***Załącznik Nr 1 do SIWZ***

**Specyfikacja techniczna**

(określa minimalne wymagania Zamawiającego)

**Przedmiot zamówienia**

Przedmiotem zamówienia publicznego jest dostawa dedykowanych urządzeń sieciowych:

1. 2 identycznych urządzeń typu router szkieletowy IP/MPLS,
2. 3 identycznych urządzeń typu przełącznik sieciowy Ethernet,
3. 2 identycznych urządzeń typu firewall.
4. **Wymagania wspólne dla urządzeń:**
5. Wszystkie urządzenia oraz elementy współpracujące z nimi (np. moduły optyczne) muszą być fabrycznie nowe (tj. nieużywane za wyjątkiem wykonania testów potrzebnych do sprawdzenia ich poprawnego działania). Na dzień złożenia oferty żadne z oferowanych urządzeń nie może być przeznaczone do wycofania ze sprzedaży przez producenta (ang. end of sale) ani wsparcia technicznego (ang. end of life).
6. Zamawiający ma prawo do dodawania do zakupionych w ramach niniejszego postępowania urządzeń nowych komponentów takich jak karty z interfejsami sieciowymi lub modułów QSFP+, QSFP28, CFP2, SFP+ oraz SFP (pochodzących od dowolnych producentów) oraz wymiany zainstalowanych komponentów samodzielnie bez utraty gwarancji na zakupiony sprzęt.
7. Do każdego typu urządzeń wymagane jest dostarczenie po 1 szt. zapasowego zasilacza umożliwiającego szybką wymianę samodzielnie przez Zamawiającego w przypadku awarii. Sumarycznie wymagane są 3 zasilacze:
	1. 1 szt. Do urządzeń tupu router IP/MPLS,
	2. 1 szt. Do urządzeń typu przełącznik sieciowy,
	3. 1 szt. Do urządzeń typu firewall.
8. Urządzenia opisane w rozdziale 2 oraz 3 tj. routery oraz przełączniki muszą pochodzić od jednego producenta.
9. Sumaryczny rozmiar 6 urządzeń w ilości: 2 sztuki routera, 2 sztuki przełącznika i 2 sztuki urządzenia firewall nie może przekroczyć wartości 25RU. Trzeci przełącznik przewidziany jest do umieszczenia w innej lokalizacji niż pozostałe 6 urządzeń. W przypadku zaoferowania urządzeń, których sumaryczna wysokość będzie mniejsza niż 25RU, Zamawiający przyzna dodatkowe punkty zgodnie z kryterium „Sumaryczna wielkość”.
10. Zamawiający może przed podpisaniem umowy wezwać Wykonawcę do dostarczenia próbki we wskazane miejsce w postaci 2 routerów, 1 przełącznika oraz 1 urządzenia firewall, skonfigurowanych identycznie z oferowanymi (różnić się mogą jedynie ilością kart interfejsów oraz ilością modułów optycznych) w celu sprawdzenia spełniania przez dostarczone urządzenia wymagań określonych przez Zamawiającego. Brak pełnej kompatybilności z którymkolwiek z wymienionych wymagań lub niedostarczenie testowych urządzeń w terminie maksymalnie tygodnia od wezwania przez Zamawiającego będzie traktowany tak samo jak odmowa podpisania umowy przez Wykonawcę. Opis oraz zakres testów zawarty został w rozdziale 5 tego załącznika.
11. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży.
12. Wykonawca dokona montażu i instalacji a następnie uruchomienia urządzeń we wskazanej przez Zamawiającego szafie RACK. Uruchomienie urządzeń zawierać będzie w szczególności podłączenie zasilania oraz podłączenie interfejsów zarządczych wraz z ich konfiguracją zgodnie ze wskazaniami Zamawiającego.
13. W ramach oferty Zamawiający wymaga przeprowadzenia szkolenia w zakresie obsługi dostarczonego sprzętu, w miejscu jego instalacji, w wymiarze 14 godzin dla 8 osób. Tematyka szkolenia musi obejmować wszelkie czynności niezbędne do poprawnej eksploatacji dostarczonego sprzętu, w tym rekonfiguracje, wymiany komponentów sprzętowych oraz obsługę interfejsów zarządzających (zarówno poprzez konsolę graficzną jak i tekstową). Program oraz tematyka szkolenia muszą zostać skonsultowane z Zamawiającym oraz zaakceptowane przez niego.
14. **Kompaktowy router szkieletowy IP/MPLS. – 2 urządzenia, każde o parametrach, co najmniej:**

|  |  |
| --- | --- |
| Lp. | **Parametry minimalne wymagane przez Zamawiającego** |
| 1 | Router musi być dedykowanym urządzeniem sieciowym przystosowanym do montowania w szafie RACK 19 cali (wraz z niezbędnymi elementami montażowymi). Musi posiadać architekturę modularną. Osobnymi modułami muszą być w szczególności:1. zasilacze,
2. karty matryc przełączających i zarządzania/routingu,
3. karty interfejsów fizycznych,
4. moduły medium transmisyjnego.
 |
| 2 | Urządzenie musi być wyposażone, w co najmniej dwa redundantne zasilacze zasilane z zewnątrz napięciem przemiennym 230V. Awaria jednego z zainstalowanych zasilaczy nie może wpływać na poprawną pracę routera w pełnej konfiguracji. |
| 3 | Zarządzanie i konfiguracja routera przez administratorów musi być realizowana przez moduł kontrolny. System operacyjny routera musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać za sterowanie i monitorowanie pracy komponentów urządzenia. Ruch tranzytowy użytkowników przechodzący przez router nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi być wyposażony, w co najmniej 16 GB pamięci RAM**,** port konsoli oraz interfejs Ethernet służący do zarządzania out-of-band. |
| 4 | System operacyjny routera musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia, musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo. |
| 5 | Urządzenie musi mieć przepustowość nie mniejszą niż 2Tbps full duplex dla długich pakietów oraz nie mniej niż 1 miliard pakietów na sekundę.  |
| 6 | Urządzenie umożliwia instalację min. 2 kart liniowych interfejsów. Oprócz tego w dostarczonym urządzeniu jeden slot powinien pozostać nieobsadzony, możliwy pod przyszłą rozbudowę.  |
| 7 | Każdy z interfejsów (wymaganych w pkt 11) na karcie liniowej musi pracować z pełną prędkością w trybie pełnego dupleksu (ang. full duplex line-rate).  |
| 8 | Wymiana danych pomiędzy matrycą przełączającą a każdą z kart liniowych routera musi odbywać się z przepustowością umożliwiającą jednoczesną pracę każdego interfejsu (wymaganego w pkt 11) na karcie liniowej z pełną prędkością medium (ang. line-rate) bez względu na pasmo zajmowane przez pojedynczy strumień danych. Powyższe wymagania muszą być spełnione dla przełączania ramek warstwy II modelu OSI oraz pakietów protokołów MPLS, IPv4 i IPv6.  |
| 9 | Karty interfejsów oraz moduły optyczne muszą być wymienialne bez powodowania przerw w pracy całego urządzenia oraz bez konieczności wyłączania urządzenia. |
| 10 | Router musi mieć możliwość obsługi następujących modułów optycznych zgodnych z odpowiednimi standardami IEEE 802.3: 1. 10GBase-SR (300m)
2. 10GBase-LR (10km)
3. 40GBase-SR4 (150m)
4. 40GBase-LR4 (10km)
5. 100GBase-SR4 (100m)
6. 100GBase-LR4 (10km)
7. 100GBase-ER4 (40km)

W szczególności przepustowości 10GE mogą być obsługiwane przez rozszczepienie portu o wyższej przepustowości. |
| 11 | Urządzenie musi być wyposażone w następujące moduły i karty/interfejsy:1. Redundantne zasilacze,
2. Redundantne karty zarządzania / routingu (w typowych terminologiach producentów: supervisor engine, control module, routing engine itp.),
3. Minimum 8 portów 10GE SFP+. 4 z tych portów muszą być obsadzone modułami optycznymi 10GBase-SR (wielomodowymi o zasięgu, co najmniej 300m).
4. Minimum 6 portów 100GE QSFP28 lub CFP2. 4 porty muszą być wyposażone w moduły optyczne 100GBase-SR4 (wielomodowe umożliwiające komunikację na dystansie 100m). W przypadku zaoferowania urządzenia posiadającego więcej niż 6 portów 100GE, z których każdy obsługuje mechanizm 802.1e (MACSEC), Zamawiający przyzna za dodatkowe porty punkty zgodnie z kryterium „Liczba portów 100G w urządzeniu Router”.
 |
| 12 | Co najmniej 1 port 100GE musi zostać wyposażony w moduł optyczny umożliwiający komunikację na długim dystansie, tj. 40 km. Moduł ten musi obsługiwać standard 100GBase-ER4. |
| 13 | Na każdym z 6 portów 100GE musi istnieć możliwość uruchomienia mechanizmu IEEE 802.1ae Media Access Control Security (MACSec) oraz szyfrowania ruchu z wykorzystaniem klucza o długości 128 bitów z pełną wydajnością portu 100GE. |
| 14 | Router musi obsługiwać ramki Jumbo o wielkości 9 KB. |
| 15 | Porty 100GE i 10GE urządzenia muszą obsługiwać mechanizm umożliwiający monitorowanie kluczowych parametrów pracy modułu optycznego takich jak moc optyczna sygnału nadawanego, moc optyczna sygnału odbieranego, temperatura pracy, napięcie zasilania, prąd lasera. Digital Optical Monitoring (DOM) lub Digital Diagnostic Monitor (DDM).  |
| 16 | Urządzenie musi obsługiwać sprzętowo routing IPv4, IPv6 oraz MPLS. |
| 17 | Urządzenie musi obsługiwać routing statyczny IPv4 oraz routing dynamiczny IPv6, co najmniej dla protokołów routingu OSPF, IS-IS i BGP. |
| 18 | Urządzenie musi obsługiwać routing statyczny IPv6 oraz routing dynamiczny IPv6 – co najmniej dla protokołów routingu OSPF, IS-IS i BGP.  |
| 19 | Router jednocześnie musi obsługiwać nie mniej niż 5 milionów wpisów w tablicy routingu i forwardingu IPv4 oraz 1 milion wpisów w tablicy routingu i forwardingu IPv6. |
| 20 | Router musi obsługiwać mechanizm tworzenia wirtualnych routerów (kontekstów, routerów logicznych) umożliwiający routing pakietów w oparciu o niezależne tablice routingu – w tym zgodnie z RFC 4026 VRF, musi m.in. umożliwiać uruchomienie nie mniej niż 5 instancji routingu BGP dla różnych numerów systemów autonomicznych. Ponadto router musi obsługiwać sprzętowo 3 pełne tablice BGP dla IPv4 oraz IPv6 dla 3 różnych numerów systemów autonomicznych (przy założeniu, że w pełnej tablicy BGP znajduje się 1 milion prefiksów (IPv4 + IPv6)). Router musi obsługiwać nie mniej niż 100 sesji BGP. |
| 21 | Urządzenie musi wspierać FlowSpec zgodnie z RFC 5575. |
| 22 | Router musi obsługiwać protokół redundancji VRRP lub HSRP. |
| 23 | Mechanizm BFD musi być obsługiwany dla IPv4, IPv6 oraz MPLS LSP. |
| 24 | Urządzenie musi posiadać funkcję filtrowania ruchu wchodzącego i wychodzącego z wszystkich interfejsów. Filtrowanie ruchu musi odbywać się, co najmniej na podstawie adresów MAC, IPv4 i IPv6. Router musi obsługiwać nie mniej niż 100 000 reguł filtrowania ruchu. Włączenie filtrowania nie może powodować degradacji wydajności urządzenia, tzn. musi być realizowane sprzętowo z prędkością łącza.  |
| 25 | Router musi obsługiwać protokół SNMP w wersjach 1, 2 i 3. Router musi udostępniać za pomocą protokołu SNMP, co najmniej 64 bitowe liczniki ramek i bajtów wysłanych i odebranych na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą protokołu SNMP liczniki odebranych ramek zawierających błędy na poszczególnych interfejsach tranzytowych. Router musi udostępniać za pomocą CLI liczniki ramek wysłanych, odebranych oraz zawierających błędy na poszczególnych interfejsach tranzytowych. Ponadto po SNMP muszą być dostępne liczniki pakietów i bajtów przechwyconych przez poszczególne filtry ruchu (ACL). |
| 26 | Router musi posiadać mechanizmy pozwalające na ograniczanie pasma dla ruchu wyjściowego i wejściowego na wszystkich interfejsach tranzytowych (z uwzględnieniem filtrów ruchu – ACL) oraz dla poszczególnych sieci VLAN. |
| 27 | Router musi posiadać mechanizmy klasyfikowania ruchu, jego filtrowanie oraz znakowanie w oparciu, co najmniej 802.1p, DSCP, ToS, MPLS EXP na wszystkich portach tranzytowych oraz dla poszczególnych sieci VLAN. Dodatkowo klasyfikacja pakietów musi się również odbywać o dane z protokołu BGP – nie mniej niż Community i AS Path. Znakowanie pakietów musi być wykonywane również przez tri-coloredpolicer. |
| 28 | Urządzenie musi wykonywać shaping oraz policing ruchu per port. |
| 29 | Router musi obsługiwać, co najmniej 8 kolejek wyjściowych dla każdego portu tranzytowego. Router musi obsługiwać mechanizm WRED. |
| 30 | Urządzenie musi posiadać minimum 1GB pamięci na każdy port 100GE, co powinno przekładać się na możliwość buforowania do 80 ms na wszystkich portach tranzytowych jednocześnie. |
| 31 | Urządzenie musi zapewniać funkcjonalność zbierania przepływów z sieci, musi obsługiwać minimum jeden z protokołów: sFlow, NetFlow, jFlow, lub analogiczny. |
| 32 | Urządzenie eksportuje dane telemetryczne z częstotliwością nie mniejszą, niż co sekundę, w zakresie, co najmniej statystyk interfejsów w tym zajętości buforów pakietów. |
| 33 | Router musi mieć zaimplementowane tunelowanie GRE oraz IP-IP bezpośrednio na karcie liniowej o wydajności przynajmniej 10Gbps. |
| 34 | Router musi obsługiwać ruch IP multicast – w zakresie, co najmniej protokołów IGMP (wersje 1, 2, 3) oraz PIM-SM. |
| 35 | Na wszystkich interfejsach przeznaczonych do obsługi ruchu tranzytowego urządzenia musi obsługiwać usługi MPLS – nie mniej niż L2 VPN, VPLS lub EVPN (oparte o LDP i BGP) oraz BGP/MPLS VPN (L3 VPN). |
| 36 | Router musi obsługiwać nie mniej niż 500 sieci VPLS, lub odpowiednio 500 instancji EVPN MPLS. |
| 37 | Dla L2 VPN oraz VPLS lub EVPN musi być obsługiwany multihoming. |
| 38 | Urządzenie musi wspierać VXLAN/EVPN, w tym funkcjonalność VTEP z przełączaniem L2 i L3. |
| 39 | Router musi obsługiwać protokół sygnalizacji RSVP-TE z mechanizmem Fast Reroute (node protection oraz link protection). |
| 40 | Router musi posiadać możliwość uruchomienia mechanizmu DiffServTraffic Engineering w celu przekierowania ruchu należącego do różnych klas obsługi ruchu na różne ścieżki MPLS. |
| 41 | Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q. Urządzenie musi pozwalać na skonfigurowanie i uruchomienie nie mniej niż 3900 sieci VLAN jednocześnie. |
| 42 | Urządzenie musi obsługiwać mechanizm Q-in-Q włącznie z funkcją terminowania wewnętrznych sieci VLAN na interfejsach warstwy trzeciej. |
| 43 | Urządzenie musi obsługiwać protokoły SpanningTree – zgodnie z co najmniej IEEE 802.1d (STP), 802.1w (RSTP) i 802.1s (MSTP). |
| 44 | Jeżeli urządzenie wspiera VPLS a nie EVPN, to ramki BPDU pomiędzy sieciami VLAN muszą być przenoszone przez urządzenie również w trybie MPLS/VPLS. |
| 45 | Router musi być zarządzany poprzez tekstowy interfejs linii komend (CLI) dostępny po porcie konsoli, oraz protokół Telnet i SSH dostępny przez interfejs do zarządzania out-of-band oraz dowolny interfejs tranzytowy. Router musi posiadać funkcję współpracy z zewnętrznymi serwerami AAA RADIUS (RFC 2138, RFC 2139) oraz TACACS+ (RFC 1492). |
| 46 | Router musi posiadać funkcję limitowania pasma dla usług, których działanie jest niezbędne do prawidłowego działania urządzenia, a które mogą stać się celem ataku Denial of Service. |
| 47 | Urządzenie musi mieć domyślnie zaimplementowane zabezpieczenia przed atakami na poziomie protokołu ARP – minimalny wymagany poziom zabezpieczeń to limitowanie ruchu ARP. |
| 48 | Router musi umożliwiać duplikacje ruchu i przesyłanie go do określonego portu wyjściowego (ang. Mirroring). Funkcja duplikacji nie może w żaden sposób zakłócać działania innych usług. |
| 49 | Router musi umożliwiać duplikacje:1. całego ruchu na porcie fizycznym,
2. ruchu z wybranego VLAN-u na porcie fizycznym.
 |
| 50 | W urządzeniu musi istnieć możliwość rejestracji wszystkich komend wydawanych przez użytkownika za pomocą:1. zapisywania ich w lokalnym pliku tekstowym,
2. wysyłania ich do zewnętrznego serwera SYSLOG,
3. wysyłania ich do zewnętrznego serwera TACACS+.
 |
| 51 | Urządzenie umożliwia edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania, blokowe uruchamianie zmian konfiguracyjnych, cofanie zmian konfiguracyjnych do poprzedniej wersji, a także automatyczne cofnięcie się do poprzedniej wersji konfiguracji w przypadku np. utraty łączności administracyjnej z urządzeniem w wyniku ostatniej wprowadzonej zmiany. |
| 52 | Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim. |
| 53 | Wykonawca musi zapewnić dostęp do wszystkich instrukcji użytkownika opublikowanych przez producenta urządzenia dostarczonego w ramach realizacji zamówienia. Dostęp do dokumentacji może być zrealizowany w formie wskazania adresu URL, pod którym znajduje się dokumentacja. |
| 54 | Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej minimum 3 lata od daty dostawy. Opieka musi zawierać:1. wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wsparcie udzielane jest najpóźniej w ciągu 1 dnia roboczego,
2. wymianę uszkodzonego sprzętu w ciągu 20 dni roboczych, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
 |
| 55 | Okres gwarancji minimum 3 lata od daty dostawy, z możliwością przedłużenia na okres 5 lat. |

1. **Przełącznik sieciowy Ethernet, liczba sztuk: 3, spełniający poniższa wymagania:**

Zamawiający wymaga, aby wspólnie do wszystkich trzech urządzeń zostały dostarczone następujące moduły optyczne:

* 1. 2 sztuki QSFP28 100GBASE-ER4, przeznaczonych do pracy na odległość 40km na światłowodach jedno modowych,
	2. 8 sztuk QSFP28 100GBASE-SR4, przeznaczonych do pracy na światłowodach wielodomowych,
	3. 8 sztuk QSFP+ 40GBase-SR4, przeznaczonych do pracy na światłowodach wielomodowych,
	4. 2 sztuki kabli typu direct attach (DA) 100Gbps miedziane lub optyczne, o długości nie mniejszej niż 1m na obu końcach zakończonych złączem typu QSFP28.

|  |  |
| --- | --- |
| Lp. | **Parametry minimalne wymagane przez Zamawiającego** |
| 1 | Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do montażu w szafie RACK 19” (wraz z niezbędnymi elementami montażowymi), wyposażonym w wymienne zasilacze oraz wentylatory. |
| 2 | Urządzenie musi być wyposażone w redundantne zasilacze dostosowane do napięcia zmiennego 220-230V. Wymagana jest redundancja w modelu 1:1, tzn. awaria pojedynczego zasilacza lub jednego z dwóch obwodów zasilających nie skutkuje degradacją funkcjonalną urządzenia. |
| 3 | Urządzenie musi być chłodzone przepływem powietrza w schemacie od przodu do tyłu. Za przód urządzenia przyjmuje się stronę z zabudowanymi interfejsami tranzytowymi. |
| 4 | Przełącznik musi być wyposażony w minimum 32 porty dostępowe 40/100 Gigabit Ethernet. Typ złącza interfejsu musi być określany przez wymienny moduł QSFP+/QSFP28. Interfejsy 40/100Gbps muszą współpracować z modułami QSFP+/QSFP28 pochodzącymi od innych producentów. Lista kompatybilnych modułów QSFP/QSFP28 musi uwzględniać, co najmniej: 1. 100Gbps: 100GBase-SR4, 100GBase-LR4, 100GBase-ER4, a także interfejsy typu direct attach (DA) 100Gbps miedziane lub optyczne, o długości maksymalnej nie mniejszej niż 10m; zamawiający wymaga dostępności min. 4 różnych długości kabli DA w tym zakresie,
2. 40Gbps: 40GBase-SR4, 40GBase-LR4, 40GBase-ER4, a także interfejsy typu direct attach (DA) 100Gbps miedziane lub optyczne, o długości maksymalnej nie mniejszej niż 10m; zamawiający wymaga dostępności min. 4 różnych długości kabli DA w tym zakresie,
3. Interfejsy QSFP rozszczepiające 100Gbps na 4x25Gbps, co najmniej 25GBase-SR a także interfejsy typu direct attach break-out o długości nie mniejszej niż 3m,
4. Interfejsy QSFP rozszczepiające 40Gbps na 4x10Gbps, co najmniej 10GBase-SR oraz 10GBase-LR, a także interfejsy typu direct attach break-out o długości nie mniejszej niż 3m.
 |
| 5 | Przełącznik musi być wyposażony, w co najmniej jeden interfejs zarządzania OOB (out-of-band) Gigabit Ethernet poprzez port RJ-45 oraz port szeregowy konsoli zarządzającej. |
| 6 | Przełącznik musi posiadać funkcjonalność stworzenia stosu liczącego minimum 2 fizyczne urządzenia do pracy w formie pojedynczego, administrowanego z pojedynczej konsoli i pod wspólnym adresem IP przełącznika logicznego. |
| 7 | Urządzenie musi umożliwiać przechowywanie minimum 10 wersji konfiguracji oraz minimum 2 w pełni funkcjonalne obrazy oprogramowania - firmware.  |
| 8 | Urządzenie musi posiadać nieblokującą architekturę o wydajności przełączania min. 3,2 Tb/s (dla połączeń typu Full Duplex) i minimum 2 miliardy pakietów na sekundę. |
| 9 | Urządzenie musi obsługiwać nie mniej niż 64000 unikalnych adresów MAC. |
| 10 | Urządzenie musi być wyposażone w system operacyjny o architekturze modularnej z ochroną pamięci, procesów oraz zasobów procesora, w tym proces odpowiedzialny za przełączanie pakietów musi być odseparowany na poziomie pamięci od procesu odpowiedzialnego za routing IP i zarządzanie urządzeniem. System powinien umożliwiać monitorowanie zajętości CPU. |
| 11 | Monitoring i zarządzanie urządzeniem musi być realizowane poprzez obsługę minimum protokołu SNMP (wersje 2c i 3) oraz obsługę RMON (obsługa minimum 4 grup). |
| 12 | Urządzenie musi posiadać funkcjonalność zarządzania nim poprzez sesje telnet (zarówno w przypadku protokołów IPv4 jak i IPv6), SSH w wersji 2 (zarówno dla protokołów IPv4 jak i IPv6) i możliwość komunikacji przy użyciu API (Application Programming Interface) w języku XML. Urządzenie musi obsługiwać bezpieczny transferu plików, poprzez protokół SCP/SFTP. |
| 13 | Urządzenie musi posiadać wbudowane narzędzia administracyjno-diagnostyczne w tym minimum (dla protokołu IPv4) ping, traceroute, klient SSH i klient telnet. |
| 14 | Urządzenie musi zapewniać funkcjonalność synchronizacji czasu przy pomocy protokołów NTP. |
| 15 | Urządzenie musi zapewniać obsługę protokołów umożliwiających wykrywanie urządzeń w sieci Ethernet (IEEE 802.3), w tym minimum protokoły: LLDP (IEEE 802.1ab) wraz z rozszerzeniem LLDP-MED lub CDP. |
| 16 | Urządzenie musi zapewniać możliwość tworzenia oraz edycji skryptów i list ACL (Access Contol List) bezpośrednio poprzez interfejs zarządzający (system operacyjny musi zawierać wbudowany edytor tekstu). |
| 17 | Urządzenie musi zapewniać możliwość uruchomiania serwera i klienta protokołu DHCP oraz urządzenie musi zapewniać obsługę DHCP Relay. |
| 18 | Urządzenie musi zapewniać możliwość przesyłania logów do minimum dwóch zdefiniowanych hostów w sieci (na zdalny serwer SYSLOG). |
| 19 | Urządzenie musi zapewniać ochronę przed atakami typu DoS/DDoS skierowanymi w routing procesor (control plane) tego urządzenia.  |
| 20 | Urządzenie musi umożliwiać definiowanie list ACL (Access Control List) realizowanych sprzętowo, bez zmniejszania wydajności przełącznika pracujących na warstwie 2, 3 i 4 modelu ISO/OSI, w tym musi być zapewniona możliwość filtrowania na podstawie źródłowych i docelowych adresu MAC (Mac Address Access Control List), źródłowych i docelowych adresów IP, filtrowania po protokołach UDP, TCP, ICMP, IGMP, OSPF, filtrowania zakresów portów źródłowych i docelowych protokołów TCP i UDP, flag protokołu TCP oraz identyfikatora sieci VLAN (VLAN ID). |
| 21 | Urządzenie musi posiadać funkcjonalność uwierzytelnienia i autoryzacji poprzez protokół TACACS+ i Radius, przy korzystaniu z CLI. |
| 22 | Urządzenie musi zapewniać funkcjonalność: DHCP Snooping, IP Source Guard, Dynamic ARP Protection. |
| 23 | Urządzenie musi zapewniać funkcjonalność powielania ruchu z dowolnego portu (zarówno w przypadku ruchu ingress jak i egress) poprzez mechanizm port mirroring lub span port.  |
| 24 | Urządzenie musi zapewniać funkcjonalność zbierania przepływów z sieci, musi obsługiwać minimum jeden z protokołów: sFlow, NetFlow, jFlow, lub analogiczny. |
| 25 | Urządzenie musi obsługiwać ramki typu Jumbo, o wielkości minimum 9KB. |
| 26 | Urządzenie musi obsługiwać sieci VLAN zgodnie z IEEE 802.1q w ilości nie mniejszej niż 4094 oraz obsługiwać sieci VLAN oparte o porty fizyczne (port-based). Urządzenie musi obsługiwać protokoły umożliwiające automatyczną konfigurację sieci VLAN: GVRP/ MVRP lub VTP. |
| 27 | Urządzenie musi zapewniać funkcjonalność minimum podwójnego tagowania VLAN (Q-in-Q IEEE 802.1ad). |
| 28 | Urządzenie musi posiadać możliwość obsługi protokołu VRRP, licencja na tą funkcjonalność nie jest przedmiotem zamówienia. |
| 29 | Urządzenie musi obsługiwać agregowanie połączeń zgodnie z IEEE 802.3ad/LACP. |
| 30 | Urządzenie musi zapobiegać powstawaniu pętli w warstwie drugiej modelu ISO/OSI, w tym musi obsługiwać protokoły STP(IEEE 802.1d), RSTP(IEEE 802.1w), MSTP (IEEE 802.1s). |
| 31 | Urządzenie musi obsługiwać mechanizm kontroli dostępu do sieci na poziomie warstwy drugiej modelu ISO/OSI zgodnie ze standardem IEEE 802.1x. |
| 32 | Urządzenie musi posiadać funkcjonalność polegającą na limitowaniu adresów MAC, zatrzaśnięciu adresu MAC na porcie, definiowaniu statycznych adresów MAC na port/VLAN i wyłączeniu mechanizmu MAC learning. |
| 33 | Urządzenie musi obsługiwać mechanizm priorytetyzowania i zarządzania ruchem sieciowym (IEEE 802.1p) i DiffServ, w tym minimum 8 kolejek/port. |
| 34 | Urządzenie musi obsługiwać protokoły transmisji multicast: IGMP v1/v2/v3, PIM-SM dla IPv4 i MLDv1/v2 dla IPv6. Urządzenie musi zapewniać bezpieczeństwo poprzez filtrowanie pakietów typu IGMP. Licencja na protokół PIM-SM nie jest przedmiotem tego zamówienia. |
| 35 | Urządzenie musi obsługiwać routing IPv4 i IPv6. W tym zapewniać obsługę routingu statycznego i obsługę protokołów routingu dynamicznego: RIP, IS-IS i OSPF. Licencja na obsługę protokołów routingu dynamicznego nie jest przedmiotem zamówienia. |
| 36 | Urządzenie umożliwia edycję konfiguracji wykonywalnej na urządzeniu bez natychmiastowego jej uruchamiania oraz blokowe uruchamianie zmian konfiguracyjnych. |
| 37 | Wykonawca musi zapewnić dostęp do wszystkich instrukcji użytkownika opublikowanych przez producenta urządzenia dostarczonego w ramach realizacji zamówienia. Dostęp do dokumentacji może być zrealizowany w formie wskazania adresu URL, pod którym znajduje się dokumentacja. |
| 38 | Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej minimum 3 lata od daty dostawy. Opieka musi zawierać:1. wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wsparcie udzielane jest najpóźniej w ciągu 1 dnia roboczego,
2. wymianę uszkodzonego sprzętu w ciągu 20 dni roboczych, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
 |
| 39 | Okres gwarancji musi wynosić minimum 3 lata od daty dostawy, z możliwością przedłużenia na okres 5 lat. |

1. **Urządzenie Firewall, liczba sztuk: 2, spełniające poniższe wymagania:**

|  |  |
| --- | --- |
| Lp. | **Parametry minimalne wymagane przez Zamawiającego** |
| 1 | Urządzenie musi być dostarczone, jako dedykowane urządzenie sieciowe w postaci chassis, przystosowanego do montażu w szafie RACK 19” (wraz z niezbędnymi elementami montażowymi), wyposażone w wymienne, redundantne zasilacze AC 230V. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. |
| 2 | Jeżeli Urządzenie jest wyposażone w wentylatory lub inne elementy wymuszające obieg powietrza, to musi być także wyposażone, w co najmniej dwa moduły wentylatorów takie, aby możliwa była wymiana jednego z modułów bez przerwy w działaniu Urządzenia. |
| 3 | 1. Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewall-a z nośnika danych podłączonego do slotu USB w Urządzeniu. Urządzenie Firewall musi posiadać dedykowany interfejs Ethernet przeznaczony do zarządzania out-of-band.
 |
| 4 | 1. Zarządzanie firewallem musi odbywać się przy pomocy tekstowego interfejsu użytkownika dostępnego przez port konsoli oraz przy pomocy graficznego interfejsu użytkownika. Urządzenie musi zapewniać szyfrowany dostęp do interfejsu zarządzania, na conajmniej jeden ze sposobów: ssh, https lub API szyfrowany protokołem w wersji minimum TLS 1.2. Urządzenie musi również posiadać możliwość zarządzania przez centralny system zarządzający tego samego producenta.
 |
| 5 | System operacyjny urządzenia musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł routingu IP, odpowiedzialny za ustalenie tras routingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie. Obsługa ruchu tranzytowego użytkowników musi być realizowana sprzętowo. System operacyjny firewall-a musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. |
| 6 | Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. |
| 7 | Urządzenie musi być dostarczone z nie mniej niż:1. 4 portami 40 Gigabit Ethernet umożliwiającymi obsadzenie modułami optycznymi QSFP+. 2 porty muszą być obsadzone modułami optycznymi 40GBase-SR4.
2. 8 portami 10 Gigabit Ethernet na moduły SFP+; musi istnieć możliwość uruchomienia modułów 1Gbps. 4 porty muszą być obsadzone modułami optycznymi 10GBase-SR.
3. Odrębnymi interfejsami służącymi do łączenia firewall-a w klaster.
4. W przypadku zaoferowania urządzenia posiadającego minimum 2 porty dostępowe 100 GE QSFP28 Zamawiający przyzna dodatkowe punkty zgodnie z kryterium „Liczba portów 100G w urządzeniu Firewall”. Przy czym porty 100GE muszą mieć możliwość pracy zamiennie z prędkością 40GE poprzez zastosowanie odpowiedniego modułu optycznego QSFP+.
 |
| 8 | Urządzenie musi być wyposażone w nie mniej niż 128GB pamięci RAM oraz w dysk SSD o pojemności co najmniej 200 GB. |
| 9 | Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej. |
| 10 | Urządzenie musi posiadać możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory / LDAP. |
| 11 | Urządzenie musi obsługiwać funkcjonalność Network Address Translation, dla adresów IP źródłowych i docelowych jednocześnie, statycznie (1:1) oraz dynamicznie, dla adresów Ipv4 i Ipv6. |
| 12 | Urządzenie musi realizować zadania Stateful Firewall z włączoną funkcjonalnością rozpoznawania i kontroli aplikacji i wydajnością nie mniejszą niż:1. 20 Gb/s liczoną dla ruchu UDP,
2. musi obsłużyć nie mniej niż 15 milionów równoległych sesji,
3. zestawić nie mniej niż 120 000 tysięcy nowych połączeń/sekundę.
 |
| 13 | Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać ruch szyfrowany o przepustowości nie mniej niż 10 Gb/s dla pakietów 1024B. |
| 14 | Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż 80 000 reguł polityki bezpieczeństwa. |
| 15 | Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) realizowaną z wydajnością, co najmniej 15 Gbps. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. |
| 16 | Funkcjonalność IPS, w przypadku wykrycia ataku, musi umożliwiać podjęcie następujących akcji na ruchu objętym inspekcją:1. brak akcji blokowania, zalogowanie zdarzenia,
2. zignorowanie połączenia (przepuszczenie bez inspekcji i logowania),
3. odrzucenie pakietu/połączenia,
4. zakończenie sesji od strony klienta, serwera, klienta i serwera,
5. wykonanie akcji rekomendowanej sygnaturą dostarczoną przez dostawcę rozwiązania.
 |
| 17 | Urządzenie musi mieć możliwość uruchomienia mechanizmów automatyzacji w zakresie wskazania hostów skompromitowanych oraz automatycznego dostrojenia polityk bezpieczeństwa. Ew. licencja nie jest objęta niniejszym postępowaniem. |
| 18 | Firewall musi mieć możliwość wykrywania złośliwego oprogramowania (malware) i jego propagacji w strefie chronionej poprzez:1. sprawdzenie reputacji plików w systemie globalnym
2. sprawdzenie plików w sandbox realizowanym w chmurze lub dodatkowych lokalnych zasobach sprzętowych.

Ewentualna licencja na w/w funkcjonalności, a także sprzęt sandbox, jeżeli jest odrębny, nie są objęte niniejszym postępowaniem. |
| 19 | Urządzenie musi obsługiwać deszyfrację ruchu SSL w trybie proxy z wydajnością nie mniejszą niż 3Gb/s. |
| 20 | Firewall musi posiadać funkcję rozpoznawania aplikacji na podstawie uaktualnianych sygnatur. Na podstawie rozpoznania aplikacji, musi być możliwe jej selektywne (tj. w połączeniu z innymi kryteriami, w tym identyfikacją użytkowników) dopuszczenie, zablokowanie, przycięcie do określonej przepustowości, oraz przekierowanie na wybrane łącze. |
| 21 | Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF oraz BGP.  |
| 22 | Urządzenie musi umożliwiać obsługę, co najmniej 1024 sieci VLAN z tagowaniem 802.1Q. |
| 23 | Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz przycinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków IP, TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.  |
| 24 | Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.  |
| 25 | Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone są w języku polskim. |
| 26 | Wykonawca musi zapewnić dostęp do wszystkich instrukcji użytkownika opublikowanych przez producenta urządzenia dostarczonego w ramach realizacji zamówienia. Dostęp do dokumentacji może być zrealizowany w formie wskazania adresu URL, pod którym znajduje się dokumentacja. |
| 27 | Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej ważnej minimum 3 lata od daty dostawy. Opieka musi zawierać:1. wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wsparcie udzielane jest najpóźniej w ciągu 1 dnia roboczego,
2. wymianę uszkodzonego sprzętu w ciągu 20 dni roboczych, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
3. dostęp do aktualnej bazy danych zawierającej sygnatury zagrożeń dla funkcjonalności IPS i rozpoznawania aplikacji dla Urządzenia Firewall.
 |
| 28

|  |
| --- |
| Okres gwarancji musi wynosić minimum 3 lata od dostawy, z możliwością przedłużenia na okres 5 lat. |

 | Okres gwarancji musi wynosić minimum 3 lata od daty dostawy, z możliwością przedłużenia na okres 5 lat. |

1. **Zakres testów akceptacyjnych urządzeń:**

Zamawiający udostępni do celów testu generator i analizator ruchu **Spirent TestCenter N11U** z dwoma interfejsami **100GBase-LR4 (moduł CFP2 ze złączem LC).** Moduły optyczne w testowanych urządzeniach muszą zostać dostarczone przez Wykonawcę. Wykonawca na swój koszt zapewni również niezbędne kable światłowodowe.

1. Router, test pojemności tablic routingu i forwardingu.

W ramach testu do trzech odrębnych instancji VRF na urządzeniu testowym załadowane zostanie po 1 milionie prefiksów Ipv4. Test polega na:

* 1. weryfikacji wyrywkowo wybranych 10 prefiksów według dostępności w tablicy routingu,
	2. weryfikacji wyrywkowo wybranych 10 prefiksów poprzez sprawdzenie dostępności adresu docelowego (ping).

2. Router, test funkcjonalności flowspec:

W ramach testu do routera zostanie wysłana, krótka (poniżej 10 wpisów) lista kontroli dostępu przez protokół BGP. Weryfikacji podlega uniemożliwienie dostępu zgodnie z treścią przesłanej listy.

3. Router, test głębokości bufora i telemetrii:

W ramach testu przez urządzenie będzie przesyłane 100Gb/s ruchu pomiędzy dwoma portami 100GE. Przez dodatkowy port zostanie wysłana z prędkością 100Gb/s niewielka (1GB) próbka dodatkowego ruchu powodująca zapełnienie bufora. Oczekiwanym rezultatem testu jest:

* 1. Bezstratność ruchu.
	2. Przesłanie przez urządzenie informacji telemetrycznej pokazującej zwiększoną zajętość kolejki.

4. Dwa routery plus przełącznik, test MACSEC i SPAN:

Topologia sieci zaprezentowana jest na Rysunku nr. 1.

W ramach testu przez routery przesłane będzie 90Gb/s ruchu (ramki 250B) podlegające zaszyfrowaniu przez MACSEC. Przełącznik przesyła kopię ruchu na dodatkowy port miernika. Oczekiwanym rezultatem testu jest:


Rysunek 1. Topologia sieci w ramach testu MACSEC i SPAN.

1. zaszyfrowanie ruchu między ruterami,
2. brak strat przesyłanych pakietów.

5. Firewall, podstawowa przepustowość:

W ramach testu przez urządzenie będzie przesyłane 20Gb/s ruchu złożone z dwukierunkowej transmisji po 10Gb/s. Przesyłany ruch to pakiety UDP długości 1500 bajtów. Oczekiwane rezultaty testu:

* 1. stratność pakietów na poziomie nieprzekraczającym 10% dla ruchu dopuszczonego polityką bezpieczeństwa
	2. weryfikacja mechanizmu stateful tj. dopuszczalność transmisji zwrotnej tylko po jej zainicjowaniu od strony interfejsu oznaczonego, jako wewnętrzny (zaufany).