Nr. postępowania 5/2018/pn
BR-VII-2121-7-18

Załącznik nr 4 do SIWZ

„Dostawa routerów i sprzętu komputerowego dla Biblioteki Raczyńskich w Poznaniu z podziałem na dwie części"

Opis Przedmiotu Zamówienia dla części I

1. Router UTM z zestawem licencji - 2 sztuki

Wdrożenie:

- przygotowanie projektu technicznego oraz harmonogramu planowanych prac
- dostawa, montaż 2 szt. firewalli w Bibliotece Raczyńskich w Poznaniu, w szczególności:
  - wykonanie instalacji oraz pełnej konfiguracji dostarczonych firewalli, w tym przeniesienie funkcjonalności obecnie użytkowanego firewalla Zamawiającego oraz wdrożenie nowych funkcjonalności zgodnie z zaleceniami Zamawiającego
  - utworzenie infrastruktury w sposób zapewniający redundancję połączeń logicznych w ramach dostarczonych elementów
  - konfiguracja klastra firewalli HA wraz z monitoringiem dla poprawnego działania klastra oraz minimalizacji przerwy w działaniu usług w przypadku HA failover
  - wdrożenie inspekcji ruchu szyfrowanego. Konfiguracja CA w powiązaniu z Active Directory oraz wygenerowanie certyfikatów z infrastruktury Zamawiającego na potrzeby inspekcji.
  - wdrożenie autentykacji użytkowników SSO, integracja firewalli z usługami katalogowymi Active Directory
  - konfiguracja minimum 1 redundantnego tunelu VPN site-to-site do jednostek zdalnych. Ruch w kierunku internetu z jednostek zdalnych należy poddawać inspekcji na klasterze firewalli
  - skonfigurowanie firewalla wraz z wydzieleniem VLAN-ów. Ruch w sieci LAN należy poddawać inspekcji na klastrze firewalli
  - konfiguracja klienckiego połączenia VPN wraz z integracją z usługami katalogowymi Active Directory oraz konfiguracją urządzeń końcowych
  - konfiguracja polityk dostępu do internetu oraz pomiędzy lokalnymi podsieciami zgodnie z zaleceniami Zamawiającego
  - konfiguracja polityk IPS, DDoS, Web filteringu, DLP, kontroli aplikacji dostosowanych do środowiska Zamawiającego oraz zgodnie z wytycznymi Zamawiającego
  - wdrożenie redundantnego połączenia WAN. Rozkład ruchu do internetu musi następować automatycznie w zależności od jakości połączeń
  - konfiguracja przesyłania do analizy zagrożeń nieznanych
- dostawa, montaż w Bibliotece Raczyńskich w Poznaniu 1 szt. przełącznika, w szczególności:
  - skonfigurowanie przełącznika wraz z wydzieleniem VLAN-ów itp.
  - utworzenie infrastruktury w sposób zapewniający redundancję połączeń logicznych w ramach dostarczonych elementów
- wykonanie testów akceptacyjnych
- wykonanie oraz przekazanie dokumentacji powykonawczej zawierającej szczegółowy opis oraz konfiguracje urządzeń
- zapewnienie szkolenia dla min. dwóch osób, które pozwoli na uzyskanie wiedzy teoretycznej oraz praktycznych umiejętności niezbędnych w administrowaniu dostarczonymi urządzeniami
- wsparcie powdrożeniowe przez okres 2 miesięcy po zakończeniu wdrożenia
- prace wdrożeniowe nie mogą zakłócać ciągłości funkcjonowania Biblioteki

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Informacje ogólne	Rozwiązanie musi być dostępne jako platforma sprzętowa. Urządzenie jest nielimitowane na użytkowników. Urządzenie musi być fabrycznie nowe. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych,

		komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
2.	Redundancja, monitoring i wykrywanie awarii	W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. W ramach postępowania system musi zostać dostarczony w postaci redundantnej. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.
3.	Parametry sprzętowe	System realizujący funkcję Firewall musi dysponować minimum: • 18 portami Gigabit Ethernet RJ-45. • 16 gniazdami SFP 1 Gbps. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System musi być wyposażony w zasilanie AC.
4.	Parametry wydajnościowe	W zakresie Firewall'a obsługa nie mniej niż 4 mln jednoczesnych połączeń oraz 300.000 nowych połączeń na sekundę. Przepustowość Stateful Firewall: nie mniej niż 32 Gbps dla pakietów 512 B. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 64 B. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 7 Gbps. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 20 Gbps. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 3 Gbps. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6.8 Gbps.
5.	Funkcje systemu bezpieczeństwa	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych: 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP. 8. Zarządzanie pasmem (QoS, Traffic shaping).

		9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11. Analiza ruchu szyfrowanego protokołem SSL. 12. Analiza ruchu szyfrowanego protokołem SSH.
6.	Polityki, Firewall	Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
7.	Połączenia VPN	System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać: • Wsparcie dla IKE v1 oraz v2. • Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19 i 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling" dla połączeń Client-to-Site. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać: • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
8.	Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.
9.	Zarządzanie pasmem	System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
10.	Kontrola Antywirusowa	Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
11.	Ochrona przed atakami	Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana

		automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
12.	Kontrola aplikacji	Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
13.	Kontrola WWW	Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
14.	Uwierzytelnianie użytkowników w ramach sesji	System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
15.	Zarządzanie	Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
16.	Logowanie	System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub

		programowej. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Musi istnieć możliwość logowania do serwera SYSLOG.
17.	Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall. • ICSA lub NSS Labs dla funkcji IPS. • ICSA dla funkcji IPSec VPN. • ICSA dla funkcji SSL VPN.
18.	Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: • Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.
19.	Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres min. 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

2. Przełącznik 24-portowy – 1 sztuka

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne
1.	Wymagania podstawowe	Przełącznik posiadający 24 porty 10/100/1000BASE-T, 8 portów 1 Gigabit Ethernet SFP oraz 4 dedykowane porty 10 Gigabit Ethernet SFP+ Możliwość instalacji dodatkowego modułu 2 portów 10 Gigabit Ethernet SFP+ Możliwość instalacji dodatkowego modułu 2 portów 40GBASE-X QSFP+ Wysokość urządzenia 1U Nieblokująca architektura o wydajności przełączania min. 296 Gb/s Szybkość przełączania min. 220 Milionów pakietów na sekundę Możliwość instalacji modułów stakujących zapewniających przepustowość 80 lub 160 Gb/s. Możliwość stakowania switchy z wykorzystaniem portów 10 Gigabit Ethernet SFP+ Tablica MAC adresów min. 96k Pamięć operacyjna: min. 1GB pamięci DRAM Pamięć flash: min. 4GB pamięci Flash Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094 Obsługa sieci wirtualnych protokołowych IEEE 802.1v Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów) Obsługa Q-in-Q IEEE 802.1ad Obsługa Quality of Service: • IEEE 802.1p • DiffServ • 8 kolejek priorytetów na każdym porcie wyjściowym Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB Obsługa LLDP Media Endpoint Discovery (LLDP-MED) Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. Możliwość instalacji redundantnego zasilacza. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika. Wbudowany DHCP Serwer i klient

		Możliwość instalacji min. dwóch wersji oprogramowania Możliwość przechowywania min. kilkunastu wersji oprogramowania
2.	Obsługa Routingu IPv4	Sprzętowa obsługa routingu IPv4 – forwarding Pojemność tabeli routingu min. 12 tys. wpisów Routing statyczny Obsługa routingu dynamicznego IPv4: • RIPv1/v2 • OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania • BGPv4 – możliwość rozszerzenia przez licencję oprogramowania • IS-IS – możliwość rozszerzenia przez licencję oprogramowania
3.	Obsługa Routingu IPv6	Sprzętowa obsługa routingu IPv6 – forwarding Pojemność tabeli routingu min. 6 tys. wpisów Routing statyczny Obsługa routingu dynamicznego dla IPv6: • RIPng • OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania • IS-IS Telnet Server dla IPv6 SSH2 Server dla IPv6 Ping dla IPv6 Tracert dla IPv6 Obsługa 6to4 (RFC 3056) Obsługa MLDv1 (Multicast Listener Discovery version 1) Obsługa MLDv2 (Multicast Listener Discovery version 2)
4.	Obsługa Multicastów	Statyczne przyłączenie do grupy multicast Filtrowanie IGMP Obsługa PIM-SM - możliwość rozszerzenia przez licencję oprogramowania Obsługa PIM-DM – możliwość rozszerzenia przez licencję oprogramowania Obsługa PIM-SSM – możliwość rozszerzenia przez licencję oprogramowania Obsługa Multicast VLAN Registration - MVR Obsługa IGMP v1 (RFC 1112) Obsługa IGMP v2 (RFC 2236) Obsługa IGMP v3 (RFC 3376) Obsługa IGMP v1/v2/v3 snooping Możliwość konfiguracji statycznych tras dla Routingu Multicastów
5.	Bezpieczeństwo	Obsługa Network Login: • IEEE 802.1x - RFC 3580 • Web-based Network Login • MAC based Network Login Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants) Możliwość integracji funkcjonalności Network Login z Microsoft NAP Przydział sieci VLAN, ACL/QoS podczas logowania Network Login Obsługa Guest VLAN dla IEEE 802.1x Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication Obsługa Identity Management Wbudowana obrona procesora urządzenia przed atakami DoS Obsługa TACACS+ (RFC 1492) Obsługa RADIUS Authentication (RFC 2138) Obsługa RADIUS Accounting (RFC 2139) RADIUS Per-command Authentication Bezpieczeństwo MAC adresów: • ograniczenie liczby MAC adresów na porcie

		• zatrzaśnięcie MAC adresu na porcie Możliwość wyłączenia MAC learning Obsługa SNMPv1/v2/v3 Klient SSH2 Zabezpieczenie przełącznika przed atakami DoS: • Networks Ingress Filtering RFC 2267 • SYN Attack Protection • Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4: • Adres MAC źródłowy i docelowy plus maska • Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6 • Protokół – np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd. • Numery portów źródłowych i docelowych TCP, UDP • Zakresy portów źródłowych i docelowych TCP, UDP • Identyfikator sieci VLAN – VLAN ID • Flagi TCP • Obsługa fragmentów Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania Obsługa bezpiecznego transferu plików SCP/SFTP Obsługa DHCP Option 82 Obsługa IP Security - Gratuitous ARP Protection Obsługa IP Security - Trusted DHCP Server Obsługa IP Security - DHCP Secured ARP/ARP Validation Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s
6.	Bezpieczeństwo sieciowe	Możliwość konfiguracji portu głównego i zapasowego Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania Obsługa STP (Spinning Tree Protocol) IEEE 802.1D Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s Obsługa PVST+ Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619 Obsługa G.8032 v1/v2 Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.
7.	Zarządzanie	Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol) Obsługa synchronizacji czasu NTP Zarządzanie przez SNMP v1/v2/v3 Zarządzanie przez przeglądarkę WWW – protokół http i https Możliwość zarządzania poprzez protokół XML Telnet Serwer dla IPv4 / IPv6 SSH2 Serwer dla IPv4 / IPv6 Ping dla IPv4 / IPv6 Traceroute dla IPv4 / IPv6 Obsługa SYSLOG z możliwością definiowania wielu serwerów Sprzętowa obsługa sFlow Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757) Obsługa RMON2 (RFC 2021) Obsługa IPFix
8.	Inne	Obsługa skryptów TCL/Tk

		Zakres temperatury pracy 0-50 °C Obsługa skryptów CLI Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych) Obsługa OpenFlow – możliwość rozszerzenia przez licencje Obsługa AVB (Audio Video Bridging) - możliwość rozszerzenia przez licencje Możliwość uruchamiania skryptów: • Ręcznie • określonym czasie lub co wskazany okres czasu – możliwość rozszerzenia przez licencję oprogramowania • Na podstawie wpisów w logu systemowym – możliwość rozszerzenia przez licencję oprogramowania Switch objęty rocznym serwisem z wymianą sprzętu w trybie NBD