**Załącznik nr 1b do SIWZ**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

1. **Definicje:**

**Awaria**

Stan niesprawności obiektu uniemożliwiający jego funkcjonowanie, występujący nagle i powodujący jego niewłaściwe działanie lub całkowite unieruchomienie. Moment wystąpienia awarii nie jest możliwy do określenia z góry, przeważnie nie sposób przewidzieć również jej zasięgu;

**Błąd**

Usterkę oprogramowania powodująca jego nieprawidłowe działanie;

**Uszkodzenie**

Przypadek losowy, powodujący utracenie chwilowe lub stałe zdatności obiektu. Uszkodzenie następuje wtedy, gdy wartości parametrów danego obiektu eksploatacji nie są w normie i przekraczają jego graniczne wartości wytrzymałości;

**Awaria/uszkodzenie**

Może dotyczyć obiektu tj. urządzenia teleinformatycznego, grupy urządzeń teleinformatycznych (maszyn), systemu teleinformatycznego (zespół urządzeń i oprogramowania) lub oprogramowania na te urządzenia;

**Wsparcie techniczne**

Gwarantowana pomoc w eksploatacji urządzenia teleinformatycznego, grupy urządzeń teleinformatycznych (maszyn), systemu teleinformatycznego (zespół urządzeń i oprogramowania) lub oprogramowania na te urządzenia udzielana Zamawiającemu przez producenta lub dystrybutora urządzenia.

1. **Przedmiot zamówienia.**

Przedmiotem zamówienia jest:

1. dostawa 2 urządzeń UTM wraz z niezbędnym oprogramowaniem oraz licencjami udzielonymi na okres zgodny z ofertą liczony od dnia podpisania protokołu odbioru urządzeń (zwane dalej: „urządzeniami”).
2. dostawa 1 urządzenia typu Przełącznik wraz z niezbędnym oprogramowaniem oraz licencjami udzielonymi na okres zgodny z ofertą liczony od dnia podpisania protokołu odbioru urządzeń (zwane dalej: „przełącznik”).
3. Przeprowadzenie prac związanych z instalacją, konfiguracją dostarczonych urządzeń i przełącznika
4. Wykonanie dokumentacji projektowej, powykonawczej, eksploatacyjnej a także scenariuszy testów akceptacyjnych;
5. Przeprowadzenie testów akceptacyjnych;
6. Przeprowadzenie szkolenia z funkcjonowania i obsługi urządzeń i przełącznika.
7. Zapewnienie wsparcia technicznego na okres zgodny z ofertą (minimum 24 miesiące) liczony od dnia podpisania protokołu odbioru urządzeń i przełącznika/
8. **Dostawa 2 urządzeń UTM**

**Wymagane minimalne parametry techniczne:**

* Urządzenie dostarczane jest jako dedykowane urządzenie sieciowe 1 U, przystosowane do montażu w szafie rack.
* W urządzeniu musi być zainstalowany nadmiarowy zasilacz AC.
* Urządzenie musi być wyposażone w co najmniej 4 GB pamięci RAM oraz dysk twardy SSD o pojemności nie mniej niż 100 GB. Do zarządzania out-of-band musi być przeznaczony dedykowany port Ethernet oraz port konsoli dostępny złączami RJ-45 oraz mini-USB.
* Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych.
* Urządzenie posiadać możliwość uruchomienia systemu operacyjnego z nośnika danych podłączonego do slotu USB w module kontrolnym
* Wraz z urządzeniem musi być dostarczony kabel RS-232 do podłączenia konsoli.
* 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 rutingu IP, odpowiedzialny za ustalenie tras rutingu 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 urządzenia musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji.
* Urządzenie musi być wyposażone w co najmniej 16 interfejsów Gigabit Ethernet 10/100/1000 TX, (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji) oraz nie mniej niż 4 interfejsów uplink 10 Gigabit Ethernet obsługujących wkładki SFP i SFP+. Wszystkie wbudowane interfejsy 1 Gigabit Ethernet muszą obsługiwać technologię PoE+ zgodnie z 802.3at.
* Urządzenie musi być wyposażone w nie mniej niż 4 sloty na dodatkowe karty z modułami interfejsów. Urządzenie musi umożliwić rozbudowę o co najmniej następujące rodzaje interfejsów: ADSL 2/2+, VDSL, 1 Gigabit Ethernet (SFP), 3G/LTE, wireless 802.11ac.
* Urządzenie musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż 120 strefami bezpieczeństwa z wydajnością nie mniejszą niż 4 000 Mb/s liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż 1 700 000 pakietów/sekundę (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż 375 000 równoległych sesji oraz zestawić nie mniej niż 48 000 nowych połączeń/sekundę. Firewall musi realizować funkcje zabezpieczeń w trybie warstwy 3 i warstwy 2 modelu OSI.
* Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE v2 w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać nie mniej niż 2 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 1 Gb/s dla ruchu IMIX. W zakresie VPN urządzenie musi obsługiwać zestawianie tuneli VPN w oparciu o certyfikaty oraz standardowe algorytmy kryptograficzne, w tym AES256, SHA-256, DH14. W celu obsługi architektury VPN hub&spoke firewall musi obsługiwać funkcje Auto VPN i Auto Discovery VPN. Urządzenie musi posiadać możliwość zestawienia tuneli VPN z użytkownikami łączącymi się przy pomocy oprogramowania klienta VPN w oparciu o protokoły IPSec VPN i SSL VPN.
* Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE v2 w konfiguracji site-to-site oraz client-to-site. Firewall musi obsługiwać nie mniej niż 2 000 równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż 1 Gb/s dla ruchu IMIX. W zakresie VPN urządzenie musi obsługiwać zestawianie tuneli VPN w oparciu o certyfikaty oraz standardowe algorytmy kryptograficzne, w tym AES256, SHA-256, DH14. W celu obsługi architektury VPN hub&spoke firewall musi obsługiwać funkcje Auto VPN i Auto Discovery VPN. Urządzenie musi posiadać możliwość zestawienia tuneli VPN z użytkownikami łączącymi się przy pomocy oprogramowania klienta VPN w oparciu o protokoły IPSec VPN i SSL VPN.
* 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. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 4 000 reguł polityki bezpieczeństwa.
* Urządzenie musi identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z aplikacjami typu Peer-to-Peer i Instant Messaging). Identyfikacja aplikacji musi odbywać się co najmniej przez sygnatury i analizę heurystyczną. Urządzenia musi identyfikować nie mniej niż 3500 różnych aplikacji, w szczególności takich, które są tunelowane w protokołach HTTP i HTTPS – w tym aplikacji Web 2.0, nie mniej niż Skype, Facebook, Youtube. Musi być dostępna możliwość definiowania własnych sygnatur aplikacji z uwzględnieniem kryteriów z warstwy 7 modelu OSI. Dostęp użytkowników do poszczególnych aplikacji musi być konfigurowany przy pomocy reguł filtrowania uwzględniających co najmniej adresy IP, nazwy użytkowników oraz wyżej wymienione aplikacje. Kontrola dostępu do dynamicznie identyfikowanych aplikacji musi być wykonywana z przepustowością nie mniej niż 1 000 Mb/s mierzoną dla transakcji HTTP o długościach 44 KB.
* Urządzenie musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention). System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych rodzajów ataków musi odbywać się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż 2 000 Mb/s mierzoną dla transakcji HTTP o długościach 44 KB. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia, nie może zawierać mniej niż 10 000 pozycji. Baza sygnatur ataków musi być aktualizowana codziennie. Musi być dostępna możliwość definiowania własnych sygnatur ataków.
* Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antywirusowej sprawdzający komunikację związaną z pocztą elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać instalowania dodatkowego serwera przez użytkownika. W celu optymalizacji działania, baza definicji wirusów i złośliwego oprogramowania nie powinna być ściągana lokalnie na urządzenie – porównywanie charakterystyki badanego ruchu z wzorcami wirusów powinno odbywać się w serwisie udostępnionym przez producenta.
* Urządzenie zabezpieczeń musi posiadać wbudowany moduł kontroli antyspamowej działający w oparciu co najmniej o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera.
* Urządzenie zabezpieczeń musi posiadać wbudowany moduł filtrowania stron WWW w zależności od kategorii treści stron oraz reputacji serwisów WWW. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera.
* Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies.
* Urządzenie musi posiadać funkcję blokowania oraz rejestrowania połączeń botnetów ze serwerami C&C, połączeń ze szkodliwymi adresami URL, połączeń z publicznymi adresami IP zlokalizowanymi w wybranych państwach. Lista adresów IP serwerów C&C, szkodliwych adresów URL, oraz powiązanie publicznych adresów IP z państwami musi być tworzona przez producenta i na bieżąco aktualizowana. Aktualizacja wpisów na liście nie może powodować zmiany konfiguracji urządzenia. Musi być dostępna możliwość dodania do listy obiektów pochodzących z innych publicznie dostępnych źródeł – nie mniej niż aktualnych adresów IP używanych przez usługę Microsoft Office 365 oraz aktualnych węzłów sieci TOR. Musi istnieć możliwość dodawania własnej listy adresów IP.
* Urządzenie musi realizować funkcję deszyfrowania ruchu SSL inicjowanego przez użytkowników z wewnątrz chronionej sieci – SSL Forward Proxy. Urządzenie musi inicjować i terminować sesje szyfrowane protokołem SSL w wersjach co najmniej TLS 1.0, TLS 1.1 i TLS 1.2 w oparciu o certyfikaty X.509v3. Na odszyfrowanym ruchu muszą być realizowane funkcje bezpieczeństwa warstwy aplikacyjnej – nie mniej niż dynamiczna identyfikacja aplikacji Web 2.0, IPS, antywirus, URL-filtering. Urządzenie musi pozwalać na wysłanie kopii odszyfrowanego ruchu do zewnętrznego analizatora.
* Urządzenie musi być zintegrowane z rozwiązaniem ochrony przed atakami zero-day pochodzącym od tego samego producenta. Kopie plików dystrybuowanych przez użytkowników protokołami co najmniej HTTP, SMTP i IMAP – przesyłanymi zarówno w postaci odszyfrowanej, jak i zaszyfrowanej w SSL - muszą być przesyłane w celu analizy pod kątem występowania w nich zagrożeń zero-day w dedykowanym systemie testującym je w odizolowanym kontrolowanym środowisku wirtualnym (tzw. sandbox). W przypadku wykrycia zagrożenia urządzenie firewall musi zablokować transfer pliku lub komunikację z zainfekowanym hostem zgodnie ze zdefiniowaną polityką bezpieczeństwa.
* Urządzenie musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF, IS-IS oraz BGP. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 128 wirtualnych routerów. Firewall musi obsługiwać następujące protokoły routingu dynamicznego IPv6: RIPng, OSPFv3, BGP. Pojemność tablicy routingu musi wynosić nie mniej niż 1 milion tras.
* Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN.
* Urządzenie musi obsługiwać co najmniej 3000 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1w) oraz Multiple STP (802.1s). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet. Pojemność tablicy adresów MAC nie może być mniejsza niż 16 000.
* W celu zapewnienia bezpieczeństwa danych przesyłanych w warstwie 2 urządzenie musi obsługiwać protokół MACSec zgodnie z 802.1AE na wszystkich wbudowanych portach 1 Gigabit Ethernet i 10 Gigabit Ethernet. Dane przesyłane protokołem MACSec muszą być zabezpieczone algorytmem szyfrowania AES z kluczem o długości nie mniej niż 256 bitów.
* Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków 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.
* Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive oraz Active/Active 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.
* Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Urządzenie musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. Musi być dostępna możliwość zarządzania oraz pozyskiwania danych z urządzenia z wykorzystaniem API. Specyfikacja API musi być udostępniona przez producenta.
* Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 5 poprzednich, kompletnych konfiguracji.
* Zamawiający wymaga aby do Urządzenia były załączone wszystkie wymagane licencje pozwalające na uzyskanie opisanych funkcjonalności np. IPS/IDS, filtr antispam, filtr antywirusowy, filtrowanie stron WWW, funkje sandobox - reagowanie na ataki zero-day, funkcje blokowania C&C,
* Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone są w języku polskim.
* W przypadku gdy do działania wymienionych wcześniej funkcji konieczne są licencje, system musi zostać w nie wyposażony. Licencje muszą być aktywne przez okres co najmniej 36-miesięcy (3 lata) od daty podpisania protokołu odbioru urządzeń.
* Dostarczane urządzenie musi być objęte co najmniej 24-miesięcznym (2 lata) od daty podpisania protokołu odbioru urządzeń wsparciem technicznym producenta urządzenia. Wsparcie techniczne świadczone telefonicznie, pocztą elektroniczną przez producenta lub polskiego dystrybutora sprzętu w języku Polskim. Zamawiający wymaga aby wsparcie było świadczone na następującym poziomie:
1. zgłaszanie uszkodzenia, awarii, błędu w dni robocze w godzinach pracy Zamawiającego (8-16)
2. wymiana urządzenia na następny dzień roboczy (NBD) po rozpoznaniu uszkodzenia, awarii, błędu w wyniku zgłoszenia przez Zamawiającego
3. nieograniczony dostęp (24 godziny na dobę, 7 dni w tygodniu) do dedykowanej przez producenta urządzenia strony pozwalający na uzyskanie pomocy technicznej, aktualizacje i uaktualnienia oprogramowania.
4. **Dostawa 1 przełącznika warstwy 3 o stałej konfiguracji z możliwością pracy w stosie:**
* Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack lub posiadającym specjalny zestaw producenta sprzętu do montowania przełącznika w szafie rack.
* Przełącznik musi posiadać co najmniej 12 portów dostępowych Ethernet 10/100/1000 Auto-MDI/MDIX.
* Przełącznik musi posiadać co najmniej 2 porty uplink 10 Gigabit Ethernet SFP+. Korzystanie z portów uplink nie może powodować wyłączenia portów dostępowych 10/100/1000. Porty uplink muszą akceptować również wkładki SFP umożliwiając obsługę połączeń uplink Gigabit Ethernet.
* Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band).
* Wraz z urządzeniem musi być dostarczony kabel RS-232 do podłączenia konsoli.
* Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego przełącznika z nośnika danych podłączonego do slotu USB. Na nośniku danych podłączonym do slotu USB musi być możliwość przechowywania plików konfiguracyjnych przełącznika.
* Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI) przez port konsoli, telnet, ssh, a także za pośrednictwem interfejsu WWW.
* Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 4 urządzenia. Dopuszczalne jest podłączanie do stosu portami uplink 10 Gb/s. Stos musi być widoczny z punktu widzenia zarządzania oraz innych urządzeń sieciowych jako jedno urządzenie. Zarządzanie wszystkimi przełącznikami w stosie musi się odbywać z dowolnego przełącznika będącego częścią stosu. Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup’u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master.
* Przełącznik musi posiadać architekturę non-blocking. Maksymalna wydajność przełączania w warstwie 2 nie może być niższa niż 64 Gb/s (bidirectional) i 47 milionów pakietów na sekundę dla pakietów 64-bajtowych. Przełącznik nie może obsługiwać mniej niż 16 000 adresów MAC.
* Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów).
* Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4093. Przełącznik musi obsługiwać sieci VLAN oparte o porty fizyczne (port-based) i adresy MAC (MAC-based). W celu automatycznej konfiguracji sieci VLAN, przełącznik musi obsługiwać protokół MVRP.
* Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grup LAG, nie mniej niż 8 linków w grupie.
* Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D i 802.1w, a także Multiple Spanning Tree zgodnie z IEEE 802.1s (nie mniej niż 64 instancje MSTP).
* Przełącznik musi obsługiwać protokół LLDP i LLDP-MED.
* Urządzenie musi obsługiwać routing między sieciami VLAN – routing statyczny, oraz protokół routingu dynamicznego RIP. Ilość tras obsługiwanych sprzętowo nie może być mniejsza niż 4096 dla ruchu unicast oraz 2048 dla ruchu multicast.
* Przełącznik musi posiadać możliwość uruchomienia protokołów routingu dynamicznego, dla IPv4 (nie mniej niż RIP v1/v2, OSPF v1/v2) oraz dla IPv6 (nie mniej niż OSPFv3 i RIPng).
* Urządzenie musi posiadać możliwość obsługi funkcji PIM sparse mode (PIM-SM), PIM source specific mode (PIM-SSM), IGMP v1, v2, v3.
* Urządzenie musi pozwalać na zarządzanie po IPv6.
* Urządzenie musi posiadać mechanizmy priorytetyzowania dla ruchu wchodzącego i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3 dla ruchu wychodzącego. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 8 kolejek per port fizyczny.
* Urządzenie musi obsługiwać filtrowanie ruchu na co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. Urządzenie musi realizować sprzętowo nie mniej niż 2000 reguł filtrowania ruchu. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu.
* Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping.
* Przełącznik musi obsługiwać IEEE 802.1x zarówno dla pojedynczego, jak i wielu suplikantów na porcie. Przełącznik musi przypisywać ustawienia dla użytkownika na podstawie atrybutów zwracanych przez serwer RADIUS (co najmniej VLAN oraz reguła filtrowania ruchu). Musi istnieć możliwość pominięcia uwierzytelnienia 802.1x dla zdefiniowanych adresów MAC. Przełącznik musi obsługiwać co najmniej następujące typy EAP: MD5, TLS, TTLS, PEAP.
* Urządzenie musi obsługiwać protokół SNMP (wersje 2 i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN.
* Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu routingu IP, odpowiedzialnego za ustalanie tras routingu i zarządzanie urządzeniem.
* Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż 20 poprzednich, kompletnych konfiguracji.
* Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim.
* W przypadku gdy do działania wymienionych wcześniej funkcji konieczne są licencje, system musi zostać w nie wyposażony. Licencje muszą być aktywne przez okres co najmniej 36-miesięcy (3 lata) od daty podpisania protokołu odbioru urządzeń.
* Dostarczane urządzenie musi być objęte co najmniej 24-miesięcznym (2 lata) od daty podpisania protokołu odbioru urządzeń wsparciem technicznym producenta urządzenia. Wsparcie techniczne świadczone telefonicznie, pocztą elektroniczną przez producenta lub polskiego dystrybutora sprzętu w języku Polskim. Zamawiający wymaga aby wsparcie było świadczone na następującym poziomie:
1. zgłaszanie uszkodzenia, awarii, błędu w dni robocze w godzinach pracy Zamawiającego (8-16)
2. wymiana urządzenia na następny dzień roboczy (NBD) po rozpoznaniu uszkodzenia, awarii, błędu w wyniku zgłoszenia przez Zamawiającego
3. nieograniczony dostęp (24 godziny na dobę, 7 dni w tygodniu) do dedykowanej przez producenta urządzenia strony pozwalający na uzyskanie pomocy technicznej, aktualizacje i uaktualnienia oprogramowania.
4. **Wykaz prac związanych z instalacją, konfiguracją dostarczonych urządzeń i przełącznika**
5. Instalacja fizyczna urządzeń i przełącznika we wskazanej przez Zamawiającego lokalizacji,
6. Wykonanie konfiguracji wraz z instalacją oprogramowania dla Urządzeń i Przełącznika,
7. Instalacja wszystkich wymaganych i dostarczonych licencji w celu uzyskania wymaganych funkcjonalności,
8. Uruchomienie dostarczonych w ramach postępowania urządzeń w klastrze HA,
9. Podłączenie dostarczonych w ramach postępowania urządzeń do centralnego systemu zarządzania Juniper Junos Space
10. Uruchomienie mechanizmów ochrony przed awariami elementów sprzętowych
i programowych systemu zabezpieczeń oraz łączy sieciowych.
11. Uruchomienie mechanizmów bezpieczeństwa – pełny UTM
12. Wykonanie testów akceptacyjnych.
13. **Dokumentacja**

### Dokumentacja projektowa

Wykonawca opracuje i przedstawi do zatwierdzenia przez Zamawiającego projekt techniczny planowanych do wykonania prac teleinformatycznych.

### Scenariusze testów akceptacyjnych

Wykonawca opracuje i przedstawi do zatwierdzenia przez Zamawiającego scenariusze testów. Scenariusze testów będą obejmować wszystkie elementy dostarczonej infrastruktury teleinformatycznej.

Scenariusze testów muszą obejmować również testy funkcjonalne urządzeń dostarczonych w ramach postępowania np. - blokowanie zainfekowanych plików, filtracja stron WWW, analiza poprawnej pracy silników IPS itd.

### Dokumentacja powykonawcza

Wykonawca przedstawi do zatwierdzenia Dokumentację Powykonawczą zawierającą zaktualizowaną Dokumentację Projektową oraz specyfikację elementów oprogramowania (np. skryptów, plików konfiguracyjnych itp.) wykonanych specjalnie dla potrzeb realizacji przedmiotu zamówienia.

### Dokumentacja eksploatacyjna

Wykonawca przedstawi do zatwierdzenia dokumentację dotyczącą Procedur Eksploatacyjnych, w tym, co najmniej:

* procedury monitorowania pracy urządzeń i oprogramowania systemowego oraz narzędziowego z uwzględnieniem alarmowania o bieżących problemach;
* procedury okresowych czynności administracyjnych dotyczących sprzętu i oprogramowania systemowego oraz narzędziowego;
* procedury działania w razie awarii systemu.
1. **Wymagania ogólne do dokumentacji**

Każda dokumentacja zostanie dostarczona na nośniku cyfrowym w wersji edytowalnej np. MS Word. Dodatkowo w oddzielnym dokumencie Wykonawca dostarczy zestawienie haseł i loginów.

**7) Przeszkolenie**

* w siedzibie Zamawiającego lub w szczególnych przypadkach online
* dla maksymalnie 5 pracowników Zamawiającego
* odbiór przeszkolenia potwierdzony będzie odpowiednim protokołem
* przeszkolenie musi zostać przeprowadzone przed podpisaniem protokołu odbioru końcowego