OPZ – Specyfikacja przedmiotu zamówienia

1. Specyfikacja przedmiotu zamówienia

Wyszczególnienie	Ilość
1. System bezpieczeństwa NGFW **1.1. Wymagania ogólne** • System bezpieczeństwa musi działać w architekturze rozproszonej tzn. takiej w której komponenty odpowiadające za zarządzanie systemem oraz wymuszanie polityki bezpieczeństwa działają na dedykowanych platformach • W ramach komponentu zarządzania systemem Zamawiający wymaga minimum następujących funkcjonalności: ▪ centralne zarządzanie polityką bezpieczeństwa (w zakresie polityki dostępowej oraz ochrony przed zagrożeniami) na wszystkich zarządzanych urządzeniach UTM/grupy klastrowej ▪ funkcja serwera logów pozwalająca na centralne przechowywanie oraz indeksowanie logów pochodzących z zarządzanych urządzeń UTM/grup klastrowych ▪ funkcja korelacji oraz wykrywania incydentów bezpieczeństwa – wykrywanie oraz raportowanie incydentów bezpieczeństwa na bazie logów pochodzących z zarządzanych urządzeń ▪ moduł raportowania ▪ moduł sprawdzania zgodności konfiguracji z co najmniej takimi standardami jak GDPR, ISO 27001, PCI DSS • Zamawiający dopuszcza realizację opisanych funkcjonalności komponentu zarządzania przy zastosowaniu platformy sprzętowej lub wirtualnej. Każda platforma, niezależnie od typu, powinna zapewniać minimalnie 2TB powierzchni dyskowej. • Zamawiający dopuszcza realizację funkcjonalności komponentu zarządzania opisanych w punkcie 1.2 przez więcej niż jedną maszynę wirtualną lub fizyczną, jeżeli taka potrzeba wynika z architektury oferowanego rozwiązania. • Zamawiający wymaga, aby komponenty odpowiedzialne za wymuszanie polityki bezpieczeństwa (urządzenia UTM/grupy klastrowe) dostarczone zostały w formie dedykowanych urządzeń fizycznych (appliance). • Zamawiający wymaga, aby wszystkie komponenty programowe oraz urządzenia wchodzące w skład systemu bezpieczeństwa pochodziły od jednego producenta. • Zamawiający wymaga, aby wszystkie komponenty systemu bezpieczeństwa zainstalowane zostały lokalnie w ramach infrastruktury Zamawiającego. • Komunikacja pomiędzy wszystkimi komponentami systemu bezpieczeństwa musi być szyfrowana i uwierzytelniona z użyciem certyfikatów cyfrowych. • Zamawiający wymaga, aby dostarczone urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na terenie Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania. • Zamawiający wymaga, aby dostarczone urządzenia były nowe oraz pochodziły z bieżącej produkcji. Zamawiający nie dopuszcza dostawy urządzeń, które mogły być używane w innych projektach i zostały poddane procesowi odnowienia. • Zamawiający zobowiązuje Wykonawcę do potwierdzenia, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich, w szczególności Wykonawca nie może zaoferować sprzętu i oprogramowania, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego. • Zamawiający wymaga, aby dostarczony system zabezpieczeń był produktem o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) przez co najmniej 36 miesięcy z rzędu. • Zamawiający wymaga, aby wszystkie określone w niniejszym dokumencie funkcje systemu były realizowane w aktualnie dostępnych komercyjnie urządzeniach oraz wersjach oprogramowania. • Zamawiający wymaga aby elementy systemu zostały dostarczone ze stabilną wersją oprogramowania. Oznacza to, iż rozwiązanie (urządzenia + oprogramowanie) musi być dostępne	**1 szt.**

na rynku nie krócej niż 3 miesiące od daty ogłoszenia postępowania przetargowego. System bezpieczeństwa musi zostać dostarczony z zestawem licencji pozwalających na realizację następujących funkcjonalności przez okres 5 lat:

- funkcja firewall
- wykrywanie i przeciwdziałanie próbom włamań (IPS)
- tworzenie reguł polityki bezpieczeństwa z wykorzystaniem definicji konkretnych aplikacji (kontrola aplikacji)
- tworzenie reguł polityki bezpieczeństwa z wykorzystaniem kategorii URL
- ochrona antywirusowa
- wykrywanie i blokowanie komunikacji z sieciami botnet
- tworzenie reguł polityki w oparciu o tożsamość użytkownika (możliwość korelacji tożsamości użytkowników z wykorzystywanym adresem IP)
- wykonywanie inspekcji ruchu szyfrowanego
- możliwość realizacji połączeń IPSec VPN
- ochrona przed atakami typu 0-day

1.2. Moduł zarządzania – wymagania funkcjonalne

- Moduł zarządzania musi mieć możliwość zarządzania minimum dwoma punktami wymuszania polityki bezpieczeństwa (grupy klastrowe)
- Moduł zarządzania musi umożliwiać jednoczesną pracę wielu administratorów - w tym także jednoczesną pracę w ramach pojedynczej polityki bezpieczeństwa.
- Moduł zarządzania musi zapewniać możliwość tworzenia wielu różnych polityk bezpieczeństwa oraz umożliwiać ich przypisanie do poszczególnych urządzeń UTM zarządzanych z poziomu serwera.
- Moduł zarządzania musi umożliwiać tworzenie modułowej polityki bezpieczeństwa. System musi umożliwiać współdzielenie modułów (zestawów reguł polityki bezpieczeństwa) pomiędzy różnymi politykami bezpieczeństwa.
- Moduł zarządzania musi posiadać mechanizmy automatycznej weryfikacji spójności i niesprzeczności implementowanej polityki bezpieczeństwa przed zainstalowaniem jej na urządzeniach UTM.
- Moduł zarządzania musi posiadać mechanizmy pozwalające na weryfikację poprawności działania nowej wersji polityki bezpieczeństwa po jej uruchomieniu na urządzeniu UTM oraz możliwość automatycznego powrotu do poprzedniej wersji w przypadku stwierdzenia nieprawidłowości na bazie zestawu testów utworzonych przez administratora- np. brak dostępu do wybranych usług powstały w wyniku błędu administratora
- Moduł zarządzania musi posiadać wbudowane mechanizmy wersjonowania polityki bezpieczeństwa. Nowa wersja polityki bezpieczeństwa powinna być tworzona każdorazowo w momencie opublikowania zmian przez administratora systemu. System wersjonowania musi zapewniać administratorom możliwość wglądu w wybraną wersję polityki bezpieczeństwa, możliwość porównywania różnych wersji polityki pod kątem różnic między nimi, a także opcję cofnięcia konfiguracji do wybranej wersji.
- Moduł zarządzania musi zapewniać możliwość uwierzytelnianie administratorów za pomocą haseł statycznych, haseł dynamicznych, certyfikatów cyfrowych oraz protokołu SAML.
- Moduł zarządzania musi zapewniać możliwość definiowania szczegółowych zestawów uprawnień dla poszczególnych administratorów (np. tylko do odczytu logów, tylko do zarządzania użytkowników)
- Moduł zarządzania musi posiadać mechanizmy zapewniające rozliczalność zmian konfiguracyjnych wykonanych przez poszczególnych administratorów w formie generowania i przechowywania logów audytowych. Logi muszą zawierając minimum informacje o tożsamości administratora oraz czasie i zakresie wykonywanych zmian
- Moduł zarządzania musi posiadać mechanizm sprawdzania i zatwierdzania zmian dokonanych przez administratora (umownie administratora poziomu 1) przez innego administratora (umownie administratora poziomu 2) przed instalacja polityki. Mechanizm ten powinien mieć możliwość notyfikacji administratora poziomu 2, że zmiany w polityce/konfiguracji czekają na zatwierdzenie. Funkcjonalność ta powinna być dostępna z systemu zarządzania bez dodatkowej licencji.
- Moduł zarządzania musi posiadać mechanizmy centralnego zarządzania licencjami dla wszystkich

komponentów wchodzących w skład systemu bezpieczeństwa (serwery logów, serwery korelacji zdarzeń i raportowania, zapory sieciowe) • Moduł zarządzania musi dostarczać mechanizmy pozwalające na monitorowanie i prezentowanie za pomocą graficznej konsoli parametrów sprzętowych zarządzanych urządzeń UTM/grup klastrowych takich jak: średnie obciążenie procesora, zajętość pamięci operacyjnej, zajętość przestrzeni dyskowej, wersję oprogramowania zapory sieciowej, nazwę i wersję zainstalowanej polityki bezpieczeństwa, listę uruchomionych modułów bezpieczeństwa • Moduł zarządzania musi dostarczać mechanizmy pozwalające na graficzne prezentowanie statystyk ruchu sieciowego, przetwarzanego przez zarządzane zapory sieciowe. Dostępne statystyki obejmują minimum informacje o najczęściej wykorzystywanych usługach sieciowych, najczęstszych źródłach transmisji, najczęstszych adresach docelowych, aktywnych i nieaktywnych tunelach IPSec VPN (site-to-site oraz remote access) • Moduł zarządzania musi posiadać dedykowane API umożliwiające automatyzację czynności administracyjnych. Mechanizm API powinien umożliwiać minimum wykonanie następujących czynności: ▪ tworzenie, edycja oraz usuwanie obiektów sieciowych i usług ▪ tworzenie, modyfikowanie oraz usuwanie reguł polityki bezpieczeństwa oraz reguł NAT ▪ instalacja polityki bezpieczeństwa ▪ zarządzania kontami administratorów systemu • Moduł zarządzania musi realizować funkcję serwera logów w ramach której musi umożliwiać agregację i indeksowanie logów ze wszystkich zarządzanych zapór sieciowych. W ramach funkcji serwera logów muszą istnieć wbudowane mechanizmy ochrony przestrzeni dyskowej przed przepełnieniem Mechanizm powinien umożliwiać wykonywanie różnych akcji systemu w zależności od poziomu zajętości dysku. Możliwe akcje to minimum wysyłanie alertów do administratorów oraz automatyczne usuwanie najstarszych plików logów • Moduł zarządzania musi posiadać mechanizmy pozwalające na implementację rozwiązania wysokiej dostępności, w ramach której możliwe jest dodanie zapasowego serwera zarządzania oraz uruchomienie automatycznej synchronizacji konfiguracji polityk bezpieczeństwa. Dostarczenie zapasowego serwera zarządzania nie jest wymagane w ramach postępowania. • Moduł zarządzania musi mieć możliwość wykrywania incydentów bezpieczeństwa na bazie logów pochodzących z zarządzanych urządzeń UTM/grup klastrowych • Moduł zarządzania musi pozwalać na wyszukiwanie wymaganych informacji (logów, incydentów bezpieczeństwa) zapisanych w wewnętrznej bazie danych bez konieczności definiowania wartości dla poszczególnych atrybutów (tzw.freetext search). • Moduł zarządzania musi pozwalać na grupowanie wyników wyszukiwania logów/incydentów bezpieczeństwa według określonych atrybutów (minimum typ incydentu, zasoby, nazwa użytkownika). • Moduł zarządzania musi umożliwiać wykonywanie analizy incydentów bezpieczeństwa od poziomu ogólnego do szczegółowych logów odpowiedzialnych za wygenerowanie zdarzenia (tzw. drill-down). • Moduł zarządzania musi umożliwiać administratorom tworzenie własnych raportów oraz ekranów (formatka prezentująca określony podzbiór danych w formie zdefiniowanej przez administratora), a także modyfikowanie raportów i widoków dostarczonych razem z systemem. • Moduł zarządzania musi umożliwiać graficzną prezentację danych (logi/incydenty bezpieczeństwa) za pomocą interaktywnych pasków, wykresów kołowych i czasowych. • Moduł zarządzania musi umożliwiać filtrowanie logów/incydentów bazując na parametrach takich jak: aplikacja, źródłowy i docelowy IP, usługa, typ zdarzenia, istotność ataku, kraj pochodzenia itd. • Moduł zarządzania musi posiadać możliwość budowania własnych raportów przez administratorów w trybie na żądanie oraz zgodnie z zadanym harmonogramem • Moduł zarządzania musi umożliwiać współdzielenie własnych/customowych raportów pomiędzy administratorami • Moduł zarządzania musi posiadać możliwość generowania raportów w formacie PDF oraz Microsoft Excel. Musi istnieć możliwość przesyłania wygenerowanych raportów poprzez pocztę elektroniczną do wskazanych odbiorców. • Moduł zarządzania musi posiadać możliwość tworzenia niestandardowych reguł korelacji zdarzeń bezpieczeństwa.	

- Moduł zarządzania musi posiadać możliwość konfigurowania automatycznych reakcji na wykryte incydenty bezpieczeństwa - minimum w postaci wysłania wiadomość e-mail, wygenerowanie SNMP trap lub uruchomienie skryptu

1.3. Zapora sieciowa – wymagania ogólne

- System zapory sieciowej musi zapewniać modułową architekturę zapewniającą skalowalność oraz wydajność składającą się z oddzielnego tzw. 'switching fabric" i grupy wewnętrznych modułów zapory ogniowej dla kontroli ruchu.
- Interfejs "switching fabric" musi umożliwiać połączenie z zewnętrzną infrastrukturą sieciową oraz przeprowadzać równomierny rozkład obciążenia pomiędzy wewnętrznymi modułami zapory sieciowej.
- Rozwiązanie musi zapewniać redundancję na poziomie „switching fabric".
- Rozwiązanie musi zapewniać redundancję na poziomie modułów zapory sieciowej.
- Rozwiązanie może być rozwiązaniem typu chassis
- Rozwiązanie musi zapewniać skalowalność modułów zapory sieciowej do co najmniej 9 oddzielnych modułów.
- Rozwiązanie musi mieć możliwość zwiększania wydajności, poprzez podłączenie dodatkowych modułów zapory ogniowej do "switching fabric" bez potrzeby rekonfiguracji lub zmian w infrastrukturze L3.
- Rozwiązanie musi zapewniać konfigurację active-active pomiędzy modułami zapory ogniowej w ramach jednej fizycznej lokalizacji
- Rozwiązanie musi mieć możliwość tworzenia wielu grup clustrowych w ramach rozwiązania, złożonych z modułów zapór ogniowych.
- Rozwiązanie musi zapewniać synchronizację stanu sesji między modułami zapory ogniowej w grupie klastrowej
- Przełączanie awaryjne między modułami zapór ogniowych w ramach grupy klastrowej musi odbywać się z zachowaniem stanu sesji
- Dodawanie\usuwanie modułu zapory do\z grupy klastrowej musi odbywać się bez konieczności zmiany ustawień zabezpieczeń i polityki
- Musi istnieć możliwość automatycznego klonowania konfiguracji do nowo dodanych modułów zapory ogniowej
- Musi istnieć obsługa tzw. skalowania w górę/skalowania w dół w odniesieniu do modułów zapór ogniowych
- Rozwiązanie musi zapewniać zbliżony do liniowego, wzrost wydajności podczas dodawania kolejnego modułu zapory ogniowej do grupy klastrowej (nie więcej niż 10% wpływu na ogólną wydajność)
- Rozwiązanie musi zapewniać akceleracją zdefiniowanego ruchu sieciowego na poziomie „switching fabric".
- Moduł „switching fabric" musi zapewniać równomierny rozkład ruchu pomiędzy poszczególnymi modułami zapory ogniowej. Rozkład ruchu musi odbywać się na podstawie monitoringu zasobów poszczególnych modułów zapory ogniowej (użycie procesorów, zużycie pamięci, itp.). Niedopuszczalne jest, aby rozkład ruchu następował tylko na podstawie sprawdzenia, czy dany moduł zapory ogniowej jest dostępny (z pomocą tzw. Heartbeats).
- Rozwiązanie musi umożliwiać współdziałanie różnych modeli modułów zapory sieciowej w ramach jednej grupy klastrowej.
- Każda grupa klastrowa musi występować jako jeden obiekt z punktu widzenia modułu zarządzania.
- Interfejsy zapory sieciowej muszą działać w trybie routera (tzn. w warstwie 3 modelu OSI),w trybie transparentnym oraz w trybie pasywnego nasłuchu (monitoring).
- Tryb pracy interfejsu zapory sieciowej musi być ustalany w konfiguracji interfejsu sieciowego, a zapora musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
- System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q z obsługą do 1024 znaczników VLAN w trybie Gateway oraz 4096 znaczników w trybie wirtualnych systemów.

- Zapora sieciowa musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP, OSPF (v2 oraz v3) oraz IS-IS.
- Zapora sieciowa musi posiadać możliwość pracy w trybie serwera DHCP oraz DHCP relay
- Zapora sieciowa musi być zgodna z poniższymi standardami (RFC) dotyczącymi IPv6:
  - RFC 1981 Path Maximum Transmission Unit Discovery for IPv6
  - RFC 2460 IPv6 Basic specification
  - RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
  - RFC 4007 IPv6 Scoped Address Architecture
  - RFC 4193 Unique Local IPv6 Unicast Addresses
  - RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers – wsparcie dla tuneli 6w4
  - RFC 4443 ICMPv6
  - RFC 4862 IPv6 Stateless Address Auto-configuration

1.4. Firewall

- Moduł Firewall musi realizować inspekcję stanową opartą na granularnej analizie komunikacji oraz stanu aplikacji w celu poprawnego śledzenia i kontroli przepływu ruchu
- Polityka zabezpieczeń modułu 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 zarządzania pasmem.
- Moduł firewall musi posiadać możliwość zaraportowania ilości „trafień" wybranej reguły polityki bezpieczeństwa do serwera zarządzania. Musi istnieć możliwość prezentowania liczby trafień dla reguł w wybranych okresach czasu, minimum w okresie 1 dnia, 7 dniu oraz miesiąca.
- Moduł firewall musi pozwalać na konfiguracje reguł polityki bezpieczeństwa z uwzględnieniem okresu czasu w jakim dana reguła będzie aktywna (egzekwowana). Definicja okresu czasu, w ramach którego dana reguła jest aktywna powinna uwzględniać następujące parametry: data i/lub godzina startu, data i/lub godziny zakończenia oraz rekurencyjność.
- Moduł firewall musi mieć możliwość automatycznego pobierania, z zewnętrznych serwerów, list z adresami IP i/lub Domenami. Pobranie powinno następować automatycznie i tylko wtedy, gdy treść zewnętrznej listy zostanie zaktualizowana. Funkcjonalność ta musi mieć również możliwość uwierzytelnienia połączenia do zewnętrznego serwera oraz możliwość użycia serwera proxy w celu pobrania listy.
- Moduł firewall musi posiadać możliwość konfiguracji reguł polityki bezpieczeństwa w oparciu o tożsamość użytkownika (identity firewall)
- Moduł firewall musi domyślnie działać zgodnie z zasadą blokowania całego ruchu sieciowego, poza tym który jest zdefiniowany w regułach polityk bezpieczeństwa i wskazany jako dozwolony
- Rozwiązanie musi pozwalać na kontrolę przynajmniej 150 predefiniowanych usług/protokołów
- Moduł 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.

1.5. Moduł przeciwdziałania próbom włamań (IPS)

- Moduł IPS musi posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system).
- Moduł IPS musi posiadać możliwość pracy zarówno w trybie pasywnym (Detect) jak i aktywnym (z możliwością blokowania ruchu)
- Moduł IPS musi dokonywać inspekcji całych sesji/połączeń. Nie dopuszcza się rozwiązań określających bezpieczeństwo sesji poprzez szczątkową analizę ruchu podczas ustanawiania sesji.
- Moduł IPS musi zapewniać co najmniej poniższe sposoby wykrywania zagrożeń:
  - sygnatury ataków opartych na exploitach
  - reguły oparte na zagrożeniach

▪ mechanizm wykrywania anomalii w protokołach • Moduł IPS musi mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu • Moduł IPS musi posiadać wiele możliwości reakcji na zdarzenia takie jak: tylko monitorowanie, blokowanie ruchu zawierającego zagrożenia oraz mieć możliwość zapisywania pakietów generujących zagrożenie • Moduł IPS musi posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji • Moduł IPS musi zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera aktualizacji w sposób uniemożliwiający ich modyfikację podczas przesyłania pomiędzy serwerem aktualizacji oraz serwerem zarządzania/zaporą sieciową. • Moduł IPS musi zapewniać mechanizm zarządzania wersjami bazy sygnatur oraz umożliwiać powrót do wybranej wersji. • Moduł IPS musi posiadać mechanizm automatycznej aktywacji sygnatur minimum w oparciu o następujący zestaw parametrów: poziom zagrożenia, wpływ na wydajność urządzenia, dokładność identyfikacji zagrożenia • Moduł IPS musi zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednoczenie. • Moduł IPS musi zapewniać możliwość obsługi reguł Snort • Moduł IPS musi zapewniać możliwość detekcji i blokowania ataków i zagrożeń opartych na protokole IPv6 • Moduł IPS musi pozwalać na objęcie ochroną protokołów SCADA bez potrzeby zakupu dodatkowych licencji • Moduł IPS musi pozwalać posiadać możliwość aktywowania ochrony dla wybranych zasobów definiowanych minimum w postaci adresów hostów, adresów sieci oraz zakresów adresów IP i przypisywanie do tych zasobów dedykowanych zestawów sygnatur. • Moduł IPS musi posiadać programowy mechanizm pozwalający na wyłączenie ochrony IPS w przypadku wysokiego obciążenia procesora lub pamięci operacyjnej zapory sieciowej. Wartości aktywujące mechanizm muszą być konfigurowalne przez administratora systemu. • Moduł IPS musi posiadać mechanizmy wykrywania i blokowania operacji tunelowania ruchu w ramach innych protokołów, np. DNS tunneling **1.6. Moduł kontroli aplikacji** • Baza modułu kontroli aplikacji powinna zawierać nie mniej niż 10.000 pozycji. Baza modułu powinna być dostępna do weryfikacji online. • Moduł kontroli aplikacji powinien pozwalać na granularną kontrolę przynajmniej 250.000 widgetów • Moduł kontroli aplikacji musi posiadać mechanizm ograniczenia użycia pasma dla poszczególnych aplikacji niezależnie dla każdego kierunku przepływu danych (download oraz upload) • Moduł kontroli aplikacji musi posiadać możliwość współpracy z modułem analizy treści w zakresie wykrywania i blokowania przesyłania określonych typów danych (np.nr kart kredytowych) oraz określonych typów plików (np. csv, pdf i inne) w ramach zidentyfikowanej aplikacji. W przypadku, kiedy opisany mechanizm wymaga dodatkowej licencji to powinna ona zostać dostarczona razem z systemem bezpieczeństwa. • Moduł kontroli aplikacji musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do aplikacji, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej aplikacji. • Moduł kontroli aplikacji musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowanie użytkowników do stron umieszczonych na zewnętrznych serwerach. • System musi umożliwiać administratorom rozszerzenie wbudowanej bazy aplikacji poprzez samodzielne tworzenie nowych sygnatur aplikacji. Jeżeli funkcjonalność ta wymaga dodatkowej licencji to stosowna licencja powinna być dostarczone razem z systemem.	

- Moduł kontroli aplikacji musi automatycznie identyfikować aplikacje bez względu na numery portów, protokoły tunelowania i szyfrowania.

1.7. Moduł identyfikacji użytkowników

- Moduł identyfikacji użytkowników musi umożliwiać uzyskiwanie informacji o tożsamości użytkowników z następujących źródeł:
  - integracja z usługą katalogową Microsoft Active Directory
  - integracja z usługą Cisco ISE
  - identyfikacja w portalu www (captive portal)
  - identyfikacja z wykorzystaniem dedykowanego agenta instalowanego na stacji użytkownika
  - integracja z serwerem RADIUS
  - integracja z serwerem syslog
  - połączenia remote access VPN
  - integracja z zewnętrznymi systemami IDP
- Moduł identyfikacji użytkowników we współpracy z usługą Microsoft Active Directory musi umożliwiać pozyskiwanie informacji o grupach, do których należy zidentyfikowany użytkownik.
- Moduł identyfikacji użytkowników musi umożliwiać skuteczną identyfikację użytkowników pracujących z wykorzystaniem serwerów teminali (np. Citrix) współdzielących pojedynczy adres IP
- Moduł identyfikacji użytkowników musi umożliwiać identyfikację użytkowników znajdujących się za urządzeniem typu http proxy poprzez wykorzystanie informacji zawartej w nagłówku X-Forwarded-For. Moduł po pozyskaniu informacji z nagłówka XFF musi go usunąć przed przekazaniem komunikacji do serwera docelowego.
- Moduł identyfikacji użytkowników przy współpracy z usługą katalogową Microsoft Active Directory powinien wykorzystywać minimalne wymagane uprawnienia po stronie usługi Active Directory. Niedopuszczalna jest integracja z domeną MS Active Directory w ramach której wymagane jest zastosowanie uprawnień administratora domeny.
- Moduł identyfikacji użytkowników musi posiadać możliwość współdzielenia informacji o zidentyfikowanych użytkownikach pomiędzy zaporami sieciowymi pochodzącymi od tego samego producenta i zarządzanymi z tego samego lub odrębnego serwera zarządzania
- System bezpieczeństwa musi umożliwiać wykorzystanie informacji uzyskanych przez moduł identyfikacji użytkowników w ramach definicji reguł polityki bezpieczeństwa w celu zapewniania użytkownikom lub grupom użytkowników spójnych reguł dostępu do zasobów niezależnie od ich lokalizacji.

1.8. Inspekcja ruchu szyfrowanego

- System bezpieczeństwa musi zapewniać mechanizmy inspekcji komunikacji szyfrowanej HTTPS oraz inspekcji komunikacji realizowanej w oparciu o protokół SSH.
- System bezpieczeństwa w ramach inspekcji ruchu HTTPS musi wspierać protokoły TLS 1.2 oraz TLS 1.3
- System bezpieczeństwa musi pozwalać na inspekcję ruchu HTTPS zarówno dla ruchu wychodzącego z sieci organizacji (np. komunikacja użytkowników z usługami w sieci Internet) jaki i ruchu przychodzącego kierowanego do usług udostępnianych przez organizację. Inspekcja powinna obejmować analizę ruchu pod kątem zgodności z regułami polityki dostępowej (np. kontrola aplikacji oraz kategorii URL) oraz weryfikować ruch pod kątem ewentualnych zagrożeń (np. moduł IPS, moduł antywirusowy).
- System musi umożliwiać administratorom zdefiniowanie reguł określających jaka część ruchu HTTPS ma zostać poddana inspekcji, a jaka ma zostać z niej wykluczona. W ramach definiowania reguł administrator musi posiadać możliwość określenia jakie mechanizmy inspekcyjne (moduły) mają zostać wykorzystane podczas analizy ruchu (np. ochrona antywirusowa).
- System musi umożliwiać utworzenie więcej niż jednego zbioru reguł określających zakres ruchu HTTPS podlegający inspekcji. System musi umożliwiać przypisywanie zbiorów reguł do określonych polityk bezpieczeństwa, a także współdzielenie określonych zbiorów reguł przez więcej niż jedną politykę bezpieczeństwa.
- W ramach mechanizmu inspekcji wychodzącego ruchu HTTPS system musi umożliwiać weryfikację stanu certyfikatu cyfrowego serwera docelowego. System musi umożliwiać blokowanie ruchu do określonego serwera docelowego w przypadku kiedy jego certyfikat został unieważniony, wygasł lub nie został podpisany przez zaufany urząd certyfikacji.

• System bezpieczeństwa musi umożliwiać tworzenie listy niezaufanych certyfikatów cyfrowych i w efekcie pozwalać na blokowanie ruchu kierowanego do serwerów, które takie certyfikaty wykorzystują. • System bezpieczeństwa musi umożliwiać wysyłanie kopii odszyfrowanego ruchu HTTPS na wskazany interfejs urządzenia w celu zasilania zewnętrznych systemów bezpieczeństwa. • System bezpieczeństwa musi zapewniać mechanizmy pozwalające na inspekcję szyfrowanej komunikacji SSH. Niedopuszczalne jest aby system do deszyfracji SSH używał jednego globalnego klucza deszyfrującego • W ramach inspekcji ruchu SSH system musi zapewniać możliwość analizy ruchu przy pomocy modułu wykrywania włamań (IPS) oraz umożliwiać analizę przesyłanych plików minimum przy pomocy modułu antywirusowego. **1.9. Moduł do realizacji połączeń zdalnych** • Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w trybie punkt-punkt (site-to-site) oraz zapewniać możliwość dostępu do zasobów dla użytkowników zdalnych (remote access) • Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w oparciu o protokół IKEv1 oraz IKEv2 • Moduł IPSec VPN musi umożliwiać nawiązywanie połączeń w następujących topologiach: full mesh, star, hub-and-spoke • Moduł IPSec VPN musi umożliwiać kreowanie tuneli w oparciu o klucz współdzielony (preshared key) oraz certyfikaty cyfrowe. W przypadku certyfikatów cyfrowych musi istnieć możliwość wykorzystania certyfikatów wystawianych przez wewnętrzny urząd certyfikacji wbudowany w produkt lub przez zewnętrzne urzędy certyfikacji • Moduł IPSec VPN musi umożliwiać uruchomienie mechanizmu split-tunneling dla połączeń od użytkowników zdalnych. • Moduł IPSec VPN musi zapewniać możliwość zestawienia minimum 50 jednoczesnych połączeń od użytkowników zdalnych. • Niedopuszczalne jest aby moduł IPSec VPN ograniczał licencyjnie liczbę tuneli punkt-punkt jakie mogą zostać nawiązane z poziomu zapory sieciowej. **1.10. Moduł filtrowania kategorii URL** • Moduł filtrowania kategorii URL musi posiadać możliwość tworzenia reguł polityki zawierających jednocześnie wiele kategorii URL. • Moduł filtrowania kategorii URL musi dostarczać wbudowane kategorie URL opisujące niebezpieczne witryny kategoryzowane w oparciu o poziom zagrożenia (np. CriticalRisk lub High Risk), a także w oparciu o rodzaj zagrożenia (np. witryny wyłudzające dane lub witryny będące centrami C&C) • Moduł filtrowania kategorii URL musi umożliwiać tworzenie własnych obiektów opisujących witryny URL oraz ich kategoryzowanie. • Moduł filtrowania kategorii URL musi umożliwiać tworzenie obiektów należących do więcej niż jednej kategorii URL. • Moduł filtrowania kategorii URL musi umożliwiać lokalne nadpisywanie domyślnej kategorii URL dla wybranych witryn. • Moduł filtrowania kategorii URL musi posiadać możliwość interakcji z użytkownikami. Interakcja musi być możliwa minimum w zakresie informowania o zablokowaniu dostępu do określonej witryny, informowania o monitorowaniu komunikacji oraz pobierania informacji od użytkownika w celu uargumentowania konieczności dostępu do określonej witryny. • Moduł filtrowania kategorii URL musi umożliwiać modyfikowanie wbudowanych stron z powiadomieniami prezentowanymi użytkownikom oraz musi umożliwiać przekierowania użytkowników do stron umieszczonych na zewnętrznych serwerach. **1.11. Moduł ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet** • System zapobiegania komunikacji z sieciami botnet musi umożliwiać wykrycie oraz zablokowanie podejrzanego zachowania w chronionych segmentach sieci • System zapobiegania komunikacji z sieciami botnet w celu identyfikacji podejrzanych zachowań musi wykorzystywać mechanizmy zabezpieczeń oparte o	

reputację adresów IP, URL oraz DNS w połączeniu z wykrywaniem wzorców ruchu specyficznych dla połączeń kierowanych do serwerów C&C.

- System zapobiegania komunikacji z sieciami botnet musi posiadać możliwość identyfikacji urządzeń wewnętrznych będących źródłem podejrzanych zapytań DNS w przypadku kiedy wykorzystują one wewnętrzny serwer DNS pośredniczący w generowaniu zapytań. Mechanizm musi umożliwiać modyfikację/fałszowanie odpowiedzi DNS i przekierowywanie urządzeń do wcześniej ustalonego adresu IP (tzw. DNS malware trap lub DNS Sinkhole).
- Moduł ochrony antywirusowej musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, SMTP/TLS, FTP, SMB/CIFS (w tym SMBv3), SFTP/SCP, IMAP, POP3
- Moduł ochrony antywirusowej musi umożliwiać skanowanie adresów URL oraz załączników znajdujących się w wiadomościach poczty elektronicznej.
- Moduł ochrony antywirusowej musi umożliwiać skanowanie plików skompresowanych. Administrator musi mieć możliwość zdefiniowania maksymalnego czasu skanowania pojedynczego archiwum oraz zdefiniowania akcji (przekaż lub zablokuj) która zostanie podjęta w momencie przekroczenia zdefiniowanego limitu.
- Moduł ochrony antywirusowej musi posiadać możliwość blokowania dostępu do określonych witryn internetowych w oparciu o informację o ich reputacji.
- Moduły ochrony antywirusowej oraz zapobiegania komunikacji z sieciami botnet muszą posiadać możliwość interakcji z użytkownikami w zakresie informowania o zablokowaniu dostępu do niebezpiecznych zasobów.
- System bezpieczeństwa musi umożliwiać rozszerzenie bazy informacji o zagrożeniach poprzez dodawanie zewnętrznych definicji IoC (Indicator of Compromise) w formacie pliku CSV lub STIX XML (STIX 1.0).

1.12. Moduł ochrony przed atakami 0-day

- Moduł musi zapewniać ochronę minimum dla następujących protokołów: HTTP/HTTPS, SMTP/TLS, IMAP, FTP, CIFS, SMBv3, SMB multi-channel oraz SFTP/SCP.
- Moduł musi zapewniać możliwość analizowania przynajmniej następujących typów plików:
  - .7z - 7z Archive
  - .bz2 - bzip2 compressed archive
  - .CAB - Compressed archive
  - .csv - Comma-separated values file
  - .doc Microsoft Word 97-2003 Document
  - .docx Microsoft Word Document
  - .dot / .dotx - Microsoft Word Template
  - .dotm / .docm - Microsoft Word macro-enabled template
  - .gz - Gz Archive
  - .hwp
  - .iqy - Excel Web Query file
  - .iso
  - .jar - Java Browser Applet
  - .msg - Mail message file format used by Microsoft Outlook and Exchange
  - .pdf - Adobe Acrobat document
  - .ppt - Microsoft PowerPoint 97-2003 Presentation
  - .pptx - Microsoft PowerPoint Presentation
  - .pps - Legacy Microsoft PowerPoint slideshow
  - .pptm - Microsoft PowerPoint macro-enabled presentation
  - .potx - Microsoft PowerPoint template
  - .potm - Microsoft PowerPoint macro-enabled template
  - .ppam - Microsoft PowerPoint add-in
  - .ppsx - Microsoft PowerPoint slideshow
  - .ppsm - Microsoft PowerPoint macro-enabled slideshow
  - .rar - Rar Archive
  - .rtf - Rich Text Format file
  - .sldx - Microsoft PowerPoint slide

▪ .sldm - Microsoft PowerPoint macro-enabled slide ▪ .swf - Flash ▪ .tar - Tar Archive ▪ .tgz - Tgz Archive ▪ .xlt - Legacy Microsoft Excel 97-2003 templates ▪ .xls - Microsoft Excel 97-2003 Worksheet ▪ .xlsx - Microsoft Excel Worksheet ▪ .xlm - Microsoft Excel macro ▪ .xltx - Microsoft Excel template ▪ .xlsm - Microsoft Excel macro-enabled workbook ▪ .xltm - Microsoft Excel macro-enabled template ▪ .xlsb - Microsoft Excel binary worksheet ▪ .xla - Microsoft Excel add-on or macro ▪ .xlam - Microsoft Excel add-on ▪ .xll - Microsoft Excel XLL (DLL based) add-on ▪ .xlw - Microsoft Excel workspace ▪ .zip - Zip Archive" • Moduł musi umożliwiać otwarcie dostarczonego za pośrednictwem wspieranych protokołów pliku w wirtualnym systemie operacyjnym, analizę skutków otwarcia pliku w tym systemie a następnie podjęcie akcji (zablokuj/przekaż do odbiorcy) w zależności od uzyskanych wyników analizy. Szczegółowy wynik analizy powinien zostać udokumentowany w formie raportu i przesłany na wskazany serwer logów. • Niedopuszczalne jest przekazanie pliku do odbiorcy przed uzyskaniem wyniku z procesu analizy w środowisku wirtualnym potwierdzającego że analizowany plik jest bezpieczny. Wyjątkiem jest dostarczenie do użytkownika bezpiecznej wersji pliku, tzn. wersji pozbawionej całej treści aktywnej. Jako treść aktywna rozumiane są między innymi makra pakietu MS Office, odnośniki do zewnętrznych zasobów, obrazy, kwerendy do baz danych, skrypty JavaScript, filmy i inne. • Moduł musi umożliwiać wykonywanie analizy zachowania plików w środowiskach wirtualnych opartych o różne wersje systemu operacyjnego Microsoft Windows oraz różne pakiety oprogramowania Microsoft Office. Licencja dostarczona wraz z modułem musi zawierać prawa do użytkowania zewnętrznego oprogramowania zawartego w obrazach systemów do celów analizy plików w środowiskach wirtualnych. • Moduł w ramach analizy plików w środowiskach wirtualnych powinien monitorować minimum następujące aktywności: ▪ zapytania API ▪ zmiany w systemie plików (np. tworzenie i usuwanie plików, modyfikowanie uprawnień do plików) ▪ zmiany w rejestrze systemowym ▪ próby nawiązania połączeń sieciowych ▪ próby eskalacji uprawnień ▪ próby ominięcia systemu UAC • Moduł musi umożliwiać wykrywanie zagrożeń na etapie przełamywania zabezpieczeń systemu (exploit). • Moduł musi umożliwiać analizowanie plików wskazywanych poprzez odnośniki znajdujące się w analizowanych wiadomościach pocztowych. • Moduł musi posiadać mechanizm pozwlalający na przekazywanie informacji o wykryciu niezbepiecznego pliku do chmury producenta w celu wygenerowania sygnatury. • Moduł musi umożliwiać wykonywanie analizy plików w środowiskach wirtualnych uruchamianych w chmurze producenta lub na lokalnym, dedykowanym urządzeniu dostarczonym przez producenta. W przypadku analizy plików w środowisku chmurowym musi istnieć możliwosc określenia obszaru geograficznego w jakim zlokalizowane są centra danych producenta do ktorych przesyłane będą pliki. Minimum wymagana jest możliwość ograniczenia obszaru geograficznego do terenu Unii Europejskiej (GDPR). • Zamawiający nie wymaga dostarczenia dedykowanego urządzenia do wykonywania analizy plików lokalnie. • Zamawiający wymaga dostarczenia wraz z modułem licencji pozwalającej na wykonywania analizy	

plików w chmurze producenta.

- Moduł musi posiadać mechanizmy pozwalające na dynamiczną analizę aplikacji www w celu ciągłej weryfikacji ataków typu web phishing. Analiza powinna być wykonywana w sposób ciągły w momencie próby dostępu do aplikacji www przez uzytkownika.
- Moduł musi posiadać mechanizmy chroniące przed atakami typu DNS Data Exfiltration:
  - Domain Generation Algorithm
  - Domain Name System Tunneling

1.13. Wymagania sprzętowe

- Urządzenia pełniące rolę zapory sieciowej muszą być przystosowane do zamontowania w szafie RACK 19" lub posiadać dostarczaną przez producenta półkę umożliwiająca taki montaż. Dodatkowo muszą zostać dostarczone wraz z niezbędnym do montażu sprzętem i okablowaniem oraz licencją na zewnętrzny centralny system zarządzania.
- Urządzenia pełniące rolę modułów zapory sieciowej muszą być wyposażone w pamięć DRAM nie mniejszą niż 32GB.
- Urządzenia pełniące rolę modułów zapory sieciowej muszą być wyposażone w dysk SSD o pojemności nie mniejszej niż 480GB każdy.
- Proponowane rozwiązanie NGFW musi posiadać sumaryczną przepływność w ruchu full-duplex nie mniej niż 32 Gbit/s dla kontroli firewall z włączoną funkcją IPS oraz kontrolą aplikacji oraz nie mniej niż 8,5 Gbit/s dla kontroli zawartości (moduły firewall, kontrola aplikacji, kategoryzacja URL, moduł antywirusowy, IPS, ochrona Zero-Day) i obsługiwać sumarycznie nie mniej niż 7 200 000 jednoczesnych połączeń z możliwością obsługi przyrostu 190.000 połączeń na sekundę.
- Podane parametry przepływności dotyczą wydajności zapory sieciowej w warunkach typu Enterprise. Zamawiający nie dopuszcza urządzeń, gdzie w/w wartość jest zdefiniowana jako „lab" „ideal" itp. zbliżone w nazwie definiujące warunki idealne lub laboratoryjne.
- Każde z urządzeń pełniących rolę „switching_fabric" musi obsługiwać interfejsy 1 Gb/s, 10 Gb/s, 25 Gb/s, 40 Gb/s, 100 Gb/s oraz być wyposażone w co najmniej:
  - 8 portów 100 GbE
  - 48 portów 10/25 GbE
- Rozwiązanie musi obsługiwać połączenie za pomocą kabli DAC
- Każde z urządzeń pełniących rolę zapory sieciowej musi być wyposażone w redundantne zasilacze zasilanie prądem przemiennym 230V (niedopuszczalne są rozwiązania zewnętrzne)
- Każde urządzenie musi być wyposażone w moduł do zarządzania out-of-band (tzw. LOM/iLO/iDrac), który pozwala na obsługę zdalną urządzenia co najmniej w poniższy sposób:
  - Instalacja systemu,
  - Restart urządzenia,
  - Wyłączenie urządzenia,
  - Włączenie urządzenia,
  - Dostęp do portu konsoli urządzenia.

1.14. Usługi

- Oferowane rozwiązanie musi być dostarczone z minimum pięcioletnim okresem gwarancji i supportu do dla wszystkich komponentów wchodzących w skład rozwiązania
- Przygotowanie projektu przedwykonawczego składającego się z m.in. z schematu logicznego L3**,** schemat fizycznego podłączenia urządzeń
- przygotowanie planu przełączenia optymalnego z punkt widzenia działania usług Geopoz (w tym godziny wieczorne bądź weekend)
- przygotowanie testów wysokiej dostępności
- instalacja i konfiguracja urządzeń w siedzibie klienta
- przygotowanie dokumentacji powykonawczej
- przygotowanie procedur Disaster Recovery – backup, odtworzenie, przełączenie działania klastra
- 2-dniowe warsztaty z zakresu administracji i utrzymania oferowanego rozwiązania dla 3 osób
- Pakiet konsultacji min. 24 godziny rocznie do wykorzystanie online bądź w siedzibie klienta (usługa konsultacji świadczenia jest w dniach roboczych w godzinach od 8-17) przez okres supportu.

Zamawiający może wystosować po dostawie sprzętu zapytanie do producenta z prośbą o weryfikację numerów seryjnych dla potwierdzenia zgodności ze specyfikacją i zastrzega sobie prawo odstąpienia od umowy i nie podpisania odbioru sprzętu w przypadku rozbieżności w zapisach.
Oferent zobowiązuje się do dostarczenia i montażu wszystkich niezbędnych komponentów potrzebnych do uruchomienia rozwiązania. Oferent zobowiązany jest do przeprowadzenia wizji lokalnej istniejącego rozwiązania.
Dopuszcza się fakturowanie częściowe z tytułu:

- dostawy sprzętu i gwarancji/supportu,
- realizacji usług towarzyszących.

Informacje dodatkowe

- Wszystkie ewentualne nazwy własne i marki handlowe urządzeń i elementów zawarte w opisie przedmiotu zamówienia, zostały użyte w celu sprecyzowania oczekiwań jakościowych i technologicznych Zamawiającego.
- Zamieszczone w specyfikacji nazwy technologicznych lub producentów kluczowych komponentów użyto jedynie w celu przykładowym.
- Zamawiający informuje, że dopuszcza składanie ofert, w których poszczególne urządzenia bądź materiały wymienione w opisie przedmiotu zamówienia mogą być zastąpione urządzeniami bądź materiałami/elementami równoważnymi. Poprzez pojęcie materiałów/elementów i urządzeń równoważnych należy rozumieć materiały zapewniające uzyskanie parametrów technicznych nie gorszych od założonych w opisie przedmiotu zamówienia. Zastosowanie rozwiązań równoważnych nie może prowadzić do pogorszenia właściwości przedmiotu zamówienia w stosunku do przewidzianych w niniejszym zaproszeniu, ani do zmiany ceny.