OPIS PRZEDMIOTU ZAMÓWIENIA

Doposażenie infrastruktury KCMRM

Spis treści

1.SŁOWNIKI I SKRÓTY

Dla potrzeb niniejszego opracowania przyjmuję się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Błąd	Oznacza Błąd Krytyczny i/lub Błąd Niekrytyczny i/lub Błąd Zwykły;
Błąd Krytyczny	Oznacza brak działania środowiska produkcyjnego Systemu Kopii Bezpieczeństwa, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Błędy Krytyczne mają jedną lub więcej z poniższych cech: 1)dane biznesowe zostały uszkodzone; 2)Funkcjonalność Krytyczna udokumentowana w Projekcie Technicznym nie działa; 3)System w zakresie Funkcjonalności Krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji; 4)wszelkie błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na: a) uwierzytelnianie, b) niezaprzeczalność, c) poufność, d) integralność, e) dostępność, f) rozliczalność, 5)wszelkie błędy związane z bezpieczeństwem dostępu do Systemu (w tym nieautoryzowanym dostępem do danych);
Błąd Zwykły	Wszelki błąd niebędący Błędem Krytycznym lub Błędem Niekrytycznym;
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8:00 do 15:35;
Lokalizacje	Oznacza wskazane przez Zamawiającego lokalizacje na terenie RP określone w Projekcie Technicznym, do których Wykonawca dostarczy wymagane przez Zamawiającego Urządzenia i Oprogramowanie wraz z odnoszącą się do nich dokumentacją techniczną producenta będące przedmiotem niniejszego zamówienia;
KCMRM	Krajowe Centrum Monitorowania Ratownictwa Medycznego
POK /Podstawowy Ośrodek Krajowy	Centrum serwerowe w oparciu, o które zbudowana została architektura systemu SWD PRM na poziomie centralnym. Jest to

Skrót/pojęcie	Definicja
	obecnie istniejąca infrastruktura SWD PRM wraz z aktualnie wykorzystywanym oprogramowaniem;
PRM	Państwowe Ratownictwo Medyczne;
SWD PRM	Systemy Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego wraz z zainstalowanym oprogramowaniem standardowym, aplikacyjnym oraz infrastrukturą sprzętową.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia;
Urządzenia	Sprzęt wraz z niezbędnym wyposażeniem i odnoszącą się do niego dokumentacją techniczną producenta
Wykonawca/Dostawca	Podmiot realizujący zamówienie;
Zamawiający	Lotnicze Pogotowie Ratunkowe;

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

1. Cel zamówienia

Przedmiotowe postępowanie dotyczy dostawy urządzeń klasy New Generation Firewall a potrzeby doposażenia infrastruktury KC MRM, jest to niezbędne celem wydzielenie bezpiecznego kanału komunikacji pomiędzy zarządzaniem o istniejącą infrastrukturą SWD PRM. Kanał komunikacji będzie służył zarówno pracownikom jak również kontrahentom i serwisowi.

Jeżeli w OPZ użyto do opisania przedmiotu zamówienia oznaczeń lub parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty, normy, standardy, aprobaty techniczne lub pochodzenie urządzeń, Zamawiający dopuszcza zastosowanie produktów równoważnych, przez które należy rozumieć produkty o parametrach nie gorszych od przedstawionych w OPZ, kompatybilne (współpracujące) z posiadanym przez Zamawiającego systemem monitoringu w tym samym zakresie, co produkty określone w OPZ oraz posiadający równoważne funkcje i parametry co produkt opisany w OPZ. W takim wypadku do oferty należy załączyć dokładny opis oferowanych produktów, z którego jasno wynikać będzie zachowanie warunków równoważności.

Wszystkie Urządzenia dostarczone w ramach realizacji przedmiotu umowy muszą spełniać co najmniej poniższe warunki:

1) muszą być dostarczone jako fabrycznie nowe, nie używane w innych projektach, oraz nie starsze niż 4 miesiące od daty produkcji,

2) muszą pochodzić z oficjalnego kanału dystrybucji na Polskę lub Unię Europejską dla danego producenta,
3) zarówno Urządzenia jak i jego elementy składowe wraz z systemami operacyjnymi oraz aplikacjami nie mogą znajdować się na aktualnej, na czas składania ofert, liście elementów producenta przewidzianych do wycofania z produkcji, sprzedaży lub serwisowania,
4) Urządzenia i Oprogramowanie muszą być objęte 36 miesięczną gwarancją.
5) Wykonawca zapewni prawo do pobierania nowych wersji i aktualizacji przez okres minimum 36 miesięcy od podpisania protokołu odbioru przedmiotu Umowy bez zastrzeżeń,
6) wszelkie koszty dostawy przedmiotu zamówienia pokryje Wykonawca (transport i wyładunek do miejsca wyznaczonego przez Zamawiającego),

2.Dostawa urządzeń typu firewall NGFW

Postępowanie obejmuje dostawę 2 (dwóch) urządzeń typu Firewall Następnej Generacji na potrzeby doposażenia infrastruktury KC MRM z wymaganymi licencjami oprogramowania oraz gwarancją producenta na okres 36 miesięcy. Urządzenia powinny zostać dostarczone w poniższym ukompletowaniu:

Produkt	Opis	Ilość
PAN-PA-820	Palo Alto Networks PA-820	2
PAN-PA-820-TP-3YR-HA2	Threat protection subscription 3-year prepaid for device in an HA pair, PA-820	2
PAN-PA-820-URL4-3YR-HA2	PANDB URL filtering subscription 3-year prepaid for device in an HA pair, PA-820	2
PAN-PA-820-WF-3YR-HA2	WildFire subscription 3-year prepaid for device in an HA pair, PA-820	2
PAN-SVC-BKLN-820-3YR	Partner enabled premium support 3 year prepaid, PA-820	2

Zamawiający dopuszcza rozwiązanie równoważne, pod warunkiem spełnienia przez nie następujących minimalnych wymagań:

Kod wymagania	Opis
NGFW.01	System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenie zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja modułu zarządzania i modułu przetwarzania danych. Całość sprzętu i oprogramowania musi być dostarczana i wspierana przez jednego producenta.
NGFW.02	System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 900 Mbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 600 Mbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 120 000 jednoczesnych połączeń.
NGFW.03	System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 10/100/1000, 8 portów 1Gbps SFP

NGFW.04	System zabezpieczeń firewall musi działać w trybie rutera (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.
NGFW.05	Tryb pracy urządzenia musi być ustalany w konfiguracji interfejsu sieciowego, a system musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
NGFW.06	System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Subinterfejsy VLAN mogą być tworzone na interfejsach sieciowych pracujących w trybie L2 i L3. Urządzenie musi obsługiwać 4094 znaczników VLAN.
NGFW.07	System zabezpieczeń firewall musi obsługiwać nie mniej niż 5 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jednej tablicy routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
NGFW.08	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).
NGFW.09	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).
NGFW.10	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.
NGFW.11	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.
NGFW.12	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 900 Mbit/s.

NGFW.13	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).
NGFW.14	Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
NGFW.15	Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
NGFW.16	System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS.
NGFW.17	System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
NGFW.18	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.
NGFW.19	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.
NGFW.20	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.
NGFW.21	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.
NGFW.22	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.

NGFW.23	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.
NGFW.24	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.
NGFW.25	System zabezpieczeń posiada 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.
NGFW.26	System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.
	Wymagania podstawowe identyfikacja użytkowników
NGFW.27	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.
NGFW.28	System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów 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.
NGFW.29	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.
NGFW.30	Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.
	Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day

NGFW.31	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.
NGFW.32	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).
NGFW.33	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
NGFW.34	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.
NGFW.35	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.
NGFW.36	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).
NGFW.37	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.
NGFW.38	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).
NGFW.39	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
NGFW.40	System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywania na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego

	producenta co producent systemu zabezpieczeń.
NGFW.41	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).
NGFW.42	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
NGFW.43	System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
NGFW.44	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).
NGFW.45	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.
NGFW.46	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.
NGFW.47	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.
NGFW.48	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
NGFW.49	System zabezpieczeń firewall musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msofffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 700 Mbit/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.

NGFW.50	Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
NGFW.51	Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msofffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.
NGFW.52	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.
	Wymagania dodatkowe NAT, DoS, IPSEC VPN, SSL VPN, QoS
NGFW.53	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.
NGFW.54	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
NGFW.55	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.
NGFW.56	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 rutingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.
NGFW.57	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.
NGFW.58	System zabezpieczeń firewall musi umożliwiać konfigurację jednolitej polityki bezpieczeństwa dla użytkowników niezależnie od ich fizycznej lokalizacji oraz niezależnie od obszaru sieci, z którego uzyskują dostęp (zasady dostępu do zasobów wewnętrznych oraz do Internetu są takie same zarówno podczas pracy w sieci korporacyjnej jak i przy połączeniu do Internetu poza siecią korporacyjną). Musi istnieć możliwość weryfikacji poziomu bezpieczeństwa komputera użytkownika przed przyznaniem mu uprawnień dostępu do sieci.

NGFW.59	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.
NGFW.60	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.
NGFW.61	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
NGFW.62	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.
	Wymagania dodatkowe środowisko wirtualne vmware
NGFW.63	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.
	Wymagania zarządzanie i raportowanie
NGFW.64	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.
NGFW.65	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.
NGFW.66	System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
NGFW.67	System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.

NGFW.68	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).
NGFW.69	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.
NGFW.70	System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
NGFW.71	System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
NGFW.72	System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240GB. 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.
NGFW.73	System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
NGFW.74	System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
NGFW.75	System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
NGFW.76	System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
NGFW.77	System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
NGFW.78	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.
NGFW.79	System zabezpieczeń firewall 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.
NGFW.80	System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.

NGFW.81	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.
NGFW.82	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

Załącznik nr ……

3. GWARANCJA, RĘKOJMIA I SERWISOWANIE

1. Wykonawca wraz z dostawą Urządzeń przekaże warunki gwarancyjne i serwisowe Urządzeń, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta.
2. Wymagania gwarancyjne:
   1) Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu:
      a) prawo do pobierania nowych wersji i aktualizacji przez okres minimum 36 miesięcy od podpisania protokołu odbioru przedmiotu zamówienia,
      b) przyjmowanie w ramach serwisu zgłoszeń Zamawiającego przez 24 godziny na dobę, 7 dni w tygodniu.
      c) wymianę Urządzeń w przypadku zdiagnozowania awarii powodującej całkowity brak możliwości korzystania z Urządzenia,
      d) dostarczenie sprawnego Urządzenia lub jego elementu podlegającego wymianie do miejsca zainstalowania Urządzenia uszkodzonego,
      e) możliwość aktualizacji oprogramowania poprzez dostęp do zasobów producenta rozwiązania,
      f) dostęp do pomocy technicznej producenta,
      g) Gwarancją producenta muszą zostać objęte wszystkie dostarczone Urządzenia wraz z Oprogramowaniem przez okres minimum 36 miesięcy, przy czym bieg okresu gwarancji rozpocznie się z chwilą podpisania bez zastrzeżeń protokołu odbioru przedmiotu umowy. Okres rękojmi za wady Urządzeń jest równy okresowi udzielonej gwarancji.
   2) Do dostarczonych Urządzeń będą dołączone karty gwarancyjne zawierające numery seryjne produktu, numery seryjne oprogramowania, termin i warunki ważności gwarancji (zgodnie z umową), adresy i numery telefonów punktów serwisowych świadczących usługi gwarancyjne.
3. Do przedmiotu Umowy muszą zostać dostarczone procedury zgłaszania awarii w formie dokumentów drukowanych.
4. Do kontaktów/zgłoszeń Wykonawca udostępnia:
   1) numer telefonu – _____ (infolinia bezpłatna), ___ (dla telefonów komórkowych i z zagranicy);
   2) numer faksu - _____;
   3) e-mail - _____
5. Wykonawca zobowiązuje się do świadczenia usług gwarancyjnych w trybie Następnego Dnia Roboczego z zastrzeżeniem postanowień Umowy.
6. Ilekroć w treści niniejszego dokumentu jest mowa o awarii rozumie się taki stan Urządzeń i Oprogramowania, który uniemożliwia korzystanie z przedmiotu zamówienia.
7. Zamawiający wymaga, aby awaria została usunięta następnego dnia roboczego od chwili jej zgłoszenia.

8. W przypadku braku możliwości wykonania naprawy w terminie podanym wyżej, Wykonawca na okres przedłużającej się naprawy bądź usuwania awarii, dostarczy Urządzenie zastępcze, równoważne funkcjonalnie. Po zakończeniu naprawy Urządzenie zastępcze zostanie zwrócone Wykonawcy z wyłączeniem nośników danych.
9. Uszkodzone elementy Urządzenia będą wymienione przez Wykonawcę na nowe, wolne od wad i o parametrach nie gorszych od uszkodzonych.
10. W okresie gwarancji, w przypadku awarii dysku twardego lub innego nośnika danych, będzie on wymieniony przez gwaranta na nowy bez konieczności zwrotu uszkodzonego dysku twardego lub innego nośnika danych przez Zamawiającego i dokonywania ekspertyzy dysku poza siedzibą Zamawiającego.
11. Przez usunięcie awarii należy rozumieć przywrócenie pierwotnej funkcjonalności sprzętu i systemu operacyjnego sprzed wystąpienia awarii.
12. Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady.
13. Z tytułu świadczenia przez Wykonawcę usługi serwisu gwarancyjnego Zamawiający nie ponosi dodatkowych kosztów.
14. Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy Producenta, rozbudowy posiadanych urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego Urządzenia.

Załącznik nr ……..

4. Zasady Odbioru Przedmiotu Umowy

1. Przedmiot Umowy należy dostarczyć zgodnie z zasadami i terminem wskazanymi w Umowie, nie później jednak niż w ciągu 14 dni od dnia podpisania Umowy.
2. Odbiór zostanie przeprowadzony w siedzibie Zamawiającego przy ul. Maszowska 20 w Warszawie , pierwsze piętro, pokój nr.14,w obecności przedstawicieli Wykonawcy i Zamawiającego w godz. 8:00-15:35.
3. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy Protokołu ilościowo-jakościowego.
4. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu umowy i potwierdzenie zgodności z ilością określoną w umowie oraz sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.
5. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego Przedmiotu Umowy.
6. Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzenia kompletności oraz poprawności działania Urządzeń wraz z dostarczanymi licencjami w ramach Umowy.

Załącznik nr

PROTOKÓŁ ODBIORU ILOŚCIOWO – JAKOŚCIOWEGO - *wzór*
do umowy nr ..... z dnia.....r.

Miejsce dokonania odbioru:
.....
Data dokonania odbioru:
.....
Ze strony Wykonawcy:
.....
(nazwa i adres)
.....
(przedstawiciel wykonawcy)
Ze strony Zamawiającego:
.....
(nazwa i adres)
Komisja do obioru przedmiotu Umowy w składzie:
……..
……..
…….

Przedmiotem odbioru ilościowo-jakościowego przeprowadzonego w ramach Umowy jest:

Lp.	Nazwa przedmiotu	j.m.	Ilość	Nr seryjny	Cena jednostkowa [netto] (w zł)	Wartość [brutto] (w zł)	Dokumentacja techniczna/ instrukcja obsługi/świadectwo jakości	Uwagi
1								
2								
3								

W ramach odbioru ilościowo-jakościowego, przeprowadzonego do Umowy nr ...z dnia…… na _____, Komisja powołana do odbioru przedmiotu Umowy na mocy Decyzji nr _____z dnia _____, przeprowadziła czynności kontrolne.
Komisja: potwierdza/nie potwierdza* zgodność jakości dostarczonego przedmiot umowy z parametrami, funkcjonalnością zawartymi w opisie Przedmiotu umowy.
Komisja potwierdza/nie potwierdza* kompletność dostarczonego przedmiotu umowy, oprogramowania i licencji na oprogramowanie zgodnie z Umową.

Wynik odbioru ilościowo-jakościowego:
- Pozytywny*
- Negatywny*

Uwagi:.....

Podpisy:

1. .....

2. .....

3..... .....

(w imieniu Zamawiającego) (Przedstawiciel Wykonawcy)

*niewłaściwe skreślić

Załącznik nr 4

……..……..
(miejscowość, data)

……..
(imię i nazwisko)

……
(miejsce zatrudnienia)

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI

Stwierdzam własnoręcznym podpisem, że zobowiązuję się do nie przekazywania, nie ujawniania oraz nie wykorzystywania bez zgody ……. wiadomości udostępnionych przez pracowników i funkcjonariuszy ……. oraz uzyskanych w związku z wykonywaniem Umowy nr …..….. z dnia ……..., zawartej pomiędzy …….. a ……..., a nie podlegających wykluczeniu na podstawie poniższych zapisów:

1) jeżeli informacja została ujawniona publicznie przez stronę, będącą właścicielem informacji chronionej;
2) jeżeli ujawnienia informacji żąda sąd lub organ ścigania w toku prowadzonych czynności na podstawie stosownych przepisów;
3) jeżeli właściciel informacji chronionej wyrazi na to uprzednio zgodę pisemną;
4) jeżeli informacja została uzyskana od osób trzecich bez naruszenia prawnych zobowiązań o poufności informacji.

.....
(podpis)