Z2.2

Nazwa przedmiotu zamówienia: Zakup i dostawa sprzętu oraz oprogramowania niezbędnego do realizacji projektu Podkarpackie e-biblioteki pedagogiczne

Numer referencyjny sprawy: PBWR-7/2018/PEBP

Część: 2. Dostawa sprzętu sieciowego

Szczegółowy opis przedmiotu zamówienia

Zakup i dostawa sprzętu oraz oprogramowania niezbędnego do realizacji projektu Podkarpackie e-biblioteki pedagogiczne w niniejszym postępowaniu dofinansowany jest w ramach Regionalnego Programu Operacyjnego Województwa Podkarpackiego na lata 2014-2020 działanie 2.1 Podniesienie efektywności i dostępności e-usług, konkurs nr RPPK.02.01.00-IZ.00-18-002/16.

Dostarczony sprzęt musi być fabrycznie nowy, nieużywany, pochodzący z legalnego kanału dystrybucji. Data produkcji sprzętu nie może być wcześniejsza niż 6 miesięcy przed dostawą. Oprogramowanie nie może być wcześniej aktywowane i używane. Licencje wystawione na zamawiającego. Użytkownikiem końcowym będzie:

Pedagogiczna Biblioteka Wojewódzka w Rzeszowie
ul. Gałęzowskiego 4
35-074 Rzeszów

1. Dostawa firewalli – sztuk 2

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
1	Podstawowe	System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). 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	Wydajność	Przepływność w ruchu full-duplex nie mniej niż 900 Mbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji. Nie mniej niż 600 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering). Obsługiwać nie mniej niż 120 000 jednoczesnych połączeń.
3	Porty	8 portów ethernet w tym minimum: • 4 porty Ethernet 10/100/1000 Base-T, • 4 porty 1Gbps SFP.
4	Tryby pracy	Tryb rutera (tzn. w warstwie 3 modelu OSI). Tryb przełącznika (tzn. w warstwie 2 modelu OSI). Tryb transparentny. Tryb pasywnego nasłuchu (sniffer).

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		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. 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.).
5	Podstawowe funkcje	Obsługa protokołu 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. System zabezpieczeń firewall musi obsługiwać nie mniej niż 5 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. 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). 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). 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. 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. 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. 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). Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall. Firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. Firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		Firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. 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. 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. Firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików. 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. 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. Firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa. Wbudowana i automatycznie aktualizowana 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 powinna stanowić automatyczne wyjątki od ogólnych reguł deszyfracji. Musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
6	Identyfikacja użytkowników	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. 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

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników. 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. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
7	Ochrona IPS, AV, anty-spyware, URL, zero-day	Firewall musi posiadać 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. Możliwość uruchomienia filtrowania stron WWW per reguła polityki bezpieczeństwa firewall. Możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa. Możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. 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 przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny. Moduł inspekcji antywirusowej powinien być uruchamiany per reguła polityki bezpieczeństwa firewall. Firewall musi posiadać moduł wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny. Moduł IPS/IDS powinien być uruchamiany per reguła polityki bezpieczeństwa firewall. Firewall musi posiadać moduł anty-spyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny. Moduł anty-spyware powinien być uruchamiany per reguła polityki bezpieczeństwa firewall. Firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe. Funkcja 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) 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.

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
8	Funkcje NAT, DoS, IPSEC VPN, SSL VPN, QoS	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. Firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa. Funkcja ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP. 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). Firewall musi umożliwiać utworzenie minimum 25 tuneli IPSec site-to-site z posiadanymi przez Zamawiającego routerami Cisco 1921 ISR, z następującymi ustawieniami: • ESP, Encryption: 3DES, Authentication: SHA1 • ESP, Encryption: AES-256, Authentication: SHA256. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. 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. Firewall musi umożliwiać 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. 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. 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. Kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
9	Zarządzanie i raportowanie	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.

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		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. Uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos. Musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS). Firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240GB. 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. Urządzenie musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu. System musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa. Selektywne wysyłanie logów bazując na ich atrybutach. Firewall musi 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. Firewall musi 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. 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.
10	Obudowa	Musi mieć możliwość montażu w szafie 19”, należy dołączyć niezbędne akcesoria.
11	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
12	Gwarancja	Minimum 36 miesięcy realizowana w miejscu instalacji sprzętu, z czasem reakcji do końca następnego dnia roboczego. Gwarancja musi obejmować wszystkie wymienione funkcje minimum przez okres gwarancji.

2. Dostawa routerów – sztuk 2

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
1	Router	Router o budowie modularnej LAN/WAN.
2	Architektura	Musi pozwalać na instalację co najmniej: • 3 kart sieciowych z interfejsami, • 1 wewnętrznego modułu DSP Sloty urządzenia przewidziane pod rozbudowę o dodatkową kartę sieciową muszą mieć możliwość obsadzenia kartami: • z portami szeregowymi o gęstości co najmniej 4 porty na moduł,

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		• z interfejsem ISDN PRI o gęstości 1 portu per moduł, 2 portów per moduł, 4 portów per moduł, • przełącznika Ethernet co najmniej 8-portowego, w tym również ze wsparciem dla POE • z co najmniej dwoma portami Gigabit Ethernet SFP • umożliwiającym komunikację do sieci komórkowej w technologii 3G/4G (LTE) • umożliwiającymi instalację dysków SSD
3	Porty	Urządzenie musi być wyposażone w 4 interfejsy Gigabit Ethernet 10/100/1000BaseT Możliwość obsługi minimum 2 łączy światłowodowych poprzez moduły SFP, wymagana obsługa następujących wkładek: 1000Base-LX/LH, 1000Base-SX, 1000BASE-BX10, CWDM. Zamawiający nie wymaga dostawy wkładek w tym postępowaniu. Musi posiadać wszystkie interfejsy „aktywne". Nie dopuszcza się stosowania kart, w których dla aktywacji interfejsów potrzebne będą dodatkowe licencje lub klucze aktywacyjne i konieczne wniesienie opłat licencyjnych. Urządzenie musi być wyposażone w minimum dwa porty USB. Port musi pozwalać na podłączenie zewnętrznych pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych.
4	Wydajność	Minimum 500Mbps z możliwością podwojenia przez klucze licencyjne.
	Pamięć	Urządzenie musi być wyposażone w minimum 8GB pamięci Flash, z możliwością rozszerzenia do min. 32GB Urządzenie musi być wyposażone w minimum 16GB pamięci RAM, pozwalającej na uruchomienie 2 sesji BGP od różnych ISP z pełnymi tablicami routingu.
5	Funkcjonalności	Obsługa protokołów routingu IPv4 takich, jak RIPv2, OSPF, BGPv4, OSPF, ISIS, a także routingu statycznego. Obsługa protokołów routingu IPv6 takich, jak RIPng, OSPFv3, BGPv4, ISIS, a także routingu statycznego. Musi posiadać obsługę protokołów routingu multicastowego PIM Sparse oraz PIM SSM, a także oraz routingu statycznego. Protokół BGP musi posiadać obsługę 4 bajtowych ASN. Obsługa BGP Router Reflector. Musi posiadać wsparcie dla funkcjonalności Policy Based Routing. Musi obsługiwać mechanizm Unicast Reverse Path Forwarding (uRPF). Musi obsługiwać tzw. routing między sieciami VLAN w oparciu o trunking 802.1Q. Obsługa Multicast Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS. Musi obsługiwać IPv6 w tym ICMP dla IPv6 oraz protokoły routingu IPv6 takie jak RIP, OSPFv3, IS-IS, Musi zapewniać obsługę list kontroli dostępu w oparciu o adresy IP źródłowe i docelowe, protokoły IP, porty TCP/UDP, opcje IP, flagi TCP, oraz o wartości TTL. Musi umożliwiać obsługę NAT dla ruchu IP unicast i multicast oraz PAT dla ruchu IP unicast.

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		Musi posiadać wsparcie dla protokołów WCCP i WCCPv2. Musi posiadać obsługę mechanizmu DiffServ. Musi mieć możliwość tworzenia klas ruchu oraz oznaczanie (Marking), klasyfikowanie i obsługę ruchu (Policing, Shaping) w oparciu o klasę ruchu. Musi zapewniać obsługę mechanizmów kolejkowania ruchu: • z obsługą kolejki absolutnego priorytetu, • ze statyczną alokacją pasma dla typu ruchu, • WFQ. Musi obsługiwać mechanizm WRED. Musi obsługiwać protokół GRE oraz zapewniać mechanizm honorowania IP Precendence dla ruchu tunelowanego. Musi obsługiwać protokół NTP. Musi obsługiwać DHCP w zakresie Client , Server. Musi posiadać obsługę tzw. First Hop Redundancy Protocol (takiego jak HSRP, GLBP, VRRP lub odpowiednika). Musi posiadać obsługę mechanizmów uwierzytelniania, autoryzacji i rozliczania (AAA) z wykorzystaniem protokołów RADIUS lub TACACS+. Musi posiadać funkcjonalność pozwalającą na monitorowanie zdarzeń systemowych i generowania akcji zdefiniowanych przez użytkownika w oparciu o język skryptowy (tzw. Embedded Event Manager – EEM, lub odpowiednik). Funkcjonalność EEM musi pozwalać monitorować zdarzenia związane z konfiguracją poprzez linię poleceń, podsystem SYSLOG, podsystem związany z wymianą modułów w czasie pracy urządzenia, podsystem sprzętowych zegarów, podsystem liczników systemowych. Funkcjonalność EEM musi pozwalać na generowanie akcji takich jak: • wykonanie komendy z poziomu linii poleceń urządzenia, • wysłanie krótkiej wiadomości tekstowej poprzez system poczty elektronicznej, • wykonanie skryptu, • wygenerowanie SNMP trap, • ustawienie lub modyfikacja określonego licznika systemowego. Musi posiadać wsparcie dla Layer-2 Tunneling Protocol Version 3. Musi posiadać możliwość rozbudowy o funkcjonalności bezpieczeństwa sieciowego: • funkcjonalność szyfrowania połączeń z wykorzystaniem algorytmów DES/3DES/AES, • algorytmy IPSec następnej generacji oparte o krzywe eliptyczne (RFC 4869), • możliwość konfiguracji tuneli IPSec VPN w oparciu o protokół IKEv2 (Internet Key Exchange v2). Wsparcie dla IKEv2 zarówno dla VPN typu site-2-site jak i dynamicznych, dla ruchu IPv4 oraz IPv6, Layer 2 and Layer 3 VPN, IPSec, Layer 2 Tunneling Protocol Version 3 (L2TPv3) • funkcjonalność VPN musi wspierać tworzenie niezależnych VPN (w tym różnego typu: site-to-site, dynamicznych) per VRF, • technologia umożliwiająca szyfrowanie IPSec ruchu unicast IPv4 bez konieczności tworzenia tuneli, z wykorzystaniem z użyciem protokołu

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		Group Domain of Interpretation (GDOI) zdefiniowanego w RFC 3547, • funkcja zapory sieciowej z analizą stanów połączenia (tzw. statefull firewall), • funkcjonalność zapory sieciowej dla protokołu IPv4 i IPv6 opartej o definicję stref bezpieczeństwa (zone-based firewall), • możliwość elastycznej definicji scenariuszy przesyłu IPv4 i IPv6 pomiędzy różnymi strefami, • ochrona centralnego procesora urządzenia (CPU) przed atakiem Denial of Service (DoS) poprzez możliwość klasyfikowania i limitowania ruchu docierającego do CPU, • możliwość logowania pakietów przekraczających skonfigurowane limity ruchu docierającego do CPU, • możliwość wymuszenia reguł złożoności haseł tworzonych na urządzeniu, Musi posiadać możliwość rozbudowy o funkcje pozwalające na automatyzację konfiguracji ustawień QoS w postaci automatycznego tworzenia wzorców konfiguracyjnych na potrzeby implementacji QoS. Zarządzanie kolejkami QoS Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing. Obsługa NBAR.
6	Zarządzanie i konfiguracja	Urządzenie musi być zarządzalne za pomocą SNMPv1, SNMPv2, SNMPv3, Telnet, SSH. Musi mieć możliwość eksportu statystyk ruchowych za pomocą protokołu sFlow, NetFlow, J-Flow lub odpowiednika. Musi być konfigurowalne za pomocą interfejsu linii poleceń (ang. Command Line Interface – CLI). Plik konfiguracyjny urządzenia (w szczególności plik konfiguracji parametrów routingu) musi pozwalać na edycję w trybie off-line, tzn. musi być możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym komputerze. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania dowolnej ilości plików konfiguracyjnych. Zmiany aktywnej konfiguracji muszą być widoczne natychmiastowo - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
7	Zasilanie	Urządzenie powinno być wyposażone w redundantne zasilanie 230V (niedopuszczalne rozwiązanie zewnętrzne).
8	Obudowa	Musi mieć możliwość montażu w szafie 19”, należy dołączyć niezbędne akcesoria.
9	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
10	Gwarancja	Minimum 36 miesięcy realizowana w miejscu instalacji sprzętu, z czasem reakcji do końca następnego dnia roboczego.

3. Dostawa przełącznika 1Gb – sztuk 1

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
1	Switch	Switch dostępowy
2	Porty	Minimum 48 porty 10/100/1000BaseT Minimum 2 dodatkowe porty uplink 10Gigabit Ethernet SFP+ Porty SFP+ muszą umożliwiać ich obsadzanie wkładkami Gigabit Ethernet: 1000BaseT, 1000Base-SX, 1000BaseLX/LH, 1000Base-BX-D/U i modułami CWDM oraz wkładkami 10Gigabit Ethernet: 10GBase-SR, 10GBase-LRM, 10GBase-LR, 10GBase-ER oraz twinax. Urządzenie musi być wyposażone w port USB umożliwiający podłączenie pamięci flash. Musi być dostępna opcja uruchomienia systemu operacyjnego z nośnika danych podłączonego do portu USB
3	Pamięć	512MB pamięci DRAM 128MB pamięci flash
4	Wydajność	Wydajność przełączania minimum 130Mpps dla pakietów 64-bajtowych. Przepustowość przełącznika minimum 108Gb/s (216Gb/s full duplex).
5	Funkcje podstawowe	Urządzenie musi obsługiwać minimum 1000 sieci VLAN Urządzenie musi obsługiwać minimum 16000 adresów MAC Urządzenie musi umożliwiać obsługę ramek jumbo o wielkości min. 9216 bajtów. Musi zapewniać obsługę min. 16 statycznych tras dla routingu IPv4 i IPv6. Obsługa ruchu multicast - IGMPv3 i MLDv1/2 Snooping. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 128 instancji protokołu STP. Obsługa połączeń link aggregation zgodnie z IEEE 802.3ad. Obsługa mechanizmów bezpieczeństwa typu Port Security i IP Source Guard na interfejsach link aggregation.
6	Funkcje dodatkowe	Wbudowane funkcje zarządzania energią zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet). Przełącznik musi posiadać możliwość uruchomienia funkcjonalności DHCP Server. Obsługa protokołu NTP. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP) Obsługa protokołu LLDP i LLDP-MED lub równoważnych (np. CDP) Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN).
7	Bezpieczeństwo	Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN i z możliwością dynamicznego przypisania listy ACL. Obsługa funkcji Guest VLAN. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
		Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X. Przełącznik musi umożliwiać elastyczność w zakresie przeprowadzania mechanizmu uwierzytelniania na porcie. Wymagane jest zapewnienie jednoczesnego uruchomienia na porcie zarówno mechanizmów 802.1X, jak i uwierzytelniania per MAC oraz uwierzytelniania w oparciu o www. Wymagana jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 Możliwość uzyskania dostępu do urządzenia przez SNMPv3, SSHv2, HTTPS z wykorzystaniem IPv4 i IPv6. Obsługa list kontroli dostępu (ACL) zarówno dla IPv4 jak i IPv6. Obsługa mechanizmów Port Security, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard. Funkcjonalność Protected Port. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard), ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard). Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (mechanizmy typu sFlow, NetFlow, J-Flow lub równoważne).
8	Mechanizmy QoS	Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP. Implementacja co najmniej czterech kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi tych kolejek. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi. Wymagana jest możliwość skonfigurowania minimum 256 różnych ograniczeń.
9	Zarządzanie	Urządzenie musi mieć możliwość zarządzania poprzez interfejs CLI z poziomu portu konsoli. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 5 plików konfiguracyjnych.
10	Zasilanie	Urządzenie powinno mieć możliwość zastosowania redundantnego zasilania.
11	Obudowa	Musi mieć możliwość montażu w szafie 19”, należy dołączyć niezbędne akcesoria.
12	Dodatkowe elementy	Patchcord prosty 1:1, kat. 6. według standardu 568B. Żyły 24AWG x 4P linka. Wtyki zalewane. Kolor czarny. Długość 3m – 48 szt.
13	Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.
14	Gwarancja	Minimum 36.

4. Dostawa szafy teleinformatycznej z wyposażeniem – sztuk 1

L.p.	Podzespół/komponent	Wymagane minimalne parametry techniczne
1	Typ	Teleinformatyczna, wolnostojąca, przeznaczona do instalacji serwerów.
2	Wymiary	19” (szer. 800mm, głęb. 1000mm), wysokość użytkowa 45U
3	Konstrukcja	2 pary belek nośnych w rozstawie 19’’ 1 para belek nośnych środkowych. Szkielet, dach, osłony, drzwi, cokół malowane farbą proszkową w kolorze czarnym (RAL 9005) Metalowe koryta kablowe pionowe ze zdejmowalną osłoną przednią w kolorze szafy, wraz z elementami mocującymi – 2 szt.
4	Ściana przednia	Drzwi blaszane perforowane o podwyższonej przewiewności (minimum 75%) wyposażone w zamek trzypunktowy z uchwytem wychylnym.
5	Ściany boczne	Osłony blaszane pełne, zdejmowane.
6	Ściana tylna	Osłona blaszana perforowana o podwyższonej przewiewności (minimum 75%) zdejmowalna.
7	Dach	Dach pełny
8	Cokół	Cokół o wysokości 100 mm z możliwością poziomowania. Tylna ściana z przepustem szczotkowym.
9	Dopuszczalne obciążenie	Minimum 1300kg (dopuszczalny ciężar sprzętu zainstalowanego w szafie)
10	Wyposażenie dodatkowe	• Przełącznik napięcia zasilającego umożliwiający automatyczne przełączanie 2 źródeł zasilania dla urządzeń wyposażonych w pojedyncze zasilacze – 1 szt. ○ Prąd znamionowy 16A ○ Czas przełączania 8 ms ○ 8 wyjść IEC C13 ○ Możliwość zarządzania i monitoringu poprzez sieć ethernet • Listwa zasilająca przystosowana do montażu pionowego (0U) wyposażona w 8 gniazd Schuko (FR), z przewodem o długości 1,8m zakończonym wtyczką Schuko (FR) wraz z elementami mocującymi – 5 szt. • Patchpanel 24 portowy z suportem na kable, kat. 6 wyposażony w złącza szczelinowe IDC, wraz z miejscem na oznaczenie przewodów, w kolorze szafy, wraz z elementami mocującymi – 1 szt. • Półka regulowana na głębokość szafy, mocowana na 4 belkach nośnych, w kolorze szafy. Minimalne obciążenie 150Kg, wraz z elementami mocującymi – 1 szt. • Prowadnica kabli metalowa o wysokości 1U, w kolorze szafy z pięcioma uchwytami ze stali ocynkowanej o wymiarach 44x88mm, wraz z elementami mocującymi – 6 szt. • Uchwyty ze stali ocynkowanej o wymiarach 66x88mm przeznaczone do mocowania na belkach nośnych, wraz z elementami mocującymi – 30 szt. • Patchcord prosty 1:1, kat. 6. według standardu 568B. Żyły 24AWG x 4P linka. Wtyki zalewane. Kolor czarny. Długość 5m – 24 szt. • Patchcord prosty 1:1, kat. 6. według standardu 568B. Żyły 24AWG x 4P linka. Wtyki zalewane. Kolor czarny. Długość 1m – 24 szt.
11	Gwarancja	24 miesiące