Lp.	Opis parametru	Parametr wymagany	Wartość oferowana - wypełnia Wykonawca
1	Wszystkie oferowane produkty fabrycznie nowe, nie rekondycjonowane, rok produkcji min. 2020	TAK, podać	
2	Wykonawca zobowiązany jest załączyć na wezwanie Zamawiającego następujące dokumenty: foldery, katalogi i/lub ulotki (wszystkie materiały w j. polskim) oferowanego typu produktu oraz inne dokumenty poświadczające, iż zaoferowany sprzęt jest wyprodukowany zgodnie z obowiązującymi normami oraz przepisami prawa.	TAK, dokumenty należy złożyć na wezwanie w zw. z art. 25. ust. 1 pkt 2	
3	Wykonawca zobowiązany jest dostarczyć wraz z protokołem zdawczo-odbiorczym: 1) instrukcję obsługi urządzenia w języku polskim: w wersji papierowej i elektronicznej, 2) skróconą wersję instrukcji obsługi i bezpiecznego użytkowania, w formie zalaminowanego dokumentu (jeżeli występuje), 3) wykaz czynności serwisowych, które mogą być wykonywane przez użytkownika samodzielnie, nieskutkujące utratą gwarancji, 4) paszport techniczny (jeśli dotyczy), 5) karty gwarancyjne, 6) wykaz punktów serwisowych na terenie Polski, Dopuszcza się dostarczyć wraz z protokołem zdawczo-odbiorczym : 1) Dokumentacja techniczna producenta w formie elektronicznej w języku angielskim – przy zapewnieniu możliwości wydrukowania tej dokumentacji. Dopuszcza się dostarczenie np. pliku PDF z dokumentacją do aktualnej/zainstalowanej na urządzeniu wersji oprogramowania systemowego 2) Certyfikaty/potwierdzenie przedłożone przez dystrybutora lub centrum serwisowe na Polskę zaświadczające, iż dostarczone urządzenia są objęte wsparciem technicznym producenta 3) Certyfikaty/potwierdzenie przedłożone przez dystrybutora lub centrum serwisowe na Polskę zaświadczające, iż dostarczone urządzenia posiadają aktywne kontrakty dla usług/licencji czasowych i subskrypcyjnych.	TAK, dołączyć na etapie dostawy wyposażenia	
4	Wykonawca jest zobowiązany (na własny koszt i we własnym zakresie) do dostawy, montażu i uruchomienia oferowanego produktu.	TAK	
5	W ramach oferty Wykonawca zobowiązany jest po dokonanej dostawie, montażu i uruchomieniu do odebrania opakowań po dostarczonym, zmontowanym i uruchomionym produkcie i utylizacji we własnym zakresie i na własny koszt.	TAK	
6	Wykonawca dostarczy i zainstaluje produkt w miejscu wskazanym przez Zamawiającego. Wymiary należy zweryfikować w miejscu instalacji przed terminem przystąpienia do realizacji przedmiotu umowy przez wykonawcę (termin do uzgodnienia z zamawiającym),(jeśli dotyczy).	TAK	

Lp.	Opis parametru	Parametr wymagany	Wartość oferowana - wypełnia Wykonawca
7	Wykonawca odbył wizję lokalną (wskazanie nie obowiązek)	TAK/NIE	
8	Wykonawca nie może podczas realizacji zawartej umowy powoływać się na jakiekolwiek okoliczności dotyczące wykonania robót, które były możliwe do ustalenia podczas przeprowadzonej z należytą starannością wizji lokalnej	TAK	
9	Warunki gwarancji i serwisu - zgodnie z zapisami SIWZ	TAK	

Pozycja 1	**Dostawa, instalacja i konfiguracja Firewall urządzenia centralnego pracującego jako dwa urządzenia działające w klastrze niezawodnościowym.**	**Liczba sztuk: 1**	
1	Nazwa produktu	podać	
2	Model/typ	podać	
3	Producent/kraj	podać	
4	Rok produkcji	podać	
	Wymagania minimalne		
1	Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19”. Całość sprzętu musi być zarządzana przez jednego producenta.	TAK/podać	
2	Urządzenie musi być wyposażone w 12 interfejsów 1GE Ethernet (RJ45 10/100/1000) 8 interfejsów 1/10GE SFP+ lub opcjonalnie 8 interfejsów 1GE SFP i 8 interfejsów 10GE SFP.	TAK/podać	
3	Urządzenie musi być wyposażone dedykowany port zarządzania. Port ten musi być wydzielony i musi pracować w innej instancji routingu co porty obsługujące ruch poddawany inspekcji. Urządzenie musi być wyposażone w rozwiązanie pozwalające co najmniej na wydzielenie modułu zarządzania i modułu przetwarzania danych na poziomie fizycznym lub sprzętowym (wówczas urządzenie musi zapewniać dedykowane procesory i pamięć dla realizacji modułu zarządzania).	TAK/podać	
4	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 6 Gbps dla Firewall/kontroli aplikacji Minimum 3 Gbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Minimumm 75 tys. nowych połączeń na sekundę. Minimum 2.000.000 równoległych sesji Scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych. Scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.	TAK/podać	
5	Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy a. routera (tzn. w warstwie 3 modelu OSI), b. przełącznika (tzn. w warstwie 2 modelu OSI), c. w trybie pasywnego nasłuchu (sniffer).	TAK/podać	

6	Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)	TAK/podać	
7	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi po-zwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.	TAK/podać	
8	Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.	TAK/podać	
9	Urządzenie musi umożliwiać zestawianie 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 musi odbywać się na bazie technologii SSL VPN.	TAK/podać	
10	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Mini-mum 3 Gbps dla IPSEC VPN Minimum 2 000 tuneli IPSEC VPN (site-to-site) Mi-nimum 2 000 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. Jeże-li wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN (dla Windows) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 2000 jednoczesnych użytkowników	TAK/podać	
11	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej - oznaczania pakietów znacznikami DiffServ, - ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. - utworzenia co najmniej 8 klas ruchu sieciowego. kształtowania ruchu sieciowego (QoS) per - sesja na podstawie znaczników DSCP. - przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego	TAK/podać	
12	Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.	TAK/podać	
13	Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.	TAK/podać	
14	Urządzenie musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu.	TAK/podać	
15	Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu	TAK/podać	
16	Urządzenie musi umożliwiać obsługę klastra niezawodnościowego– tworzenia konfiguracji	TAK/podać	

	odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.		
17	Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 5 000 reguł polityki bezpieczeństwa oraz obsługę minimum 100 stref bezpieczeństwa.	TAK/podać	
18	Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. 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. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.	TAK/podać	
19	Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM), w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.	TAK/podać	
20	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.	TAK/podać	
21	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.	TAK/podać	
22	Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w identyfikowanych 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.	TAK/podać	
23	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download"	TAK/podać	
24	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.	TAK/podać	
25	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH	TAK/podać	

26	Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory, b) usługi katalogowe LDAP, c) serwery Terminal Services. d) logi z syslog	TAK/podać	
27	Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.	TAK/podać	
28	Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. W takim przypadku należy wraz z firewallem dostarczyć dedykowaną konsolę zarządzania. Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia.	TAK/podać	
29	Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia.	TAK/podać	
30	Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu	TAK/podać	

	bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. W takim przypadku należy wraz z firewallem dostarczyć dedykowaną konsolę zarządzania. Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia.		
31	Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę 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). Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia	TAK/podać	
32	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej	TAK/podać	
33	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. W takim przypadku należy wraz z firewallem dostarczyć dedykowaną konsolę zarządzania. Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia	TAK/podać	
34	Urządzenie musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msoff-fice, java, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) 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. Zamawiający NIE wymaga dostarczenia licencji na współpracę z sandboxem lokal-nym i sandboxem chmurowym w chwili zakupu urządzenia.	TAK/podać	
35	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).	TAK/podać	
36	System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa	TAK/podać	

	konta typu: a. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu b. Operator, który ma możliwość tylko odczytu konfiguracji. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą a. bazy lokalnej, b. serwera LDAP, c. RADIUS lub TACACS+ d. SAML 2,0 Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS		
37	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej.	TAK/podać	
38	Urządzenie musi zapewniać interfejs API - co najmniej jeden z: JSON, REST, XML- będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI)	TAK/podać	
39	Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określnego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.	TAK/podać	
40	Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.	TAK/podać	
41	Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie.	TAK/podać	
42	Urządzenie musi pozwalać na blokowanie transmisji plików szyfrowanych co najmniej a. Dokumentów office (doc, xls, ppt) b. Plików skompresowanych (zip, rar)	TAK/podać	
43	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.	TAK/podać	
44	Urządzenie 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.	TAK/podać	

45	Usługa wsparcia technicznego. Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji zgłoszeń gwarancyjnych w trybie 24x7. Usługa wsparcia technicznego musi obejmować również usługi abonamentowe (subskrypcje) obejmujące aktualizacje sygnatur dla wszystkich wymaganych funkcji ochrony opisanych w OPZ dla poszczególnych urządzeń.	TAK/podać	
46	Szkolenie dla pracowników Działu Informatyki WSRM w Łodzi w wymiarze 15 godzin dla 3 osób.	TAK/podać	

Pozycja 2	**Dostawa, instalacja i konfiguracja Firewall urządzeń w lokalizacjach zdalnych**	**Liczba sztuk: 4**	
1	nazwa produktu	podać	
2	model/typ	podać	
3	producent/kraj	podać	
Wymagania minimalne			
1	Urządzenie musi być dostarczone jako dedykowane urządzenie typu appliance, przystosowane do montażu w szafie Rack 19”. Całość sprzętu musi być zarządzana przez jednego producenta.	TAK/podać	
2	Urządzenie musi być wyposażone w 8 interfejsów 1GE Ethernet (RJ45 10/100/1000)	TAK/podać	
3	Urządzenie musi być wyposażone dedykowany port zarządzania.	TAK/podać	
4	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 500 Mbps dla Firewall/kontroli aplikacji Minimum 250 Mbps dla Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Minimum 3 000 nowych połączeń na sekundę. Minimum 50.000 równoległych sesji Scenariusz Firewall/kontroli aplikacji Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa w tym przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych. Scenariusz Firewall/IPS/Antywirus/kontroli aplikacji/Antymalware Zamawiający rozumie, iż urządzenie pozwoli na wykrycie aplikacji, przydzielenie do niej polityki bezpieczeństwa obejmującej przypisanie uprawnień użytkownikom do korzystania z określonych aplikacji sieciowych, inspekcje IPS, Antywirus, Anty Spyware. Zakres kontroli musi też obejmować przesyłanie plików do sandboxa lokalnego i chmurowego w tym przechwytywanie i blokowanie plików określonego typu. Scenariusz ten musi być realizowany z włączonym pełnym zakresem ochrony tj. z włączonymi wszystkimi dostępnymi dla urządzenia sygnaturami IPS, antywirus i antyspyware.	TAK/podać	
5	Urządzenie musi umożliwiać działanie co najmniej w trzech trybach pracy a. routera (tzn. w warstwie 3 modelu OSI), b. przełącznika (tzn. w warstwie 2 modelu OSI), c. w trybie pasywnego nasłuchu (sniffer).	TAK/podać	
6	Tryb pracy urządzenia musi być ustalany bądź w konfiguracji interfejsu sieciowego bądź w ustawieniach systemu, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny kontekst/system/firewall/, wirtualna domena, itp.)	TAK/podać	
7	Urządzenie musi obsługiwać protokół Ethernet z obsługą sieci VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN zgodnych z 802.1q. Urządzenie musi pozwalać na tworzenie tzw. subinterfejsów na interfejsach pracujących w trybie L2 i L3.	TAK/podać	

8	Urządzenie musi umożliwiać translację adresów IP (NAT) zarówno statyczną jak i dynamiczną. Reguły dotyczące NAT muszą być odrębne od reguł definiujących polityki bezpieczeństwa tak aby reguły dotyczące translacji nie powodowały w żaden sposób zależności od konfiguracji tych polityk.	TAK/podać	
9	Urządzenie musi umożliwiać zestawianie 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 musi odbywać się na bazie technologii SSL VPN.	TAK/podać	
10	Urządzenie musi spełniać co najmniej następujące parametry wydajnościowe: Minimum 400 Mbps dla IPSEC VPN Minimum 200 tuneli IPSEC VPN (site-to-site) Minimum 200 tuneli SSL VPN Remote Access z wykorzystaniem klienta VPN. Jeżeli wykorzystanie funkcji VPN (IPSec i SSL) wymaga zakupu dodatkowych licencji, lub jeżeli dedykowany klient VPN (dla Windows) oferowany przez producenta firewall wymaga zakupu dodatkowych licencji to należy je przewidzieć w ofercie dla maksymalnej jego wydajności tzn. dla 200 jednoczesnych użytkowników.	TAK/podać	
11	Urządzenie musi zapewniać zarządzanie pasmem sieci (QoS) w zakresie co najmniej oznaczania pakietów znacznikami DiffServ, ustawiania dla dowolnych aplikacji priorytetu, pasma maksymalnego i gwarantowanego. utworzenia co najmniej 8 klas ruchu sieciowego. kształtowania ruchu sieciowego (QoS) per sesja na podstawie znaczników DSCP. przydzielania takiej samej klasy QoS dla ruchu wychodzącego i przychodzącego	TAK/podać	
12	Urządzenie musi posiadać funkcję ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.	TAK/podać	
13	Urządzenie musi umożliwiać obsługę protokołów routingu minimum RIP, OSPF oraz BGP.	TAK/podać	
14	Urządzenie musi obsługiwać nie mniej niż 2 wirtualne routery posiadające odrębne tabele routingu	TAK/podać	
15	Urządzenie musi wspierać mechanizm PBR (policy base routing) dla wybranych aplikacji i wskazanych użytkowników – mechanizm przekierowania ruchu z pominięciem tablicy routingu.	TAK/podać	
16	Urządzenie musi umożliwiać obsługę klastra niezawodnościowego – tworzenia konfiguracji odpornej na awarie dla urządzeń. Urządzenia w klastrze muszą funkcjonować w trybie Active/Passive i Active/Active.	TAK/podać	
17	Polityka bezpieczeństwa systemu zabezpieczeń musi prowadzić kontrolę ruchu sieciowego i uwzględniać strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji, kategorie URL reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem QoS. Urządzenie musi umożliwiać zdefiniowanie nie mniej niż 500 reguł	TAK/podać	

	polityki bezpieczeństwa oraz obsługę minimum 10 stref bezpieczeństwa.		
18	Urządzenie musi umożliwiać rozpoznawanie aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM). Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury. 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. Urządzenie musi wykrywać co najmniej 3000 predefiniowanych aplikacji wspieranych przez producenta (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS oraz pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi.	TAK/podać	
19	Urządzenie musi przeprowadzać kontrolę aplikacji w sposób umożliwiający potraktowanie informacji o niej jako atrybutu a nie jako wartości w polityce bezpieczeństwa. W szczególności dotyczy to implementacji w modułach innych jak firewall (np. w IPS lub innym module UTM) w których informacja o aplikacji będzie mogła być tylko wykorzystana jako „wartość" w polityce.	TAK/podać	
20	Urządzenie musi pozwalać na definiowanie i przydzielanie różnych profili ochrony (antywirus, IPS, URL, blokowanie plików) per aplikacja. Musi być możliwość przydzielania innych profili ochrony (AV, IPS, URL, blokowanie plików) dla dwóch różnych aplikacji pracujących na tym samym porcie.	TAK/podać	
21	Urządzenie musi pozwalać na blokowanie transmisji plików, nie mniej niż: bat, cab, pliki MS Office, rar, zip, exe, gzip, hta, pdf, tar, tif. Rozpoznawanie pliku musi odbywać się na podstawie nagłówka i typu MIME, a nie na podstawie rozszerzenia.	TAK/podać	
22	Urządzenie musi pozwalać na analizę i blokowanie plików przesyłanych w identyfikowanych 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.	TAK/podać	
23	Urządzenie musi zapewniać ochronę przed atakami typu „Drive-by-download"	TAK/podać	
24	Urządzenie musi posiadać możliwość zdefiniowania ruchu SSL który należy poddać lub wykluczyć z operacji deszyfrowania i głębokiej inspekcji rozdzielny od polityk bezpieczeństwa.	TAK/podać	
25	Urządzenie musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.	TAK/podać	
26	Rozwiązanie musi umożliwiać uwierzytelnienie użytkowników lub transparentne ustalenie jego tożsamości w oparciu o: a) Microsoft Active Directory, b) usługi katalogowe LDAP, c) serwery Terminal Services. d) logi z syslog	TAK/podać	

27	Polityka kontroli dostępu urządzenia musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług sieci i musi być utrzymywana nawet gdy użytkownik zmieni lokalizację i adres IP a w przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.	TAK/podać	
28	Urządzenie musi posiadać funkcjonalność Intrusion Prevention System (IPS) wraz z aktualizacją sygnatur w okresie gwarancji. System IPS musi działać w warstwie 7 modelu OSI. Baza sygnatur IPS/IDS musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent urządzenia. Moduł IPS/IDS musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja IPS/IDS uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa) Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. W takim przypadku należy wraz z firewallem dostarczyć dedykowaną konsolę zarządzania. Zamawiający wymaga dostarczenia licencji na IPS w chwili zakupu urządzenia.	TAK/podać	
29	Urządzenie musi posiadać funkcjonalność Antywirus (AV) wraz z aktualizacją sygnatur w okresie gwarancji Moduł AV musi być uruchamiany per aplikacja oraz wybrany dekoder taki jak http, smtp, imap, pop3, ftp, smb Baza sygnatur AV musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny nie rzadziej niż co 24 godziny i pochodzić od tego samego producenta co producent systemu zabezpieczeń Moduł AV musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby modułu inspekcji antywirusowej uruchamiany był per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Zamawiający wymaga dostarczenia licencji na ochronę antywirusową w chwili zakupu urządzenia.	TAK/podać	
30	Urządzenie musi zapewniać ochronę przed atakami typu Spyware – Zamawiający dopuszcza by odbywało się to poprzez silnik AV lub silnik IPS lub silnik antymalware lub dedykowany silnik antyspyware. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń. Reguły/silnik anty-spyware musi uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja ta była uruchamiana była per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Urządzenie musi zapewniać możliwość ręcznego tworzenia sygnatur tego typu bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. W takim przypadku należy wraz z firewallem dostarczyć dedykowaną konsolę zarządzania. Zamawiający wymaga dostarczenia licencji na silnik Antyspyware w chwili zakupu urządzenia	TAK/podać	

31	Urządzenie musi posiadać narzędzia wykrywające i blokujące ruch do domen uznanych za złośliwe (sygnatury DNS). Rozwiązanie musi umożliwiać podmianę 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). Zamawiający wymaga dostarczenia licencji na ochronę DNS w chwili zakupu urządzenia.	TAK/podać	
32	Urządzenie musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.	TAK/podać	
33	Urządzenie musi posiadać możliwość rozbudowy o funkcjonalność URL Flitering. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 200 milionów rekordów URL. Moduł filtrowania stron WWW musi mieć możliwość uruchomienia per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja filtrowania stron WWW uruchamiana była tylko per całe urządzenie lub jego interfejs fizyczny/logiczny (np. interfejs sieciowy, interfejs SVI, strefa bezpieczeństwa). Moduł filtrowania stron WWW musi zapewniać możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta. Zamawiający dopuszcza, aby funkcja ręcznego tworzenia sygnatur była realizowana z poziomu centralnej konsoli zarządzania i monitorowania. W takim przypadku należy wraz z firewallem dostarczyć dedykowaną konsolę zarządzania. Zamawiający wymaga dostarczenia licencji na URL Filtering w chwili zakupu urządzenia.	TAK/podać	
34	Urządzenie musi posiadać funkcjonalność ochrony przed atakami day 0 i współpracy z sandboxem Urządzenie musi umożliwiać przechwytywanie i przesyłanie do zewnętrznych systemów typu „Sand-Box" plików różnych typów (exe, dll, pdf, msofffice, java, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus (zdefiniowaną w szczegółowych wymaganiach wydajnościowych) 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. Zamawiający NIE wymaga dostarczenia licencji na współpracę z sandboxem lokalnym i sandboxem chmurowym w chwili zakupu urządzenia.	TAK/podać	
35	Zarządzanie urządzeniem musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).	TAK/podać	
36	System zabezpieczeń musi pozwalać na zdefiniowanie wielu administratorów o różnych uprawnieniach w szczególności Urządzenie musi mieć zdefiniowane w systemie co najmniej dwa konta typu: a. Administrator, który ma pełen dostęp do konfiguracji, odczytu i zapisu b. Operator, który ma możliwość tylko odczytu konfiguracji. Urządzenie musi umożliwiać uwierzytelnianie administratorów za pomocą a. bazy lokalnej,	TAK/podać	

	b. serwera LDAP, c. RADIUS lub TACACS+ d. SAML 2,0 Musi być zapewniona możliwość stworzenia sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS		
37	Praca na urządzeniu musi odbywać się na konfiguracji kandydackiej, a nie aktywnej. Zmiany w konfiguracji aktywnej odbywają się poprzez zatwierdzanie zmian (ang. Commit). Przed zatwierdzaniem zmian na urządzeniu musi być możliwość przejrzenia zmian, które zostały wykonane na konfiguracji kandydackiej.	TAK/podać	
38	Urządzenie musi zapewniać interfejs API - co najmniej jeden z: JSON, REST, XML - będący integralną częścią systemu zabezpieczeń za pomocą którego możliwa jest konfiguracja i monitorowanie stanu urządzenia bez użycia konsoli zarządzania lub linii poleceń (CLI)	TAK/podać	
39	Urządzenie musi zapewniać możliwość zapisania min. 20 poprzednich wersji konfiguracji na dysku twardym urządzenia. Urządzenie musi mieć możliwość przywrócenia konfiguracji z określnego dnia, w którym były dokonywane zmiany, tzn. po każdym zapisie konfiguracji na urządzeniu powinna być automatycznie zapisywana kompletna konfiguracja, a podczas wyboru konfiguracji musi być widoczna data zapisania konfiguracji.	TAK/podać	
40	Urządzenie musi umożliwiać eksportowanie logów do zewnętrznych serwerów SYSLOG.	TAK/podać	
41	Urządzenie musi być wyposażone w zasilacze typu AC pracujące redundantnie.	TAK/podać	
42	Urządzenie musi pozwalać na blokowanie transmisji plików szyfrowanych co najmniej a. Dokumentów office (doc, xls, ppt) b. Plików skompresowanych (zip, rar)	TAK/podać	
43	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.	TAK/podać	
44	Urządzenie 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.	TAK/podać	
45	Usługa wsparcia technicznego. Wymagane jest dostarczenie wsparcia producenta na okres 36 miesięcy od podpisania protokołu odbioru. Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie i automatyczny system obsługi zgłoszeń przez autoryzowany ośrodek serwisowy. Usługa powinna obejmować dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Sposób realizacji	TAK/podać	

	zgłoszeń gwarancyjnych w trybie 24x7. Usługa wsparcia technicznego musi obejmować również usługi abonamentowe (subskrypcje) obejmujące aktualizacje sygnatur dla wszystkich wymaganych funkcji ochrony opisanych w OPZ dla poszczególnych urządzeń.		
46	Szkolenie dla pracowników Działu Informatyki WSRM w Łodzi w wymiarze 15 godzin dla 3 osób.	TAK/podać	