OPIS PRZEDMIOTU ZAMÓWIENIA
DOT. ROZBUDOWA INFRASTRUKTURY SIECIOWEJ W PODZIALE NA 3 CZĘŚCI

I.NAZWA ZAMÓWIENIA

Przedmiotem zamówienia jest „**Rozbudowa infrastruktury sieciowej w podziale na 3 części**", w szczególności:

- wymiana zewnętrznych zapór sieciowych;
- wymiana strukturalnych przełączników sieciowych;
- zakup i wdrożenie klastra deduplikatorów w celu modernizacji systemu kopii zapasowych;

II.INFORMACJE SZCZEGÓŁOWE DOTYCZĄCE PRZEDMIOTU ZAMÓWIENIA

CZĘŚĆ I - WYMIANA ZEWNĘTRZNYCH ZAPÓR SIECIOWYCH

Przedmiotem zamówienia jest dostawa i wdrożenie systemu zewnętrznych zapór sieciowych - zbudowany jako redundantny układ 2 urządzeń typu firewall pracujących w trybie klastra niezawodnościowego (tzw. tryb HA – High Availability, active-passive), dostawy i konfiguracji subskrypcji/ licencji:

- sygnatur ataków/ (IPS, wykrywania zagrożeń sieciowych, zabezpieczeń antywirusowych,
- katalogu zagrożeń na podstawie URL (URL Filtering),
- zdalnego dostępu oraz dostarczeniem Dokumentacji Powykonawczej.

Zamawiający obecnie wykorzystuje klaster urządzeń PaloAlto PA-3020. W ramach dostawy Wykonawca przeprowadzi instalacje i wdrożenie polegające na przeniesieniu konfiguracji (około 200 reguł), W skład sytemu wchodzi dostęp zdalny VPN (Global Protect) oraz dostęp zdalny bezagentowy. W ramach konfiguracji skonfigurowane są niezależne wirtualne routery. Urządzenia pełnią rolę serwera DCHP dla wybranych podsieci. Urządzenia posiadają skonfigurowane połączenie site-to-site z innym firewallem PaloAlto.

W ramach dostawy dostarczone zostanie 8 wkładek 10Gbase-SR zgodnych z dostarczonym systemem oraz 8 wkładek 1000Base-SX. (4 wkładki 10Gbase-SR i 4 wkładki 1000Base-SX do każdego urządzenia)

Pracownicy Zamawiającego ukończyli certyfikowane szkolenia z zakresu instalacji, konfiguracji i administracji urządzeniami PaloAlto. W przypadku zaoferowania rozwiązania innego niż PaloAlto Wykonawca zapewni certyfikowane szkolenia z zakresu instalacji, konfiguracji i administracji dostarczonymi urządzeniami dla 6 pracowników Zamawiającego.

Zamawiający korzysta z systemu PAM CyberArk, który zarządza kontami użytkowników w obecnie eksploatowanych Firewallach PaloAlto (dysponuje odpowiednimi konektorami). W przypadku zaproponowania rozwiązania innego niż PaloAlto Wykonawca dostarczy i skonfiguruje odpowiednie konektory do zarzadzania kontami użytkowników dla dostarczonego rozwiązania w sposób, który nie narazi Zamawiającego na utratę gwarancji na rozwiązanie PAM.

Zamawiający wykorzystuje pomiędzy obecnie eksploatowanymi firewallami funkcjonalność przekazywania informacji o użytkownikach (User-ID). Wymagane jest aby dostarczone rozwiązanie przekazywało i przyjmowało informację o użytkownikach pomiędzy dostarczonymi firewallami, a obecnie eksploatowanymi PaloAlto PA-3250. Informacja o użytkownikach musi być odnotowywana w logu ruchu sieciowego i musi być możliwość tworzenia reguł na podstawie informacji o użytkowniku. Sposób przekazywania informacji o użytkownikach musi być wspierany przez posiadane przez Zamawiającego urządzenia PA-3250.

Zamawiający korzysta ze zdalnego dostępu w oparciu o agentów GlobalProtect. Dostarczone rozwiązanie musi być kompatybilne z wykorzystywanym oprogramowaniem klienta VPN lub Wykonawca przeprowadzi migrację klienta na około 250 komputerach zamawiającego i na około 250 telefonach (Android i IOS) zamawiającego. Migracja musi odbywać się w sposób niezauważalny dla użytkowników.

Dostawa subskrypcji/licencji na użytkowanie wdrażanego Systemu zostanie dokonana do siedziby Zamawiającego, tj. na adres ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa.

Sprzęt zostanie dostarczony, zainstalowany i wdrożony w siedzibie Zamawiającego i Lokalizacji Zapasowej na terenie Warszawy.

Zamawiający wymaga aby wdrożony System posiadał funkcje Sandbox. Dostawa Systemu nie obejmuje dostawy licencji/subskrypcji na funkcje Sandbox.

OPIS TECHNICZNY I WYMAGANIA FUNKCJONALNE POJEDYŃCZEGO URZĄDZENIA

Id.	**Kategoria wymagania**	Opis wymagania
WP1	Wymagania podstawowe	System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenia zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość Systemu musi być dostarczona i wspierana przez jednego producenta.
WP2	Wymagania podstawowe	System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 5 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 2,2 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 1 000 000 jednoczesnych połączeń.
WP3	Wymagania podstawowe	System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000, minimum 4 porty 1Gbps/10Gbps SFP/SFP+ oraz 4 wkładek 10Gbase-SR, minimum 4 porty 1Gbps SFP oraz 4 wkładki 1000Base-SX. Wkładki nie mogą w jakikolwiek sposób negatywnie wpływać na prawidłową pracę Systemu oraz warunki gwarancji na System. Wkładki składają się na System. Wykonawca zobowiązany jest do zapewnienia prawidłowego działania wdrożonego Systemu jako całości w Systemie informatycznym Zamawiającego, jak również każdego z elementów wdrożonego Sytemu oraz zobowiązany jest do zapewnienia gwarancji na cały System oraz na każdy z elementów wdrożonego Sytemu.
WP4	Wymagania podstawowe	Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie przełącznika (tzn. w warstwie 2 modelu OSI), w trybie transparentnym oraz w trybie pasywnego nasłuchu (sniffer). 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.
WP5	Wymagania podstawowe	System zabezpieczeń firewall musi obsługiwać terminowanie tuneli GRE.
WP6	Wymagania podstawowe	Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych

		powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
WP7	Wymagania podstawowe	System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne ze standardem IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.
WP8	Wymagania podstawowe	System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tablica routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
WP9	Wymagania podstawowe	System zabezpieczeń 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).
WP10	Wymagania podstawowe	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).
WP11	Wymagania podstawowe	System zabezpieczeń firewall 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.
WP12	Wymagania podstawowe	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.
WP13	Wymagania podstawowe	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. Wydajność kontroli firewall i kontroli aplikacji musi być taka sama i wynosić w ruchu full-duplex nie mniej niż 5 Gbit/s.
WP14	Wymagania podstawowe	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).
WP15	Wymagania podstawowe	Nie jest dopuszczalne, aby blokowanie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
WP16	Wymagania podstawowe	Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
WP17	Wymagania podstawowe	System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf itp.) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. System zabezpieczeń musi obsługiwać inspekcję protokołu http/1.x oraz http/2.0.
WP18	Wymagania podstawowe	System zabezpieczeń firewall musi wykonywać inspekcję danych przesyłanych wewnątrz tuneli VXLAN.
WP19	Wymagania podstawowe	System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
WP20	Wymagania podstawowe	System zabezpieczeń firewall musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (AV, IPS, AS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, AS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.

WP21	Wymagania podstawowe	System zabezpieczeń 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.
WP22	Wymagania podstawowe	System zabezpieczeń 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.
WP23	Wymagania podstawowe	System zabezpieczeń firewall musi zapewniać ochronę przed atakami typu „Drive-by-download" poprzez możliwość konfiguracji strony blokowania z dostępną akcją „kontynuuj" dla funkcji blokowania transmisji plików.
WP24	Wymagania podstawowe	System zabezpieczeń 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.
WP25	Wymagania podstawowe	System zabezpieczeń 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.
WP26	Wymagania podstawowe	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący ruch SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.
WP27	Wymagania podstawowe	System zabezpieczeń musi posiadać wbudowaną i automatycznie aktualizowaną 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 stanowi automatyczne wyjątki od ogólnych reguł deszyfracji.
WP28	Wymagania podstawowe	System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
WP29	Wymagania podstawowe	System zabezpieczeń firewall musi zapewniać możliwość rozbudowy do klastra Active-Active zbudowanego z minimum 4 urządzeń rozproszonych w dwóch Data Center.
WP30	Wymagania podstawowe	Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt), fabrycznie nowe, pochodzić z oficjalnego kanału sprzedaży w Polsce.
WPI1	Wymagania podstawowe identyfikacja użytkownika	System zabezpieczeń 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.

WPI2	Wymagania podstawowe identyfikacja użytkownika	System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów MS Windows oraz innych niż MS Windows (np. Linux lub Unix) w celu łączenia nazw użytkowników z adresami IP hostów z których ci użytkownicy nawiązują połączenia. Funkcja musi umożliwiać wykrywanie logowania jak również wylogowania użytkowników.
WPI3	Wymagania podstawowe identyfikacja użytkownika	System zabezpieczeń 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.
WPI4	Wymagania podstawowe identyfikacja użytkownika	Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
WO1	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń 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 i posiadać nie mniej niż 20 milionów rekordów URL.
WO2	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW, który można uruchomić per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
WO3	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
WO4	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.
WO5	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń 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 przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
WO6	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać modułu inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
WO7	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać modułu wykrywania i blokowania ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
WO8	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać moduł IPS/IDS uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).

WO9	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
WO10	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
WO11	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać moduł anty-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anty-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
WO12	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
WO13	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
WO14	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać funkcję 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).
WO15	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń 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.
WO16	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać funkcję automatycznego przeglądania logowanych informacji oraz pobierania z nich źródłowych i docelowych adresów IP hostów biorących udział w konkretnych zdarzeniach zdefiniowanych według wybranych atrybutów. Na podstawie zebranych informacji musi istnieć możliwość tworzenia obiektów wykorzystywanych w konfiguracji urządzenia w celu zapewnienia automatycznej ochrony lub dostępu do zasobów reprezentowanych przez te obiekty.
WO17	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów, do których użytkownicy mogą wysyłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
WO18	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
WO19	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi zapewniać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msoffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus, czyli nie mniej niż 2.2 Gbit/s, w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo

		wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
WO20	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych pomiędzy konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
WO21	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msoffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.
WO22	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	System zabezpieczeń firewall musi generować raporty dla każdego analizowanego pliku tak, aby administrator miał możliwość sprawdzenia, które pliki i z jakiego powodu zostały uznane za złośliwe, jak również sprawdzić którzy użytkownicy te pliki pobierali.
WO23	Wymagania ochrony IPS, AV, Anty-Spyware, URL, Zero-Day	Dostarczenie subskrypcji na funkcje Sand-box nie jest wymagane na tym etapie postępowania – taka rozbudowa ma być możliwa w przyszłości bez dokupowania dodatkowego hardware po instalacji odpowiedniej subskrypcji/licencji.
WD1	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System zabezpieczeń 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.
WD2	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
WD3	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System zabezpieczeń firewall musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
WD4	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System zabezpieczeń 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 routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych (Android, IOS) musi odbywać się na bazie technologii SSL VPN – obsługa nie mniej niż 1000 jednoczesnych połączeń. Jeśli funkcja wymaga dodatkowej licencji lub subskrypcji musi być dostarczona w ramach postępowania.
WD5	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System zabezpieczeń 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.
WD6	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System zabezpieczeń 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.
WD7	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System zabezpieczeń 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.

WD8	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
WD9	Wymagania dodatkowe NAT, DOS, IPSEC, VPN, SSL VPN, QOS	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. Musi istnieć możliwość przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego.
WDW1	Wymagania dodatkowe Środowisko wirtualne VMware	System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.
WZR1	Wymagania 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.
WZR2	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi posiadać koncept konfiguracji kandydackiej, którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu.
WZR3	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
WZR4	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
WZR5	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi być wyposażony w interfejs XML API będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI).
WZR6	Wymagania zarządzanie i raportowanie	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.
WZR7	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
WZR8	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
WZR9	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. 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.
WZR10	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
WZR11	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.

WZR12	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
WZR13	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
WZR14	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
WZR15	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall 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.
WZR16	Wymagania zarządzanie i raportowanie	System zabezpieczeń 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.
WZR17	Wymagania zarządzanie i raportowanie	System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
WZR18	Wymagania zarządzanie i raportowanie	System zabezpieczeń 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.
WWG1	Wymagania dotyczące wsparcia i gwarancji	W ramach przedmiotu zamówienia zostanie: a) udzielona minimum 36-miesięczna gwarancja na dostarczony oraz wdrożony System – liczona od dnia podpisania przez obie strony bez zastrzeżeń protokołu odbioru końcowego przedmiotu zamówienia, b) zapewnione minimum 36-miesięczne wsparcie techniczne i subskrypcja - od dnia podpisania bez zastrzeżeń przez obydwie strony protokołu odbioru końcowego przedmiotu zamówienia.
WWG2	Wymagania dotyczące wsparcia i gwarancji	Tryb świadczenia gwarancji: a) dostępność serwisu w okresie gwarancji – 24 godziny na dobę przez 7 dni w tygodniu, b) zgłoszenia będą przyjmowane przez wykonawcę usługi gwarancyjnej telefonicznie lub na adres mailowy lub przez dedykowany portal zgłoszeniowy, c) czas naprawy (przywrócenie stanu funkcjonowania systemu sprzed awarii) – następny dzień roboczy następujący po dniu zgłoszenia (Next Business Day - NBD), d) serwis w okresie gwarancji musi być świadczony w miejscu wdrożenia systemu firewall, czyli w siedzibie Zamawiającego oraz Lokalizacji Zapasowej. e) usunięcie uszkodzenia nienaprawialnego nastąpi w terminie wskazanym w lit. c, poprzez wymianę na sprzęt sprawny o co najmniej takich samych walorach funkcjonalnych, f) zapewniona naprawa lub wymiana urządzeń lub ich części na części nowe i oryginalne, zgodnie z metodyką z zaleceniami producenta sprzętu. g) wymienione urządzenia lub elementy muszą być objęte takim samym zakresem usług serwisowych jakim objęte były urządzenia i elementy, które zostały wymienione. h) wykonawca usługi gwarancyjnej ponosi wszystkie koszty napraw gwarancyjnych, włączając w to koszty części i transportu.

WWG2	Wymagania dotyczące wsparcia i gwarancji	Wsparcie techniczne: a) musi być świadczone przez producenta lub jego autoryzowanego polskiego przedstawiciela, b) będzie świadczone telefonicznie oraz drogą elektroniczną, c) obejmuje: dostęp do nowych wersji oprogramowania, aktualizację bazy aplikacji, sygnatur ataków IPS, definicji wirusów, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. d) Wsparcie techniczne dla oprogramowania rozumiane jest jako gotowość przystąpienia do rozwiązywania problemów technicznych związanych z oprogramowaniem systemu firewall w trybie 8 godzin na dobę, 5 dni roboczych w tygodniu
WT1	Wymagania dotyczące testów	Testy: a) weryfikacja dostępu do sieci zewnętrznych (m.in. Internet, SIP trunk) b) weryfikacja dostępu z sieci Internet do zasobów publikowanych w sieci Zamawiającego c) weryfikacja połączeń klientów VPN d) weryfikacja połączeń VPN site-to-site e) weryfikacja przełączenia węzłów klastra (planowe i awaryjne) f) weryfikacja identyfikacji użytkowników i przekazywania informacji o użytkownikach między urządzeniami posiadanymi przez Zamawiającego g) weryfikacja zarządzania kontami administracyjnymi w systemie PAM

CZĘŚĆ II – WYMIANA STRUKTURALNYCH PRZEŁĄCZNIKÓW SIECIOWYCH

Przedmiotem zamówienia jest dostawa trzech przełączników sieciowych wraz z dodatkowym wyposażeniem.

Zamawiający obecnie wykorzystuje przełączniki HP serii 5400 oraz HP serii 6600 w ramach dostawy Wykonawca przeprowadzi instalacje i wdrożenie polegające na odzwierciedleniu obecnej konfiguracji m.in. VLANy, STP, LACP

Zamawiający wykorzystuje do zarządzania i monitorowania przełącznikami sieciowymi oprogramowanie Intelligent Management Center IMC). Zamawiający wymaga aby dostarczone przełączniki były natywnie wspierane przez ww. oprogramowanie do zarządzania przełącznikami. W przypadku gdy dostarczone przełączniki nie będą wspierane natywnie przez oprogramowanie IMC Wykonawca dostosuje i skonfiguruje oprogramowanie w taki sposób aby możliwe było zarządzanie i monitorowanie dostarczonych urządzeń sieciowych. Wymagane jest aby kastomizacja oprogramowania była trwała i nie wymagała ponownej kastomizacji po aktualizacji oprogramowania IMC.

Zamawiający korzysta z systemu PAM CyberArk, który zarządza kontami użytkowników w obecnie eksploatowanych przełącznikach sieciowych HPE/ARUBA (dysponuje odpowiednimi konektorami dla urządzeń HPE/ARUBA). W przypadku zaproponowania innego rozwiązania Wykonawca dostarczy i skonfiguruje odpowiednie konektory do zarzadzania kontami użytkowników dla dostarczonych urządzeń w sposób, który nie narazi Zamawiającego na utratę gwarancji na rozwiązanie PAM.

Wyposażenie dodatkowe:

- 80 sztuk - wkładka SFP+ 10G Ethernet SR LC
- 8 sztuk – kabel DAC 10G SFP+ SFP+ o długości 1,5 metra
- 4 sztuki – kabel DAC 10G SFP+ SFP+ o długości 5 metrów
- wyposażenie dodatkowe musi być tego samego producenta co producent przełączników
- gwarancja producenta na wkładki optyczne i kable DAC na okres 36 miesięcy

Wymagania pojedynczego urządzenia:

1. Obudowa przełącznika
   - Obudowa modularna umożliwiająca montaż w standardowej szafie typu RACK 19”
   - Ilość dedykowanych slotów na karty liniowe minimum 5
   - Ilość dedykowanych slotów na karty zarządzające minimum 2.
   - Urządzenie powinno być wyposażone w 1 moduł zarządzający z możliwością rozbudowy do dwóch.
   - Ilość dedykowanych slotów na zasilacze minimum 2
   - Ilość dedykowanych slotów na układy wentylujące (fan tray) minimum 2
   - Maksymalna wysokość obudowy 45cm [7U]
   - Maksymalna głębokość obudowy 45cm

2. Zasilanie i wentylacja
   - Minimum 2 układy wentylacji (Fan Tray)
   - Przepływ powietrza chłodzącego w trybie front-to-back lub back-to-front.
   - Minimum dwa redundantne zasilacze wewnętrzne 230V AC
   - Maksymalny pobór mocy pojedynczego zasilacza 1800W.
   - Możliwość wymiany jednego z zasilaczy w trybie hot-swap (w trakcie pracy urządzenia).

3. Wymagane ilość portów:
   - Port konsoli szeregowej RS-232C RJ45
   - Port konsoli USB
   - Port zarządzania w trybie out-of-band typu Ethernet
   - Port USB na potrzeby instalacji konsoli bezprzewodowej np. Bluetooth
   - 48 porty 25 Gigabit Ethernet na wkładki SFP28, porty 25G SFP28 muszą mieć możliwość pracy także w trybie 10 Gigabit Ethernet z wkładkami SFP+ i trybie 1 Gigabit Ethernet z wkładkami SFP
   - 48 portów 1 Gigabit Ethernet 1000Base-T z zasilaniem PoE+ w standardzie IEEE 802.3at Power over Ethernet (dostępny budżet mocy PoE nie mniejszy niż 300W)
   - Na potrzeby rozbudowy ilości portów, po wyposażeniu urządzenia w wymagane porty, muszą zostać co najmniej 3 sloty wolne na dodatkowe karty liniowe. Przełącznik musi mieć możliwość doposażenia w kartę liniową z portami 24 Ethernet 10GBase-T.

4. Parametry wydajnościowe

   - Przepustowość matrycy przełączającej minimum 14Tb/s
   - Przepustowość przełącznika w ilości pakietów 5,7 Bpps
   - Średnie opóźnienia dla pakietów 64B i portów 1Gb Ethernet nie większe niż 6 µS
   - Średnie opóźnienia dla pakietów 64B i portów 10/25Gb Ethernet nie większe niż 3 µS
   - Średnie opóźnienia dla pakietów 64B i portów 40/100Gb Ethernet nie większe niż 2 µS
   - Rozmiar tablicy MAC address: 32 768
   - Rozmiar tablicy routingu IPv4: 60 000
   - Rozmiar tablicy routingu IPv4: 16 000
   - Rozmiar tablicy multicast routing: 8000
   - Rozmiar tablicy ARP: 49000
   - Ilość grup IGMP: 8000
   - Ilość grup MLD: 8000
   - Ilość portów SVI (Switched Virtual Interfaces): 1024
   - Ilość obsługiwanych VLAN ID min. 4000 (802.1q)
   - Ilość zagregowanych grup połączeń w trybie IEEE 802.3ad LACP: 256 LAGs
   - Ilość połączeń w ramach grupy LAG do 8

5. Zarządzanie:

- Zarządzanie urządzeniem za pomocą: linii komend CLI, przeglądarki www w trybie GUI (http lub https), protokołów telnet lub SSHv2.
- Zarządzenie przy pomocy zapytań REST API
- Możliwość uruchamiania skryptów Python
- Możliwość przechowywania co najmniej 2 wersji oprogramowania systemowego w pamięci nieulotnej
- Możliwość przechowywania co najmniej 4 wersji konfiguracji systemu w pamięci nieulotnej
- Możliwość zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
- Obsługa SNTP lub Network Time Protocol (NTP)
- Wsparcie dla RMON przynajmniej grupy: events, alarms, history, statistics
- Wsparcie dla sFLOW lub odpowiednika.
- Wsparcie dla mechanizmów SNMP v2c/v3, ICMP.
- Zarządzenie przez protokół IPv4 i IPv6 (dual-stack)
- Możliwość nadawanie portom własnych nazw

6. Funkcje warstwy L2

- Obsługa sieci VLAN zgodnie z 802.1q
- Agregacja portów zgodna z 802.3ad LACP
- Obsługa ramek Jumbo 9198B
- Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol oraz Rapid Per-VLAN Spanning Tree (RPVST+)
- Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
- Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD)
- Port mirroring: możliwość kopiowania ruchu z portu;
- Obsługa ruchu Multicast ze wsparciem dla Internet Group Management Protocol (IGMP) i IGMP Snooping;
- Obsługa ruchu Multicast ze wsparciem dla Multicast Service Discovery Protocol (MSDP) i MSDP Anycast RP oraz MLD Snooping
- Wsparcie dla funkcji smart-link umożliwiające zapewnienie redundancji połączeń bez konieczności stosowania protokołu Spaning Tree Protocol

7. Funkcje warstwy L3:

- Routing IPv4 – minimum: statyczny, RIP, OSPF, BGP-4
- Routing IPv6 – minimum: statyczny, RIPng, OSPFv3, MP-BGP
- Routing w trybie policy route
- Routing w trybie Equal-Cost Multipath (ECMP)
- Routing Multicast zgodnie z Protocol Independent Multicast (PIM) Sparse Mode (SM) i Dense Mode (DM) dla protokołu IPv4 i IPv6
- Wsparcie dla VRF/VFR-lite minimum 256 instancji
- Funkcja bramy wirtualnej zgodnie z Virtual Router Redundancy Protocol (VRRP) dla IPv4 i IPv6
- Wsparcie dla funkcji Dynamic Host Configuration Protocol (DHCP) server, DHCP Relay
- Możliwość tunelowania ruchu IPv4 i IPv6 w tunelach VXLAN/EVPN
- Optymalizacja pracy sieci VXLAN przez ograniczanie ruchu typu ARP i ND w segmentach sieci VXLAN
- Wsparcie dla serwisu Domain Name System (DNS)

- Funkcjonalność tunelowania ruch LAN w sieciach VXLAN ze wsparciem Multi-Protocol BGP eVPN jako protokołu kontrolnego.
- Funkcjonalność tunelowania ruch LAN w sieciach VXLAN z możliwością statycznej definicji tunelowania.
- Funkcjonalność Generic Routing Encapsulation (GRE) na potrzeby tunelowania ruchu L2/L3 w sieciach L3

8. Funkcje QoS

- Wsparcie dla mechanizmów QoS: strict priority (SP) queuing i deficit weighted round robin (DWRR) lub odpowiedniki
- Obsługa standardu 802.1p Class of Service (CoS) i DiffServ
- Wsparcia dla ograniczania pasma Rate limiting
- Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres IP, źródłowy/docelowy port TCP/UDP, IP Type of Service (ToS), port źródłowy
- Prioryteryzacja zgodna z 802.1p
- Zabezpieczenie przed sztormami pakietów typu broadcast i multicast z możliwością ustalania przez administratora progów.

9. Funkcje wirtualizacji

- Przełączniki tego samego typu muszą posiadać funkcję łączenia w cluster niezawodnościowy złożony z 2 urządzeń.
- Urządzenia połączone w klaster muszą symulować jedno logiczne urządzenie z punktu widzenia drugiej warstwy sieci Ethernet umożliwiając tworzenie zagregowanych połączeń Ethernet jednocześnie do obu przełączników klastra.
- Wymagana realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie.
- Przełączniki wchodzące w skład klastra powinny być zarządzane niezależnie.

10. Elementy bezpieczeństwa

- Funkcja autoryzacji/autentykacji za pomocą serwerów RADIUS (Remote Authentication Dial-In User Service) albo TACACS+ (Terminal Access Controller Access-Control System)
- Funkcja STP Root Guard oraz STP Bridge Protocol Data Units (BPDUs) port protection
- Funkcja DHCP Protection
- Wsparcie dla autentykacji i autoryzacji metodami IEEE 802.1X, Web i MAC authentication
- Możliwość tworzenia Access control lists (ACLs) na bazie informacji z warstw L2/3 modelu OSI (w szczególności na bazie adresów docelowych/źródłowych IP, portów TCP/UDP).
- Możliwość stosowania ACL dla sieci VLAN i portów.
- Wsparcie dla zabezpieczeń typu CPU protection
- Zabezpieczenie protokołu STP: STP BPDU Protection, STP Root Guard
- Wbudowane mechanizmy: Dynamic IP Lockdown i Port Security
- Secure FTP
- Wsparcie dla mechanizmów Dynamic ARP Protection lub odpowiednika
- Zintegrowany moduł trusted platform module (TPM)

11. Wymagania gwarancyjne i wsparcie techniczne

Tryb świadczenia gwarancji:

a) dostępność serwisu w okresie gwarancji – 8 godzin na dobę przez 5 dni w tygodniu,
b) zgłoszenia będą przyjmowane przez wykonawcę usługi gwarancyjnej telefonicznie lub na adres mailowy lub przez dedykowany portal zgłoszeniowy,
c) czas naprawy (przywrócenie stanu funkcjonowania urządzeń sprzed awarii) – następny dzień roboczy następujący po dniu zgłoszenia (Next Business Day - NBD),
d) serwis w okresie gwarancji musi być świadczony w siedzibie Zamawiającego oraz Lokalizacji Zapasowej.
e) usunięcie uszkodzenia nienaprawialnego nastąpi w terminie wskazanym w lit. c, poprzez wymianę na sprzęt sprawny o co najmniej takich samych walorach funkcjonalnych,
f) zapewniona naprawa lub wymiana urządzeń lub ich części na części nowe i oryginalne, zgodnie z metodyką z zaleceniami producenta sprzętu.
g) wymienione urządzenia lub elementy muszą być objęte takim samym zakresem usług serwisowych jakim objęte były urządzenia i elementy, które zostały wymienione.
h) wykonawca usługi gwarancyjnej ponosi wszystkie koszty napraw gwarancyjnych, włączając w to koszty części i transportu.
i) Zamawiający ma prawo do bezpośredniego zgłaszania usterek i awarii sprzętu do producenta na poziomie 8x5 przez okres trwania gwarancji.
j) gwarancja musi obejmować chassis, moduły liniowe, moduły zarządzania, zasilacze i wentylatory.

Wsparcie techniczne:
a) musi być świadczone przez producenta lub jego autoryzowanego polskiego przedstawiciela,
b) będzie świadczone telefonicznie oraz drogą elektroniczną,
c) obejmuje: dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
d) Wsparcie techniczne dla oprogramowania rozumiane jest jako gotowość przystąpienia do rozwiązywania problemów technicznych związanych z oprogramowaniem urządzeń w trybie 8 godzin na dobę, 5 dni roboczych w tygodniu

12. Wymagania ogólne

- Wszystkie wymagane funkcje muszą być dostępne bezterminowo.
- Jeżeli wymagane funkcjonalności wymagają odrębnych licencji to licencje te muszą być zawarte w ofercie.
- Producent oferowanego rozwiązania musi być sklasyfikowany w kwadracie Gartner Magic Quadrant for Wired/Wireless LAN Access Infrastructure w edycji aktualnej na dzień składania ofert.
- Oferowane przełączniki LAN i ich elementy, wkładki optyczne, przewody DAC muszą pochodzić od jednego producenta.
- Zamawiający wymaga by dostarczone urządzenia były fabrycznie nowe oraz nie były używane. Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
- Zamawiający wymaga, aby całość dostarczanego sprzętu i oprogramowania pochodziła z autoryzowanego kanału sprzedaży producenta i wymaga by przed podpisaniem umowy dołączyć certyfikat legalności produktów - oświadczenie z oficjalnego kanału dystrybucji na rynek Polski danego producenta potwierdzające, że dostawca jest autoryzowanym partnerem oraz że produkty i wsparcie oferowane klientowi pochodzą z autoryzowanego i legalnego kanału sprzedaży oraz posiadają wsparcie producenta.
- Zamawiający wymaga, aby sprzęt zakupiony przez zamawiającego był zarejestrowany w systemach producenta na Zamawiającego jako klient końcowy.

CZĘŚĆ III – ZAKUP I WDROŻENIE KLASTRA DEDUPLIKATORÓW W CELU MODERNIZACJI SYSTEMU KOPII ZAPASOWYCH

Przedmiotem zamówienia jest dostawa 2 urządzeń do przechowywania kopii zapasowych tzw. deduplikatorów wraz z instalacją, konfiguracją i uruchomieniem.

W ramach zamówienia Wykonawca:

- Dostarczy i zainstaluje urządzenia w PCPD i ZCPD Zamawiającego, znajdujących się w Warszawie
- Podłączy urządzenia do sieci elektrycznej oraz skonfiguruje połączenie do sieci LAN i SAN Zamawiającego
- Skonfiguruje polaczenia pomiędzy dostarczonymi urządzeniami (replikacja)
- Zintegruje urządzenia z posiadamy przez Zamawiającego systemem Veeam Backup&Replication 9.5 lub nowszym.
- W ramach wdrożenia Wykonawca jest zobowiązany do przeprowadzenia warsztatów szkoleniowych na dostarczonym sprzęcie obejmujących zakres instalacji i konfiguracji w zakresie co najmniej:
    - konfiguracja deduplikatorów;
    - konfiguracja mechanizmów przełączania urządzeń w razie awarii;
    - obsługa mechanizmów replikacji danych;
    - tworzenie, modyfikacja, usuwanie grup dyskowych;
    - konfiguracja urządzeń do współpracy z oprogramowaniem Veeam;
    - konfiguracja i obsługa mechanizmów kompresji i deduplikacji;
    - monitorowanie i statystyki wykorzystania urządzeń i linków połączeniowych.

Każde z dostarczonych urządzeń musi spełniać następujące wymagania funkcjonalne:

Nazwa elementu, parametru lub cechy	**Opis minimalnych wymagań**
Obudowa - rozbudowa	Możliwość rozbudowy do min. 5 modułów łącznie, 2U każdy moduł, czyli łącznie 10U.
Pojemność	Urządzenie musi posiadać przestrzeń netto co najmniej 99TB. Oznacza to, że na unikalne bloki wraz z metadanymi (informacjami o referencjach) mogą zajmować do 99TB netto.
Pojemność - rozbudowa	Urządzenie musi skalować się do co najmniej 315TB netto. Oznacza to, że na unikalne bloki wraz z metadanymi (informacjami o referencjach) mogą zajmować do 315TB netto. Cała dostępna przestrzeń musi znajdować się na urządzeniu niedopuszczalne jest użycie innych narzędzi, bramek czy mechanizmów tieringu do chmury (publicznej czy prywatnej) w celu zwiększenia pojemności. Rozbudowa pojemności wymaga jedynie zakupu odpowiedniej licencji na pojemność. Jeśli wraz z rozbudową urządzenia o pojemność wymagane jest dostarczenie dodatkowych komponentów (takich jak pamięci RAM, kontrolery

	SAS, półki rozszerzeń, dyski twarde) to komponenty te powinny być dostarczone (ilościowo i jakościowo z wymogami producenta) w ramach kosztu licencji.
Appliance	Urządzenie musi być rozwiązaniem kompletnym w postaci gotowego urządzenia (appliance'a) łączące w sobie sprzęt i odpowiednie oprogramowanie realizujące funkcjonalności wymagane w tym postępowaniu. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway z uwagi na brak miarodajnych danych dotyczących ich wydajności oraz dostępności. Zamawiający dopuszcza możliwość rozbudowy urządzenia przez dodanie modułów dyskowych.
Interfejsy dostępowe	Zarządzanie urządzeniem oraz jego konfiguracją musi być możliwe z następujących poziomów: ● linia poleceń CMD, ● panel administracyjny WWW, ● RestAPI.
Deduplikacja	Technologia de-duplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych. Oznacza to, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości. Deduplikacja zmiennym blokiem musi być wykonywana dla wszystkich protokołów nieważne jakim interfejsem dostępowym zostały one zapisane na urządzeniu. Deduplikacja musi być globalna w ramach całego urządzenia - tj. musi być jedna baza deduplikatów, która globalnie obsługuje wszystkie referencje. Oznacza to, że unikalne bloki muszą referować z danymi, bez względu jak te dane zostały dostarczone do urządzenia (tj. nieważne jakim protokołem i interfejsem) oraz jak zostały logicznie podzielone w ramach danego protokołu (np. dwa share CIFS/SMB). Niedopuszczalne jest posiadanie kilku baz deduplikacji na jednym urządzeniu lub osiągniecie ofektu globalnej deduplikacji przez inne rozwiązania sprzętowe lub/i programowe. Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie znajdujące się jeszcze w systemie dyskowym urządzenia. Dla wybranych protokołów takich jak: ● OST, ● RMAN SBT API, ● deduplikacja dla systemów plików, deduplikacja musi odbywać się na źródle, tj. na systemie, który wysyła dane tym protokołem do deduplikatora.
Kompresja	Unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane.
Bezpieczeństwo	Urządzenie musi przechowywać dane na dyskach chronionych za pomocą technologii RAID6 lub równoważnej oferując taki sam lub wyższy poziom bezpieczeństwa – odporności na awarię nośnika.
Interfejsy sieciowe	Oferowane urządzenie musi posiadać minimum: ● 2 porty 1GbE Copper (miedź) ● 2 porty 10GbE Optical (wraz z modułam SFP)
Interfejsy sieciowe - rozbudowa	Możliwość rozbudowy o kolejne 2 karty rozszerzeń. Każda karta może posiadać następujące, dowolne warianty: ● 4 porty 10GbE Copper (miedź), ● 4 porty 10GbE Optical (wraz z modułami SFP),

	● 2 porty 25GbE DAC (wraz z odpowiednim okablowaniem) lub Optical (wraz z modułami SFP28), ● 2 porty 16GbFC Optical.
Protokoły - obsługa	Oferowany produkt musi posiadać wsparcie dla następujących protokołów dostępowych: ● CIFS/SMB, ● NFS, ● OST, ● RMAN SBT API, ● Deduplikacja na źródle dla systemu plików. Dla wszystkich wymienionych protokołów musi być dostarczona licencja wieczysta która opiewa na maksymalną pojemność netto urządzenia.
Protokoły - obsługa - rozbudowa	Urządzenie musi posiadać mechanizmy integracji z oprogramowaniem Veeam poprzez wykorzystanie dodatkowego protokołu: Veeam Data Mover Service (VDMS). Dostarczona funkcjonalność licencja musi pozwalać: ● obsługę na całej pojemności urządzenia ● umożliwiać replikację tego protokołu, ● na deduplikację zasobów przyjmowanych tym protokołem ● integrację z funkcjonalnością Fast Clone (ReFS lub XFS).
Protokoły - liczba urządzeń	Urządzenie musi umożliwiać składowanie danych poprzez udostępnianie min.: ● 128 zasobów NAS w sieci Ethernet wykorzystując protokoły CIFS/SMB, NFS, RMAN SBT API, deduplikację na źródle dla systemu plików,
Protokoły - wydajność	Urządzenie musi oferować wydajność co najmniej dla protokołu: ● OST - 17TB/h, ● NFS - 16,5TB/h, ● CIFS/SMB - 14TB/h, ● RMAN SBT API, deduplikacja na źródle dla systemu plików - 34TB/h,
Replikacja	Urządzenie musi umożliwiać replikacji danych z mniejszymi i większymi modelami urządzeń tego samego producenta jak również z modelami wirtualnymi. Replikacja musi być możliwa w trybie co najmniej 10 do 1 (many to one) oraz co najmniej 1 do 2 (fan out). Wymagane jest dostarczenie licencji, pozwalającej na obsługę replikacji dla wszystkich protokołów CIFS/SMB, NFS, OST, RMAN SBT API i deduplikacji na źródle dla systemu plików. Replikowane dane w trakcie transmisji muszą być szyfrowane kluczem min. 256bit - np. AES 256. Replikacja może być skonfigurowana w trybie: ● asynchroninym - na podstawie harmonogramu, ● semisynchronicznym - w trybie rzeczywistym, dane są replikowane na drugie urządzenie w czasie rzeczywistym. Potwierdzenie replikacji jest wykonywane automatycznie po zamknięciu pliku (CIFS/SMB), po maksymalnie 5 minutach (NFS). Licencje muszą być dostarczone na całe urządzenie i do pełnej pojemności urządzenia.
Monitorowanie	Urządzenie musi posiadać zestaw oprogramowania umożliwiający monitorowanie wydajności aktualnej oraz historycznej (do 6 lat wstecz) w zakresie co najmniej: ● wykorzystania CPU, ● wykorzystania przestrzeni dyskowej (przed deduplikacją, po deduplikacji), ● redukcji danych (z podziałem na kompresję i deduplikację), ● aktywności interfejsów sieciowych LAN i FC z uwzględnieniem interfejsów zaagregowanych (bond), ● dedykowane statystyki dla protokołu OST, ● wydajności deduplikacji,

	● wydajności procesów reklamacji, ● chargeback.
Kompatybilność	Oferowane urządzenie musi wspierać, co najmniej następujące aplikacje: ● Arcserve Arcserve Backup, ● Atempo Time Navigator, ● Commvault Simpana/Next Generation Platform, ● EMC NetWorker, ● IBM Tivoli Storage Manager/Spectrum Protect, ● Micro Focus/HP Data Protector, ● Nakivo BU and Replication, ● NovaStor NovaStor DataCenter, ● Oracle Oracle Recovery Manager (RMAN), ● Retrospect Inc Retrospect for Windows, ● Veeam Backup and Replication, ● Veritas Backup Exec, ● Veritas NetBackup, ● Veritas System Recovery.
Kompatybilność - RMAN SBT API	W przypadku współpracy z aplikacją Oracle RMAN, urządzenie musi umożliwiać deduplikację na źródle (de-duplikację po stronie media serwera). Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
Kompatybilność - system plików	W przypadku współpracy natywnymi systemami plików, urządzenie musi umożliwiać deduplikację na źródle (przed wysłaniem danych do urządzenia).
Kompatybilność - Veeam	W przypadku współpracy z aplikacją Veeam, urządzenie musi umożliwiać deduplikację po stronie usługi VDMS uruchomionej bezpośrednio na oferowanym urządzeniu. Deduplikacja taka musi zapewniać by z serwerów do urządzenia były transmitowane tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu. Integracja musi być poszerzona o: ● wykorzystanie techniki “Fast Clone” (dla systemu plików XFS) w procesie tworzenia kopii syntetycznych pełnych z poziomu aplikacji Veeam, ● hardeningu urządzenia do przyspieszenia operacji “Instant VM Recovery”. Wymagane jest dostarczenie licencji na wyżej wymienioną funkcjonalność.
Wymagania produktowe	Dostarczone urządzenie musi stanowić całość pochodzącą od jednego producenta (oprogramowanie oraz sprzęt), fabrycznie nowe, pochodzić z oficjalnego kanału sprzedaży w Polsce.
Wymagania dotyczące wsparcia i gwarancji	W ramach przedmiotu zamówienia zostanie: a) udzielona minimum 36-miesięczna gwarancja na dostarczony oraz wdrożony System – liczona od dnia podpisania przez obie strony bez zastrzeżeń protokołu odbioru końcowego przedmiotu zamówienia, b) zapewnione minimum 36-miesięczne wsparcie techniczne - od dnia podpisania bez zastrzeżeń przez obydwie strony protokołu odbioru końcowego przedmiotu zamówienia.
Wymagania dotyczące wsparcia i gwarancji	Tryb świadczenia gwarancji: a) dostępność serwisu w okresie gwarancji – min 8 h na dobę, 5 dni w tygodniu przez cały rok, b) zgłoszenia będą przyjmowane przez wykonawcę usługi gwarancyjnej telefonicznie lub na adres mailowy lub przez dedykowany portal zgłoszeniowy, c) czas naprawy (przywrócenie stanu funkcjonowania systemu sprzed awarii) – następny dzień roboczy następujący po dniu zgłoszenia (Next Business Day - NBD),

	d) serwis w okresie gwarancji musi być świadczony w miejscu wdrożenia, czyli w siedzibie Zamawiającego oraz Lokalizacji Zapasowej. e) usunięcie uszkodzenia nienaprawialnego nastąpi w terminie wskazanym w lit. c, poprzez wymianę na sprzęt sprawny o co najmniej takich samych walorach funkcjonalnych, f) zapewniona naprawa lub wymiana urządzeń lub ich części na części nowe i oryginalne, zgodnie z metodyką z zaleceniami producenta sprzętu. g) wymienione urządzenia lub elementy muszą być objęte takim samym zakresem usług serwisowych jakim objęte były urządzenia i elementy, które zostały wymienione. h) wykonawca usługi gwarancyjnej ponosi wszystkie koszty napraw gwarancyjnych, włączając w to koszty części i transportu. i) w przypadku awarii nośników danych, pozostają one u Zamawiającego.
Wymagania dotyczące wsparcia i gwarancji	Wsparcie techniczne: a) musi być świadczone przez producenta lub jego autoryzowanego polskiego przedstawiciela, b) będzie świadczone telefonicznie lub drogą elektroniczną, c) obejmuje: dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. d) Wsparcie techniczne dla oprogramowania rozumiane jest jako gotowość przystąpienia do rozwiązywania problemów technicznych związanych z oprogramowaniem w trybie min 8 godzin na dobę, 5 dni roboczych w tygodniu.
Wymagania dotyczące testów	Testy: a) utworzenie i publikacja zasobu do repozytorium VEEAM, b) wykonanie pełnej kopii zapasowej oraz odtworzenie z kopii zapasowej, c) weryfikacja stopnia deduplikacji i kompresji, d) weryfikacja działania klastra deduplikatorów – wykonanie kopii oraz odtworzenie kopii z urządzenia zapasowego, e) symulacja awarii urządzenia i wykonanie kopii na urządzenie zapasowe, f) uruchomienie maszyn wirtualnych z deduplikatora w trybie instant recovery.

III. TERMIN REALIZACJI ZAMÓWIENIA

Termin realizacji zamówienia (dot. wszystkich części zamówienia): do 12 tygodni do dnia zawarcia umowy.

IV. DOSTAWA I MIEJSCE SERWISU

1. Dostawa w zakresie realizacji Umowy siedziba zamawiającego: 00-546 Warszawa ul. Skorupki 4 oraz serwerownia zapasowa na terenie Warszawy.
2. Serwis świadczony będzie w dwóch lokalizacjach na terenie Warszawy.