługa certyfikatów CA:**

1. System posiada funkcję zintegrowanego centrum certyfikacji, Certificate Authority (CA) lub zapewniać współpracę z zewnętrznym centrum CA.
2. Funkcja CA umożliwia wystawianie certyfikatów dla urządzeń, które uzyskują dostęp do sieci w procesie BYOD, dla realizacji bezpiecznego uwierzytelniania przy pomocy EAP-TLS.
3. System wspiera hierarchiczność CA dla rozproszonego wdrożenia w dużej skali. W sytuacji rozproszenia systemu na wiele serwerów, serwery nadrzędne oferują funkcję Root CA, zaś serwery przetwarzające wspierają funkcję Subordinate CA (SCEP RA) dla wystawiania certyfikatów.
4. Funkcja CA zapewnia przynajmniej następujące funkcjonalności:
   1. Certificate Issuance: sprawdzenie i podpisywanie Certificate Signing Request (CSR) dla stacji końcowych, które chcą uzyskać dostęp do sieci za pomocą bezpiecznej metody uwierzytelniania EAP-TLS
   2. Key Management: generacja i bezpieczne przechowywanie kluczy i certyfikatów w modelu rozproszonym
   3. Certificate Storage: bezpieczne przechowywanie certyfikatów użytkowników i stacji
   4. Online Certificate Status Protocol (OCSP): wsparcie dla sprawdzenia ważności certyfikatów za pomocą protokołu OCSP wraz ze wsparciem dla wysokiej dostępności, przynajmniej dwóch serwerów OCSP per CA

**Raportowanie:**

1. System umożliwia generowanie m.in. następujących raportów:
   1. raportów dla protokołów AAA:
      1. diagnostyki protokołów AAA
      2. trendów uwierzytelnienia 802.1X
      3. accountingu RADIUS
      4. uwierzytelniania RADIUS
   2. raportów dozwolonych protokołów
      1. sumarycznej informacji o uwierzytelnieniach RADIUS per protokół, w tym:

- uwierzytelnień pomyślnych  
- uwierzytelnień nieudanych

* + 1. „N” największych ilości uwierzytelnień RADIUS per protokół EAP (Top5), w tym:

- uwierzytelnień pomyślnych  
- uwierzytelnień nieudanych

* 1. raportów dla poszczególnych instancji serwerów systemu, w tym:
     1. uwierzytelnień RADIUS per serwer
     2. Top „N” uwierzytelnień per serwer
     3. monitorowania Online Certificate Status Protocol (OCSP)
     4. administratorów systemu i ich uprawnień
     5. logowania administratorów do systemu
     6. zmian konfiguracji serwera dokonanych przez administratorów
     7. stanu serwera (w tym użycia CPU, pamięci, stanu procesów i opóźnienia RADIUS)
     8. zmian operacyjnych serwera dokonanych przez administratorów
     9. zmian haseł przez użytkowników
  2. raportów dla stacji końcowych, w tym:
     1. uwierzytelnień typu MAC Authentication
     2. Top „N” uwierzytelnień per adres MAC stacji
     3. Top „N” uwierzytelnień per maszyna
     4. Top „N” uwierzytelnień per RADIUS Calling Station ID
     5. działań podsystemu profilera per adres MAC
     6. czasu wymaganego na sprofilowanie stacji per adres MAC
  3. raportów dla błędów, w tym:
     1. błędów uwierzytelniania per szczegółowy kod błędu, który wystąpił
     2. sumarycznych przyczyn nieudanych uwierzytelnień
     3. Top „N” uwierzytelnień per rodzaj błędu
  4. raportów dla urządzeń sieciowych:
     1. sumarycznych uwierzytelnień dla urządzeń sieciowych
     2. Top „N” uwierzytelnień per urządzenie sieciowe
     3. niedostępności serwera AAA dla urządzenia sieciowego
     4. wiadomości logowanych przez urządzenia sieciowe
     5. stanu portów i sesji urządzenia sieciowego widocznych przez SNMP
  5. raportów użytkowników:
     1. sumarycznych uwierzytelnień użytkowników
     2. Top „N”uwierzytelnień per użytkownik
     3. sesji użytkowników gościnnych
     4. aktywności użytkowników gościnnych
     5. sumarycznych uwierzytelnień sponsorów dostępu gościnnego
     6. uwierzytelnień per unikalny użytkownik
  6. raportów katalogu sesji
     1. aktywnych sesji RADIUS
     2. historii sesji RADIUS
     3. zaterminowanych sesji RADIUS

**Alarmy:**

1. System umożliwia generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
   1. wiadomości e-mail
   2. syslog
2. Alarmy mogą być generowane w następujących sytuacjach:
   1. ilość obsługiwanych transakcji RADIUS na sekundę spadnie poniżej zadanego poziomu
   2. opóźnienie (latency) obsługi transakcji RADIUS będzie dłuższe od zadanego
   3. status krytycznych procesów będzie niepożądany, w tym status:
      1. procesu wewnętrznej bazy danych systemu
      2. serwera aplikacyjnego systemu
      3. bazy danych sesji
      4. kolektora i procesora wiadomości log
      5. błędy generowane przez system mają ważność powyżej "Error" w rozumieniu protokołu Syslog (Severity 3 i wyżej)
      6. stan obciążenia systemu wzrośnie powyżej zadanego poziomu, w tym:

- obciążenie systemu (load)  
- zajętość pamięci

1. System posiada zintegrowany z interfejsem graficznym zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
   1. badanie łączności IP za pomocą ping, nslookup, traceroute
   2. wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
      1. nazwy użytkownika
      2. adresu MAC
      3. statusu uwierzytelnienia (udana lub nieudana)
      4. powodu, jeżeli uwierzytelnienie nieudane
      5. zakresu czasowego, co do dnia, godziny i minuty
   3. wykonanie zdalnego polecenia na urządzeniu sieciowym
   4. ewaluację zgodności konfiguracji urządzenia sieciowego pod kątem:
      1. definicji serwerów AAA
      2. protokołu RADIUS
      3. odkrywania urządzeń
      4. logowania
      5. uwierzytelniania Web
      6. konfiguracji trybu 802.1X
      7. wykonanie zrzutu ruchu sieciowego (TCP Dump) docierającego do systemu

**Wsparcie dla protokołu IPv6:**

1. System posiada wsparcie dla SSH IPv6
2. System pozwala na zarządzanie administracyjne za pomocą interfejsu graficznego udostępnionego administratorowi z wykorzystaniem adresacji IPv6
3. System pozwala na konfigurację NTP IPv6
4. System umożliwia stworzenie reguł ograniczających dostęp administracyjny do linii poleceń lub interfejsu graficznego w oparciu o adres IPv6
5. System umożliwia konfigurację serwerów SNMP w oparciu o adresację IPv6
6. System umożliwia wysyłanie SNMP Trap do serwera SNMP IPv6
7. System umożliwia integrację z Active Directory w oparciu o IPv6
8. System umożliwia połączenie z serwerem Radius z wykorzystaniem adresu IPv6

**Dobre praktyki realizacji rozwiązania:**

1. System spełnia następujące warunki dobrych praktyk realizacji systemu uwierzytelnienia dostępu do sieci:
   1. System może występować w formie pojedynczego rozwiązania jak też systemu złożonego z kilku komponentów.
   2. W przypadku zastosowania rozwiązania złożonego z kilku komponentów system zapewnia pojedynczy interfejs konfiguracyjny, zarządzający i monitorujący zapewniający możliwość wymuszenia spójnej polityki bezpieczeństwa dla dostępu LAN/WLAN/VPN.
   3. Niezależnie od tego czy system występuje w formie pojedynczego rozwiązania lub jest złożony z kilku komponentów, może on być serwisowany jako jeden system w ramach pojedynczej usługi wsparcia.

# POBM – Przełącznik typ 1

1. Typ i liczba portów:

- 16 portów 10/100/1000BaseT RJ-45 + uplink 2x1G SFP

1. Porty SFP możliwe do obsadzenia następującymi rodzajami wkładek:

- Gigabit Ethernet 1000Base-SX

- Gigabit Ethernet 1000Base-LX/LH

1. Urządzenie posiada funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi
2. Zasilanie i chłodzenie:

- Urządzenie wyposażone jest w wbudowany zasilacz AC230V

- Urządzenie wykonanie jest w wersji bezwentylatorowej, głębokość urządzenie nie przekracza 33 cm

1. Parametry wydajnościowe:
   1. Przepustowość przełącznika (switching bandwidth) 36Gb/s (full duplex)
   2. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów (L3) 26.78Mpps
   3. Pamięć DRAM – 512 MB
   4. Pamięć flash – 256 MB
   5. Wielkość bufora pakietów - 1.5 MB
   6. Ilość wpisów w listach kontroli dostępu Security ACL – 600
   7. Ilość wpisów w listach kontroli dostępu QoS ACL – 600
2. Obsługa:
   1. 256 aktywnych sieci VLAN
   2. 15000 adresów MAC
   3. 16 statycznych tras IPv4
   4. 16 statycznych tras IPv6
   5. 64 interfejsów SVI L3
   6. MTU-L3 9198B
   7. ramek Ethernet Jumbo 10240B
   8. 1024 grupy IGMP
   9. 6 połączeń zagregowanych typu „port channel”
   10. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
3. Porty dostępowe przełącznika posiadają zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
4. Obsługa protokołu NTP
5. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
6. Przełącznik wspiera 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 64 instancji protokołu STP
7. Obsługa protokołu LLDP i LLDP-MED
8. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
9. Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad
10. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
11. Możliwość uruchomienia funkcji serwera DHCP
12. Mechanizmy związane z bezpieczeństwem sieci:
    1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia 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,
13. 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.
14. 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;
15. Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6,
16. Przełącznik umożliwia 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,
17. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),
18. 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,
19. 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;
20. Ukompletowanie urządzenia:
    1. Przełącznik wyposażony jest w następujące wkładki interfejsowe:
       1. 2 x Gigabit Ethernet 1000Base-LX/LH umożliwiający transmisję z wykorzystaniem pojedynczej pary światłowodu jednomodowego (SM).

# PAG – Przełącznik typ 2

1. Rodzaj urządzenia:

- Przełącznik typu standalone wyposażony w 24 porty 1/10/25 Gigabit Ethernet SFP/SFP+/SFP28 oraz 4 porty uplink 40/100 Gigabit Ethernet QSFP

1. Porty SFP/SFP+/SFP28 umożliwiają zastosowanie następujących wkładek interfejsowych:
   1. Gigabit Ethernet 1000Base-T,
   2. Gigabit Ethernet 1000Base-SX,
   3. Gigabit Ethernet 1000Base-LX/LH,
   4. Gigabit Ethernet 1000Base-EX,
   5. Gigabit Ethernet 1000Base-ZX,
   6. Gigabit Ethernet 1000Base-BX-D/U,
   7. 10Gigabit Ethernet 10GBase-SR,
   8. 10Gigabit Ethernet 10GBase-LR,
   9. 10Gigabit Ethernet 10GBase-ER,
   10. 10Gigabit Ethernet 10GBase-ZR,
   11. 10Gigabit Ethernet 10GBase-BX-D/U,
   12. 10Gigabit Ethernet typu twinax (SFP+ - SFP+),
   13. 25Gigabit Ethernet 25GBASE-SR,
   14. 25Gigabit Ethernet typu twinax (SFP28 – SFP28),
   15. 10/25Gigabit Ethernet 10/25GBASE-CSR (MMF),
   16. 10/25Gigabit Ethernet 10/25GBASE-LR (SMF);
2. Porty QSFP umożliwiają zastosowanie następujących modułów interfejsowych:

3.1.Dla transmisji 40Gb/s:

* 1. 40G-SR4,
  2. 40G-LR4,
  3. 40G-ER4,
  4. 40G-SR-BD,
  5. 40G-CSR,
  6. 40G-CSR4,
  7. 40G-LR4-Lite (zasięg 2 km dla światłowodu SMF G.652),
  8. adapter 40G QSFP->10G SFP+,
  9. 40Gigabit Ethernet typu twinax (QSFP - QSFP);

3.2.Dla transmisji 100Gb/s:

* 1. 100GBASE-SR4,
  2. 100GBASE-LR4,
  3. 100Gigabit Ethernet typu twinax (QSFP - QSFP);

1. Architektura:
   1. Urządzenie jest wyposażone w wymienne moduły wentylatorów
   2. Urządzenie może zostać wyposażone w zasilacz redundantny do pracy w trybie 1:1
2. Wydajność:
   1. Urządzenie posiadana 32MB bufor pamięci,
   2. 16GB pamięci DRAM i 16GB pamięci flash,
   3. Przepustowość przełącznika (switching capacity) wynosi 1.6 Tbps,
   4. Prędkość przesyłania (forwarding rate) wynosi 1 miliard pps (1Bpps),
3. Obsługa:
   1. 1000 aktywnych sieci VLAN,
   2. 80 000 adresów MAC,
   3. 212 000 tras IPv4,
   4. 212 000 tras IPv6,
   5. Ilość wpisów w listach kontroli dostępu Security ACL – 27 000,
   6. ilość wpisów w listach kontroli dostępu QoS ACL – 16 000,
   7. 1000 interfejsów SVI L3,
   8. Jumbo frame 9198B,
   9. 128 połączeń zagregowanych typu „port channel”,
   10. 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
4. 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 umożliwia wgrywanie poprawek bez konieczności restartowania platformy,
   5. System operacyjny przełącznika jest 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 realizuje 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 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 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (priviledge-level),
   13. Autoryzacja prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+,
   14. Obsługa list kontroli dostępu (ACL) następujących typów:
       1. Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika,
       2. VLAN ACL umożliwiające kontrolę ruchu pomiędzy stacjami znajdującymi się w tej samem sieci VLAN w obrębie przełącznika,
       3. Routed ACL umożliwiające kontrolę ruchu routowanego pomiędzy sieciami VLAN,
       4. Możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia);
   15. Przełącznik realizuje następujące mechanizmy związane z zapewnieniem, jakości usług w sieci:
       1. 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
       2. Implementacja algorytmu Shaped Round Robin lub podobnego 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;
   16. Przełącznik posiada 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 realizuje routing statyczny i dynamiczny dla IPv4 i IPv6 w zakresie:
       1. Routing statyczny dla IPv4 i IPv6,
       2. Routing dynamiczny dla IPv4: BGP, ISIS,
       3. Routing dynamiczny dla IPv4: OSPF, EIGRP (rfc7868) wraz z obsługą mechanizmu IP FRR (Fast Reroute) Loop Free Alternate (LFA),
       4. Routing dynamiczny dla IPv6: OSPFv3,
       5. Funkcjonalności Policy-based routing,
       6. multicast routing (PIM-SM, PIM-SSM) ,
       7. Obsługa protokołu redundancji bramy (VRRP) z obsługą 255 grup,
       8. Obsługa 200 tuneli GRE (Generic Routing Encapsulation),
       9. Obsługa 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 realizuje protokołu LISP zgodnie z RFC 6830,
   22. Urządzenie umożliwia enkapsulację ruchu przy pomocy VXLAN’ów,
   23. Wsparcie dla BGP EVPN z wykorzystaniem VXLAN w zakresie min. funkcjonalności węzłów leaf / spine / border
   24. 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
   25. Urządzenie jest 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
   26. Klastrowanie wspiera funkcję eliminacji przesyłania ruchu BUM (Broadcast, unknown-unicast and multicast traffic) poprzez połączenie realizujące klaster pomiędzy przełącznikami
   27. Przełącznik umożliwia 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
   28. 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)
   29. 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
   30. Przełącznik posiada funkcjonalność umożliwiającą przechwytywanie ruchu z wybranych interfejsów fizycznych urządzenia i generowanie plików typu „pcap” do dalszej analizy przy pomocy oprogramowanie zewnętrznego
   31. Wbudowany analizator pakietów,
   32. 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
   33. Możliwość dynamicznego załadowania do przełącznika polityki kontroli ruchu pracującej w oparciu o znaczniki bezpieczeństwa (secure tag) z centralnego systemu zarządzania kontrolą dostępu,
   34. 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,
   35. Urządzenie umożliwia uruchamianie dodatkowych aplikacji w kontenerach Docker,
   36. Urządzenie może zostać wyposażone w zewnętrzną pamięć przeznaczoną np. do wykorzystania przez aplikacje uruchomiane w kontenerach Docker w postaci dysku M2 SATA o pojemności 240/480/960GB,
   37. Możliwość realizacji funkcji kontrolera dla radiowych punktów dostępowych WiFi z obsługą do 200 AP oraz 4000 klientów bezprzewodowych poprzez dokupienie dodatkowych licencji.
   38. 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,
5. Urządzenie realizuje następujące funkcjonalności z zakresu MPLS:
   1. L2VPN - Ethernet over MPLS (EoMPLS) – obsługa do 1000 połączeń wirtualnych VC
   2. L2VPN - Virtual Private LAN Services (VPLS) - obsługa 1000 wirtualnych instancji (VFI), 32 sąsiadów w ramach jednej instancji
   3. L3 VPN - MPLS Virtual Private Network (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
6. Zarządzanie i konfiguracja:
   1. Urządzenie realizuje sprzętowo tworzenie statystyk ruchu w oparciu o pełen NetFlow (bez próbkowania), wielkość tablicy monitorowanych strumieni wynosi 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 posiada 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 posiada port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB,
   6. Urządzenie jest wyposażone w port konsoli USB,
   7. Urządzenie umożliwia 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 posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą i identyfikacji konkretnego urządzenia,
   10. Przełącznik posiada 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
7. Obudowa:

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

1. Przełącznik wyposażony jest w zasilacz redundantny identyczny jak zasilacz podstawowy
2. Ukompletowanie urządzenia:
   1. Każdy przełącznik wyposażony jest w następujące wkładki interfejsowe:
      1. 12 x Gigabit Ethernet 1000Base-LX/LH umożliwiający transmisję z wykorzystaniem pojedynczej pary światłowodu jednomodowego (SM) zakończony konektorem LC.
      2. 4 x Moduł optyczny QSFP28 umożliwiający transmisję z wykorzystaniem pojedynczej pary światłowodu jednomodowego (SM), prędkość transmisji 100Gb o zasięgu pracy 500m SMF (G.652) zakończony konektorem LC.

# RTR - Router

1. Posiada co najmniej 8 interfejsów 10 GE i co najmniej 8 interfejsów 1 GE. Wszystkie interfejsy są definiowane za pomocą wkładek typu SFP/SFP+.
2. Urządzenie modularne umożliwiające posiadające slot na moduł rozszerzeń umożliwiający rozbudowę urządzenia o dodatkowe interfejsy 10GE/40GE/100GE
3. Przepustowość urządzenia nie mniejsza niż 44Gbps z możliwością jej zwiększania do 100Gbps
4. Wydajność routingu mierzona dla ruchu IPv4 (pakiety 64 bajtowe) nie mniejsza niż 78Mpps
5. Urządzenie posiada dedykowany akcelerator kryptograficzny osiągający wydajność 8 Gbps dla ruchu IMIX z możliwością dalszego zwiększania wydajności do 25Gbps poprzez zakup dodatkowej licencji bez konieczności rozbudowy sprzętowej
6. Urządzenie posiada 16GB pamięci RAM
7. Urządzenie obsługuje 3 000 000 prefiksów w tablicach routingu IPv4
8. Urządzenie obsługuje 3 000 000 prefiksów w tablicach routingu IPv6
9. Urządzenie obsługuje co najmniej 50 000 prefiksów w tablicach routingu multicast i co najmniej 1000 grup.
10. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv4: OSPF, ISIS, BGP
11. Urządzenie obsługuje następujące protokoły routingu dynamicznego dla IPv6: OSPFv3, ISIS, BGP
12. Urządzenie obsługuje Policy Based Routing, w tym także routing oparty o pomiar parametrów łącza (opóźnienie, obciążenie, jitter)
13. Obsługa 8000 instancji VRF
14. Bidirectional Forwarding Detection (BFD) ze wsparciem dla protokołów BGP, OSPF, IS-IS, routingu statycznego
15. Urządzenie obsługuje funkcjonalność BFD dla interfejsów skonfigurowanych do współpracy z VRF
16. Urządzenie obsługuje multicast, w szczególności: PIM sparse/dense/SSM, IGMP, MLD, Multicast VPN
17. Funkcjonalności związane z niezawodnością pracy:
    1. IP FRR
    2. BGP Prefix-Independent Convergence (PIC)
    3. Graceful Restart dla OSPF, BGP, ISIS, LDP, RSVP
    4. funkcjonalność VRRP
18. Obsługa MPLS, w szczególności:
    1. LDP
    2. EoMPLS, VPLS
    3. MPLS L3 VPN
    4. MPLS TE
    5. MPLS FRR w trybach protekcji łącza oraz węzła
19. Urządzenie obsługuje następujące mechanizmy jakości usług (QoS):
    1. klasyfikacja, kolejkowanie, oznaczanie, policing, shaping per port/VLAN zarówno dla IPv4 jak i IPv6
    2. hierarchiczny QoS (H-QoS) - 3 poziomy
    3. dynamiczna alokacja kolejek
    4. możliwość obsługi jednej kolejki z priorytetem w stosunku do innych
    5. mechanizm ograniczania ilości ruchu w kolejce priorytetowej
    6. możliwość ograniczania pasma wejściowego dostępnego na danym porcie dla ruchu o danej klasie obsługi (ingress policing, rate limiting)
    7. mechanizm WRED
    8. możliwość wykorzystania rodzajów aplikacji/ruchu aplikacyjnego w tworzeniu polityk QoS
20. Urządzenie obsługuje następujące funkcje i elementy bezpieczeństwa:
    1. sprzętowa ochrona warstwy zarządzającej (Control Plane Policing), ze wsparciem dla list kontroli dostępu
    2. Unicast RPF (Reverse Path Forwarding)
    3. listy kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL
    4. obsługa 4000 list kontroli dostępu (ACL) – z liczbą wpisów nie mniejszą niż 50 000 wpisów dla IPv4 / 25 000 wpisów dla IPv6 dla wszystkich list ACL
    5. dostęp administracyjny oparty o role z przypisanymi uprawnieniami
    6. ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU
    7. logowanie pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU
21. Funkcjonalność zapory ogniowej typu statefull (ang. statefull firewall), przy czym zapora ogniowa:
    1. umożliwia definicję stref bezpieczeństwa (zone-based firewall) z elastyczną definicją scenariuszy przesyłu ruchu pomiędzy różnymi strefami (inspekcja ruchu, odrzucanie ruchu, brak inspekcji)
    2. obsługuje ruch IPv4 oraz IPv6
    3. umożliwia konfigurację polityk per wirtualna tablica routingu (VRF)
    4. umożliwia obsługę 6 000 000 równoczesnych sesji
22. Możliwość obsługi połączeń VPN:
    1. sieci VPN typu site-to-site oparte o IPSec (8000 tuneli)
    2. dynamiczne zestawianie VPN z wykorzystaniem protokołu NHRP (ang. Next Hop Resolution Protocol) w relacji spoke to spoke w celu optymalizacji transmisji danych pomiędzy oddziałami
    3. beztunelowe sieci VPN w relacji każdy z każdym w celu zapewnienia optymalnej transmisji pomiędzy dowolnymi węzłami oraz optymalnej realizacji polityk jakości usług (QoS) i transmisji multicast. Obsługa protokołu GDOI (RFC 3547)
    4. algorytmy IPSec nowej generacji oparte o algorytmy Suite B (RFC 4869), w szczególności:
       1. Elliptic Curve Diffie-Hellman (ECDH)
       2. Galois Counter Mode Advanced Encryption Standard (GCM-AES) - 128/256 bitów
       3. Galois Message Authentication Code (GMAC-AES) - 128/256 bitów
       4. Elliptic Curve Digital Signature Algorithm (ECDSA) dla IKEv2
    5. konfiguracja tuneli IPSec VPN w oparciu o protokół IKEv2 dla ruchu IPv4 i IPv6, site-to-site, jak i dynamicznych
    6. funkcjonalność VPN per VRF
23. Urządzenie ma możliwość rozszerzenia funkcjonalności (poprzez zakup odpowiedniej licencji) o obsługę MACSec na wbudowanych portach GE i 10GE
24. Obsługa 4000 tuneli GRE z zapewnianiem mechanizmu honorowania IP Precendence dla ruchu tunelowanego
25. W ramach funkcjonalności zarządzania, urządzenie:
    1. umożliwia zarządzanie poprzez: CLI (Telnet, SSHv2, port konsoli), SNMPv3
    2. obsługuje Ethernet OAM (IEEE 802.3ah, IEEE 802.1ag, ITU-T Y.1731)
    3. obsługuje MPLS OAM
    4. umożliwia pisanie skryptów konfiguracyjnych
    5. obsługuje protokół Netflow ze wsparciem dla multicast oraz IPv4/IPv6
    6. posiada narzędzia IP SLA umożliwiające pomiar parametrów jakościowych łącza (np. czas odpowiedzi aplikacji/serwera, opóźnienie, jitter, straty pakietów) i dostęp do tych informacji za pomocą SNMP
    7. posiada obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS i TACACS+
    8. posiada dedykowane porty do zarządzania urządzeniem: port konsoli (RJ45 i USB), port Ethernet 10/100/1000 oraz port AUX
    9. posiada 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
    10. urządzenie posiada możliwość wyszukiwania fragmentów konfiguracji z linii poleceń urządzenia, dzięki stosowaniu wyrażeń-filtrów
26. Urządzenie posiada zintegrowane redundantne zasilacze AC 230V
27. Urządzenie umożliwia montaż w szafie 19”, wysokość 2RU.
28. Każdy router wyposażony jest w następujące wkładki interfejsowe:
    1. 8 x Gigabit Ethernet 1000Base-LX/LH umożliwiający transmisję z wykorzystaniem pojedynczej pary światłowodu jednomodowego (SM) zakończony konektorem LC.
    2. 8 x moduł SFP+ o prędkości 10Gb umożliwiający połączenie z wykorzystaniem pojedynczej pary światłowodów jednomodowych (SM) zakończony konektorem LC.

# FWPA – Next Generation Firewall

1. System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance) lub w formie maszyny wirtualnej. W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
2. System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 35 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 18 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 8 mln. jednoczesnych połączeń.
3. System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 100/1000/10000, 16 portów 1Gbps SFP/10Gps SFP+ oraz 4 porty 40Gbps/100Gb QSFP/QSFP28.
4. System zabezpieczeń firewall musi działać w trybie rutera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych jak również nie może wprowadzać segmentacji sieci na odrębne domeny kolizyjne w sensie Ethernet/CSMA.
5. Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
6. System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
7. System zabezpieczeń firewall musi obsługiwać nie mniej niż 20 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF. Nie jest wymagana licencja na obsluge wirtualnych routerów nie mniej niż 20).
8. System zabezpieczeń firewall zgodnie z ustaloną polityką musi prowadzić kontrolę ruchu sieciowego pomiędzy obszarami sieci (strefami bezpieczeństwa) na poziomie warstwy sieciowej, transportowej oraz aplikacji (L3, L4, L7).
9. Polityka zabezpieczeń firewall musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, kategorie URL, użytkowników aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasma sieci (minimum priorytet, pasmo gwarantowane, pasmo maksymalne, oznaczenia DiffServ).
10. System zabezpieczeń firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege”, tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi które w regułach polityki bezpieczeństwa firewall są wskazane jako dozwolone.
11. System zabezpieczeń firewall musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
12. Identyfikacja aplikacji nie może wymagać podania w konfiguracji urządzenia numeru lub zakresu portów na których dokonywana jest identyfikacja aplikacji. Należy założyć, że wszystkie aplikacje mogą występować na wszystkich 65 535 dostępnych portach. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 35 Gbit/s.
13. Zezwolenie dostępu do aplikacji musi odbywać się w regułach polityki firewall (tzn. reguła firewall musi posiadać oddzielne pole gdzie definiowane są aplikacje i oddzielne pole gdzie definiowane są protokoły sieciowe, nie jest dopuszczalne definiowane aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).
14. Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
15. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
16. System zabezpieczeń firewall musi wykrywać co najmniej 2300 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
17. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
18. System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.
19. System zabezpieczeń firewall musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, dll, doc, szyfrowany doc, docx, ppt, szyfrowany ppt, pptx, xls, szyfrowany xls, xlsx, rar, szyfrowany rar, zip, szyfrowany zip, exe, gzip, hta, mdb, mdi, ocx, pdf, pgp, pif, pl, reg, sh, tar, text/html, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.
20. System zabezpieczeń firewall musi pozwalać na analizę i blokowanie plików przesyłanych w zidentyfikowanych aplikacjach. W przypadku gdy kilka aplikacji pracuje na tym samym porcie UDP/TCP (np. tcp/80) musi istnieć możliwość przydzielania innych, osobnych profili analizujących i blokujących dla każdej aplikacji.
21. System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download” poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj” dla funkcji blokowania transmisji plików.
22. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej HTTPS (HTTP szyfrowane protokołem SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie) oraz ruchu przychodzącego do serwerów firmy. System musi mieć możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
23. System zabezpieczeń firewall musi zapewniać inspekcję komunikacji szyfrowanej protokołem SSL dla ruchu innego niż HTTP. System musi mieć możliwość deszyfracji niezaufanego ruchu SSL i poddania go właściwej inspekcji, nie mniej niż: wykrywanie i kontrola aplikacji, wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-wirus i any-spyware), filtracja plików, danych i URL.
24. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
25. System zabezpieczeń posiada wbudowaną i automatycznie aktualizowaną przez producenta listę serwerów dla których niemożliwa jest deszyfracja ruchu (np. z powodu wymuszania przez nie uwierzytelnienia użytkownika z zastosowaniem certyfikatu lub stosowania mechanizmu „certificate pinning”). Lista ta stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
26. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
27. Wymagania podstawowe identyfikacja użytkowników
28. System zabezpieczeń firewall musi zapewniać możliwość transparentnego ustalenia tożsamości użytkowników sieci (integracja z Active Directory, Ms Exchange, Citrix, LDAP i serwerami Terminal Services). Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.
29. System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
30. System zabezpieczeń firewall musi odczytywać oryginalne adresy IP stacji końcowych z pola X-Forwarded-For w nagłówku http i wykrywać na tej podstawie użytkowników z domeny Windows Active Directory generujących daną sesje w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.
31. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
32. Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day
33. System zabezpieczeń firewall musi posiadać możliwość rozszerzenia licencyjnego o moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.
34. System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
35. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
36. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
37. System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
38. System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
39. System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
40. System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
41. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
42. System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
43. System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
44. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
45. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
46. System zabezpieczeń firewall musi posiadać funkcję podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
47. System zabezpieczeń firewall musi posiadać funkcję automatycznego pobierania, z zewnętrznych systemów, adresów, grup adresów, nazw dns oraz stron www (url) oraz tworzenia z nich obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
48. System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
49. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
50. System zabezpieczeń firewall musi posiadać możliwość rozbudowy o moduł przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 9 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
51. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
52. Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.
53. System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak aby administrator miał możliwość sprawdzenia które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
54. Wymagania NAT, DoS, IPSEC VPN, SSL VPN, QoS
55. System zabezpieczeń firewall musi wykonywać statyczną i dynamiczną translację adresów NAT. Mechanizmy NAT muszą umożliwiać co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
56. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
57. System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
58. System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
59. System zabezpieczeń firewall musi umożliwiać inspekcję (bez konieczności zestawiania) tuneli GRE i nieszyfrowanych AH IPSec w celu zapewnienia widoczności i wymuszenia polityk bezpieczeństwa, DoS i QoS dla ruchu przesyłanego w tych tunelach.
60. System zabezpieczeń firewall musi umożliwiać rozbudowę modułów o konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.
61. System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentiaction) do wybranych zasobów. Polityki definiujące powinny umożliwiać wykorzystanie adresów źródłowych, docelowych, użytkowników, numerów portów usług oraz kategorie URL. Minimalne wymagane mechanizmy uwierzytelnienia to: RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0.
62. System zabezpieczeń firewall musi wykonywać zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. System musi umożliwiać stworzenie co najmniej 8 klas dla różnego rodzaju ruchu sieciowego.
63. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
64. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
65. Wymagania dla środowiska wirtualnego vmware
66. System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
67. Wymagania zarządzanie i raportowanie
68. Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.
69. System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
70. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
71. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
72. System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
73. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji). System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach.
74. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
75. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
76. System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 2 TB działający w trybie RAID1. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
77. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
78. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
79. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
80. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
81. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
82. System zabezpieczeń firewall pozwalać na korelowanie zbieranych informacji oraz budowania raportów na ich podstawie. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, aplikacjach, zagrożeniach i filtrowaniu stron www.
83. System zabezpieczeń firewall pozwalać na tworzenie wielu raportów dostosowanych do wymagań Zamawiającego, zapisania ich w systemie i uruchamiania w sposób ręczny lub automatyczny w określonych przedziałach czasu. Wynik działania raportów musi być dostępny w formatach co najmniej PDF, CSV i XML.
84. System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
85. System zabezpieczeń firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive lub Active-Active. Moduł ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
86. Dostarczone rozwiązanie musi składać się z kompletu dwóch identycznych urządzeń, działającym w trybie wysokiej dostępności Active-Passive.
87. Jeżeli jest taka możliwość, dostarczone licencję powinny być dostarczone w modelu dla środowiska klastra dwóch urządzeń działających w trybie Active-Passive
88. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.