**Załącznik nr 1 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 co najmniej 36 miesięcy liczony od dnia podpisania protokołu odbioru urządzeń (zwane dalej: „urządzeniami”).
2. Przeprowadzenie prac związanych z migracją z posiadanych przez Zamawiającego urządzeń UTM (przeniesienie istniejących usług) na nowe dostarczone urządzenia.
3. Wykonanie dokumentacji projektowej, powykonawczej, eksploatacyjnej a także scenariuszy testów akceptacyjnych
4. przeprowadzenie szkolenia z funkcjonowania i obsługi urządzeń.
5. zapewnienie wsparcia technicznego na okres co najmniej 36 miesięcy liczony od dnia podpisania protokołu odbioru urządzeń

Z uwagi na to, że art. 30 ust. 5 ustawy prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę jako tego, kto jest zobowiązany wykazać, że oferowane Urządzenia spełniają wymagania postawione przez Zamawiającego, Zamawiający, w przypadku jakichkolwiek wątpliwości, zastrzega sobie prawo sprawdzenia pełnej zgodności zaoferowanych przez Wykonawcę produktów z wymogami specyfikacji Sprawdzenie to będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych na sprzęcie Oferenta,   
z użyciem urządzeń peryferyjnych Zamawiającego. W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby Zamawiającego, w terminie 5 dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego przedmiotu dostawy.   
W odniesieniu do oprogramowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt. 2 ustawy.

Nieprzedłożenie oferowanych produktów do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia.

Po wykonaniu testów, dostarczone do testów egzemplarze będą zwrócone oferentowi.

1. **Dostawa 2 urządzeń UTM**

**Wymagane minimalne parametry techniczne:**

1. Urządzenie dostarczane jest jako dedykowane urządzenie sieciowe 1 U, przystosowane do montażu w szafie rack.
2. W urządzeniu musi być zainstalowany nadmiarowy zasilacz AC.
3. Urządzenie musi być wyposażone w co najmniej 12 interfejsów Gigabit Ethernet 10/100/1000 TX, co najmniej 4 interfejsy GigabitEthernet definiowane przez moduły SFP, wraz z modułami w standardzie 1000 Base-SX (Zamawiający wymaga ich dostarczenia w ramach postępowania), co najmniej 4 interfejsy 10 GigabitEthernet definiowane przez moduły SFP+, wraz z modułami w standardzie 10GBase-SR (Zamawiający wymaga ich dostarczenia w ramach postępowania)
4. Wraz z urządzeniem musi być dostarczony kabel RS-232 do podłączenia konsoli.
5. Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP.
6. Urządzenie musi obsłużyć minimum 2 miliony prefiksów w RIB oraz 1 milion w FIB.
7. Urządzenie musi posiadać funkcję tworzenia wirtualnych ruterów w liczbie co najmniej 512, oraz sieci VLAN z tagowaniem 802.1Q. Urządzenie musi umożliwiać obsługę co najmniej 3500 sieci VLAN oraz 64 000 adresów MAC.
8. 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 funkcję tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach.
9. Mechanizmy QoS (policing, kolejkowaniem, shaping) oraz funkcje ochrony przed atakami DoS i DDoS muszą być realizowane sprzętowo.
10. Urządzenie musi obsługiwać protokoły sygnalizacji RSVP oraz LDP, w tym funkcję Fast Reroute.
11. Urządzenie musi obsługiwać aplikacje MPLS, co najmniej Circuit Cross-Connect (CCC), Translational Cross-Connect (TCC), L2 VPN/L2 Circuit, VPLS oraz Next-Generation Multicast VPN (NG-MVPN).
12. Urządzenie musi być wyposażone w co najmniej 16 GB pamięci RAM oraz w dysk SSD o pojemności co najmniej 120 GB.
13. Urządzenie musi posiadać osobne moduły kontroli oraz przetwarzania ruchu   
    w postaci osobnych zasobów sprzętowych.
14. 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.
15. System operacyjny urządzenia musi być instalowany i uruchamiany na module kontrolnym. Moduł kontrolny musi odpowiadać za sterowanie i monitorowanie pracy komponentów urządzenia. Ruch tranzytowy użytkowników przechodzący przez urządzenia nie może być przesyłany przez moduł kontrolny. Moduł kontrolny musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego urządzenia z nośnika danych podłączonego do slotu USB na module kontrolnym. Moduł kontrolny musi posiadać dedykowany interfejs Ethernet przeznaczony do zarządzania out-of-band.
16. Z punktu widzenia systemu operacyjnego urządzenia wszystkie usługi bezpieczeństwa muszą być zdefiniowane w tym samym pliku konfiguracyjnym zdefiniowanym na module kontrolnym.
17. Zarządzanie urządzeniem musi odbywać przy pomocy tekstowego interfejsu użytkownika (dostępnego przez port konsoli, telnet, ssh) oraz przy pomocy graficznego interfejsu użytkownika. Urządzenie musi być kompatybilne i posiadać możliwość zarządzania przez centralny system zarządzający posiadany przez Zamawiającego tj. Juniper Junos Space.
18. Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być możliwość przechowywania co najmniej 5 poprzednich, kompletnych konfiguracji.
19. Urządzenie musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń. Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Active oraz 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.
20. Urządzenie musi realizować zadania Stateful Firewall z wydajnością nie mniejszą niż 5 Gb/s liczoną dla ruchu IMIX. Urządzenie musi obsłużyć nie mniej niż 2 miliony równoległych sesji oraz zestawić nie mniej niż 50 tysięcy nowych połączeń/sekundę.
21. Urządzenie musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu   
    o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. Urządzenie musi obsłużyć ruch szyfrowany o przepustowości nie mniej niż 1,3 Gb/s dla ruchu IMIX.
22. 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 co najmniej 16 000 reguł polityki bezpieczeństwa.
23. System zabezpieczeń musi realizować zadania firewall, wykonując kontrolę na poziomie sieci oraz oferować możliwość kontroli na poziomie aplikacji w oparciu   
    o moduł prewencji włamań IPS.
24. Urządzenie zabezpieczeń musi posiadać dedykowany układ sprzętowy przyspieszający działanie modułu IPS.
25. Moduł IPS musi wykrywać ataki bazując co najmniej na wymienionych metodach: detekcja anomalii protokołów, detekcja w oparciu o sygnatury pełno-stanowe, detekcja w oparciu o złożenie metod detekcji anomalii protokołów oraz sygnatur pełno-stanowych.
26. Sygnatury systemu IPS muszą być aktualizowane nie rzadziej niż raz na dzień.
27. System IPS musi oferować różne możliwości reagowania na incydenty: brak akcji, oznaczanie pakietów wartościami DSCP, zaprzestanie dalszego skanowania ruchu   
    z wykrytym atakiem, zamykanie całego połączenia, zamykanie połączenia   
    z wysłaniem pakietu RST do klienta, zamykanie połączenia z wysłaniem pakietu RST do serwera, zamykanie połączenia z wysłaniem pakietów RST zarówno do klienta jak i do serwera oraz akcji rekomendowanej przez producenta platformy zabezpieczeń. Dodatkowo musi oferować akcje dotyczące wyszczególnionego ruchu pomiędzy danymi adresami IP: powiadamianie, ciche blokowanie pakietów należących do danej sesji, zamykanie nowych sesji dotyczących danych adresów IP poprzez wysłanie pakietów RST
28. Powiadomienie systemu IPS musi przybierać różne formy: Alarmowanie, wysyłanie maili, uruchomienie skryptów, ustawienie poziomów ważności zdarzeń.
29. Urządzenie musi posiadać wbudowany moduł kontroli antywirusowej z możliwością skanowania całych plików, wielokrotnie spakowanych (co najmniej 4 poziomy) dla ruchu http, FTP, SMTP, POP3, IMAP. Baza wzorców wirusów nie powinna być mniejsza niż 400 000 wpisów.
30. Urządzenie zabezpieczeń posiada wbudowany moduł filtrowania treści stron WWW wywoływanych przez użytkowników umożliwiający blokowanie adresów URL oraz adresów IP w oparciu o dostarczone przez producenta lub własne kategorie. Włączenie filtrowania treści stron WWW nie wymaga dodatkowego serwera. Istnieje możliwość samodzielnego tworzenia lokalnych białych i czarnych list adresów URL. Zewnętrzna baza adresów URL, z której korzysta system, nie powinna być mniejsza niż 26 milionów adresów z podziałem na kategorie.
31. Urządzenie zabezpieczeń posiada wbudowany moduł do filtrowania ruchu pozwalający określić niepożądany w sieci typ ruchu na podstawie następujących kryteriów: MIME, rozszerzenia plików, polecenia protokołów, oraz dla ruchu http blokowanie kontrolek ActiveX, apletów Java, obiektów Cookie, plików EXE oraz ZIP.
32. Urządzenie zabezpieczeń posiada wbudowany moduł antyspamowy z możliwością blokowania oraz oznaczania wiadomości e-mail.
33. System zabezpieczeń musi wykrywać i blokować ataki intruzów (in-line IDS), posiadać mechanizmy zarządzania pasmem sieci (QoS) oraz zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE   
    w konfiguracji site-to-site oraz client-to-site.
34. Urządzenie musi posiadać integrację z zewnętrznymi źródłami danych zawierającymi znane adresy C&C (Command&Control) oraz geoIP, swoje własne adresy IP lub passive sendbox.
35. 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.
36. Dostarczane urządzenie musi być objęte co najmniej 36-miesięcznym (3 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:
37. zgłaszanie uszkodzenia, awarii, błędu w dni robocze w godzinach pracy Zamawiającego (8-16)
38. wymiana urządzenia na następny dzień roboczy (NBD) po rozpoznaniu uszkodzenia, awarii, błędu w wyniku zgłoszenia przez Zamawiającego
39. 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.
40. **Migracja istniejącego rozwiązania na dostarczone Urządzenia**
41. Zamawiający posiada 2 lokalizacje w Warszawie:

Węzeł Komunikacyjny ul. Koszykowa 16 (WK) i węzeł komunikacyjny ul. Taborowa 33 (WT), oba ośrodki posiadają styk z siecią Internet. WK jest węzłem podstawowym a WT działa jako węzeł zapasowy. Obie lokalizacje połączone są punkt-punkt za pomocą własnego światłowodu. WK świadczy usługi dla pracowników Zamawiającego m.in. poczta, vpn., a także dostęp do sieci Internet dla pracowników. WT jest węzłem awaryjnym gdzie podczas normalnej pracy dostarcza dostęp do Internetu dla pracowników pracujących w lokalizacji Taborowa 33, w przypadku awarii łącza w WK, przejmuje rolę łącza podstawowego.

Urządzenia obsługujące WK to 2 Juniper SRX 650 działające w klastrze Active-Passive.

Urządzenia obsługujące WT to 2 Juniper SRX 110 działające w klastrze Active-Passive.

Urządzenia te zarządzane są poprzez centralny system zarządzający Juniper Junos Space moduł Security Director.

1. Wykaz prac:
2. Wykonanie analizy istniejącego rozwiązania
3. Uruchomienie dostarczonych w ramach postępowania urządzeń w klastrze Active-Active, po jednym urządzeniu w węźle.
4. Podłączenie dostarczonych w ramach postępowania urządzeń do centralnego systemu zarządzania Juniper Junos Space
5. Przeniesienie istniejących usług na dostarczone w ramach postępowania urządzenia dla obu węzłów
6. Uruchomienie mechanizmów ochrony przed awariami elementów sprzętowych   
   i programowych systemu zabezpieczeń oraz łączy sieciowych.
7. Uruchomienie mechanizmów bezpieczeństwa – pełny UTM
8. Wykonanie testów akceptacyjnych.
9. Wykonanie testów wydajnościowych urządzeń dostarczonych w ramach postępowania. Testy muszą potwierdzić parametry minimalne parametrów technicznych
10. **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 wydajnościowe urządzeń dostarczonych w ramach postępowania np. ochrona przed atakami DoS i DDoS, Stateful Firewall dla ruchu IMIX dla pełnego UTM

### 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 oraz w co najmniej 2 wersjach papierowych. Dodatkowo w oddzielnym dokumencie Wykonawca dostarczy zestawienie haseł i loginów.

1. **Szkolenia**
2. Zamawiający wymaga przeprowadzenia autoryzowanych przez producenta urządzeń szkoleń dla 3 osób. Szkolenia muszą się składać się z bloków tematycznych zawierających następujący zakres:
3. Podstawy administrowania systemem Junos Space – szkolenie co najmniej 2 dni
4. Wprowadzenie do Junos Space
5. Zagadnienia związane z instalacją Junos Space
6. Administracja systemem
7. Zarządzanie urządzeniami sieciowymi
8. Szablony konfiguracji
9. Automatyzacja działań administratora
10. JUNOS w urządzeniach zabezpieczeń – szkolenie co najmniej 5 dni
11. Wprowadzenie w tematykę platform zabezpieczeń JUNOS
12. Koncepcja stref oraz ochrona screening
13. Polityki bezpieczeństwa
14. Zarządzanie politykami za pomocą Security Directora
15. Zaawansowane polityki bezpieczeństwa
16. Rozwiązywanie błędów ze strefami i politykami bezpieczeństwa
17. NAT – translacja adresów
18. Zaawansowane funkcje NAT
19. Koncencja tuneli IPSec VPN
20. Implementacja IPSEC
21. Hub-and-Spoke VPN
22. Group VPN
23. PKI oraz ADVPN
24. Dodatkowe zagadnienia konfiguracji IPSec
25. Rozwiązywanie problemów w tunelach IPSec
26. Koncepcja klastrowania urządzeń
27. Budowanie klastra niezawodnościowego
28. Rozwiązywanie problemów w klastrze niezawodnościowym
29. Bezpieczeństwo w systemie JUNOS – szkolenie co najmniej 5 dni
30. Funkcje L2 w Junos Security oraz ich zabezpieczenia
31. Wirtualizacja
32. Moduł AppSecure
33. Implementacja AppSecure
34. Zarządzanie systemem Log Director
35. Sky ATP w teorii
36. Implementacja SkyATP
37. Implementacja funkcji UTM
38. Wprowadzenie do systemu IPS
39. Konfiguracja oraz polityki IPS
40. Software Defined Secure Network
41. Identyfikacja,monitorowanie i raportowanie
42. Rozwiązywanie problemów na platformach SRX
43. Szkolenia muszą się odbyć w Warszawie. Wykonawca musi zapewnić sale wykładowe wraz z wyposażeniem i sprzętem niezbędnym do przeprowadzenia szkoleń. Wykonawca zobowiązany jest do zapewnienia obsługi technicznej sprzętu w trakcie szkoleń.
44. Szkolenie musi się odbywać w dni robocze od poniedziałku do piątku, w godzinach 8 – 17.
45. Szkolenie musi być prowadzone w języku polskim, Zamawiający dopuszcza, aby materiały i prezentacje były w języku angielskim.
46. Uczestnicy szkolenia muszą otrzymać certyfikat jego ukończenia.
47. Zamawiający wymaga dostarczenia dla każdego uczestnika szkolenia materiałów szkoleniowych w postaci papierowej i elektronicznej.
48. Zamawiający wymaga zapewnienia w dniu zajęć, jednego ciepłego posiłku (obiad dwudaniowy) oraz napojów: kawa, herbata, woda mineralna, drobne przekąski   
    (np. ciasteczka, owoce) itp. dla każdego uczestnika.