

Znak sprawy: BA.ais.0420.4.2021

ZAPYTANIE OFERTOWE

Ministerstwo Rolnictwa i Rozwoju Wsi zwraca się z prośbą o złożenie oferty cenowej zgodnie z przedstawionymi wymogami:

1. Przedmiot zamówienia:

Przedmiotem zamówienia jest zakup i wdrożenie zapory sieciowej dla Ministerstwa Rolnictwa i Rozwoju Wsi na okres 36 miesięcy. Szczegółowy zakres rzeczowy zamówienia stanowi załącznik nr 2 do zapytania ofertowego.

2. Termin realizacji zamówienia do 15 dni od dnia zawarcia umowy

3. Kryteria oceny ofert:

Cena = 100 %

4. Wymagania co do oferty cenowej:

- wypełniony w języku polskim formularz „OFERTA”, według wzoru określonego w załączniku nr 1 do zapytania ofertowego

- do oferty należy dołączyć wymagane dokumenty/certyfikaty.

5. Osoba uprawniona do kontaktu: Pan Marek Sychowiec, tel. 22 623 11 14, adres e-mail:

marek.sychowiec@minrol.gov.pl

6. Termin złożenia oferty: do dnia 16 kwietnia do godz 15⁰⁰

7. Termin zgłaszania pytań: do dnia 13 kwietnia do godz 15⁰⁰

8. Sposób złożenia oferty: elektronicznie na adres poczty: marek.sychowiec@minrol.gov.pl, w tytule wpisując: BA.ais.0420.4.2021

Niniejsze zapytanie ofertowe nie stanowi zobowiązania Ministerstwa Rolnictwa i Rozwoju Wsi do zawarcia umowy. Wybór oferty zostanie dokonany zgodnie z przedstawionymi kryteriami oceny ofert.

Grzegorz Żbikowski Dyrektor Biura
Administracyjnego/podpisano elektronicznie/

.....
(miejsowość i data)

.....
.....
(imię i nazwisko lub nazwa i adres wykonawcy)

NIP:
tel. kontaktowy:
adres e-mail:

Zamawiający:
Ministerstwo Rolnictwa
i Rozwoju Wsi
ul. Wspólna 30
00-930 Warszawa

OFERTA

Oferuję realizację zamówienia, którego przedmiotem jest zamówienia jest zakup i wdrożenie zapory sieciowej dla Ministerstwa Rolnictwa i Rozwoju Wsi na okres 36 miesięcy zgodnie z poniższą tabelą:

L.p.	Urządzenie	Ilość	Cena netto [PLN]	Cena brutto [PLN]
1.	Zapora sieciowa	1		
2.	Usługa serwisowa 7/24/NBD	1		
3.	Subskrypcja Threat prevention	1		
4.	Wdrożenie	-		
ŁĄCZNIE WARTOŚĆ BRUTTO				

Wskazana wartość brutto oferty cenowej będzie oceniana w kryterium „Cena”– waga 100 %.

Deklaracja zgodności z opisem minimalnych wymagań technicznych dotyczących zapory sieciowej określonych przez Zamawiającego w poniższej tabeli.

Wymagania minimalne	Spełnia wymagania TAK / NIE
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.	
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.	

System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 10/100/1000, 8 portów 1Gbps SFP.	
Interfejsy sieciowe systemu zabezpieczeń firewall muszą 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.	
Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).	
System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.	
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.	
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).	
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).	
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.	
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.	
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.	
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).	
Nie jest dopuszczalne, aby blokowanie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.	
Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.	
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.	
System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.	

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.	
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.	
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.	
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.	
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.	
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.	
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.	
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.	
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	
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, ustalenie tożsamości musi odbywać się również transparentnie.	
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.	
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 sesję w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.	

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, anti-spyware, URL, zero-day	
System zabezpieczeń firewall musi posiadać moduł filtrowania stron WWW w zależności od kategorii treści stron HTTP bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza web filtering musi być regularnie aktualizowana w sposób automatyczny i posiadać nie mniej niż 20 milionów rekordów URL.	
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).	
System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.	
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.	
System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekodery taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	
System zabezpieczeń firewall musi posiadać moduły inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduły inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).	
System zabezpieczeń firewall musi posiadać moduły 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 przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	
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).	
System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.	
System zabezpieczeń firewall musi posiadać moduł anti-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anti-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.	
System zabezpieczeń firewall musi posiadać moduł anti-spyware uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby funkcja anti-spyware uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).	
System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anti-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.	
System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.	
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).	

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.	
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.	
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.	
System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.	
System zabezpieczeń firewall musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msoffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu antywirus czyli nie mniej niż 600 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.	
Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielanie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".	
Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msoffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.	
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	
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.	
System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.	
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.	
System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.	
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.	

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.	
System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentication) 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.	
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.	
System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.	
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 zarządzanie i raportowanie	
Zarządzanie systemu zabezpieczeń musi odbywać się z linii poleceń (CLI) oraz graficznej konsoli Web GUI dostępnej przez przeglądarkę WWW. Nie jest dopuszczalne, aby istniała konieczność instalacji dodatkowego oprogramowania na stacji administratora w celu zarządzania systemem.	
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.	
System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.	
System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.	
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).	
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.	
System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.	
System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).	
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.	
System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.	
System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.	

System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.	
System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.	
System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.	
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.	
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.	
System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.	
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 łącz sieciowych.	
Pomoc techniczna produktu muszą być dostępne w Polsce.	

- Zobowiązuję się do wykonania przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia stanowiącym załącznik do oferty w terminie wskazanym w zapytaniu ofertowym.
- Zobowiązuję się do zawarcia umowy w terminie i miejscu wskazanym przez Zamawiającego.
- Oferta ważna 30 dni od terminu składania ofert.

.....
 (podpis, pieczęć wykonawcy lub osoby upoważnionej do złożenia oferty)

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest zakup i wdrożenie zapory sieciowej dla Ministerstwa Rolnictwa i Rozwoju Wsi na okres 36 miesięcy.

L.p.	Urządzenie	Ilość
1.	Zapora sieciowa	1
2.	Usługa serwisowa 7/24/NBD	1
3.	Subskrypcja Threat prevention	1
4.	Wdrożenie	-

Dostarczone urządzenie ma być fabrycznie nowe, wolne od wad oraz pochodzić z oficjalnego kanału sprzedaży producenta na rynek polski lub rynek Europejskiego Obszaru Gospodarczego.

I. Zakres wdrożenia:

Celem wdrożenia firewalla jest zapewnienie bezpiecznego dostępu do sieci Internet użytkownikom pracującym w lokalizacji ul. Nowy Świat 6/12 oraz zasobów sieciowych dostępnych w siedzibie głównej Ministerstwa Rolnictwa i Rozwoju Wsi za pośrednictwem bezpiecznego tunelu IPSec VPN.

II. Czynności do wykonania przez Wykonawcę:

1. Instalacja rekomendowanego przez producenta wersji systemu operacyjnego firewalla na urządzeniu
2. Montaż w szafie RACK wskazanej przez zamawiającego w lokalizacji: ul. Nowy Świat 6/12
3. Podłączenie firewalla do przełącznika agregującego za pomocą okablowania typu patchcord o kategorii 6 lub wyższej (warto określić długość wymaganych patchcordów)
4. Dostarczenie niezbędnego okablowania w tym: modułów SPF do prawidłowego podłączenia urządzenia, patchcordów min kat. 6, patchcordy światłowodowe
5. Konfiguracja firewalla:
 - Wstępna konfiguracja firewalla (konfiguracja interfejsów sieciowych, MGMT, NTP, DNS, logowania, VLAN etc.)
 - Stworzenie ZONE bezpieczeństwa oraz polityk dostępowych wraz z profilami bezpieczeństwa
 - Konfiguracja Source NAT
 - Zestawienie tunelu IPSec pomiędzy firewallem, a firewalem pracującym w siedzibie Ministerstwa (PA-3050)
 - Konfiguracja routingu statycznego zapewniającego dostęp do sieci Internet użytkownikom pracującym w sieci lokalnej oraz dostęp do podsieci znajdujących się w podsieci Ministerstwa za pośrednictwem tunelu IPSec
 - Konfiguracja deszyfracji ruchu SSL

6. Konfiguracja switcha posiadanego przez Zamawiającego:
 - Stworzenie VLAN
 - Konfiguracja usługi DHCP na urządzeniu sieciowym
 - Konfiguracja protokołu spanning tree
 - Stworzenie polityk bezpieczeństwa
 - Konfiguracja urządzeń w taki sposób aby zapewnić dostęp do zasobów sieciowych znajdujących się w siedzibie głównej MRiRW pracownikom zlokalizowanym przy ul. Nowy Świat 6/12
 - Instalacja rekomendowanej przez producenta wersji systemu dla urządzeń: Cisco C2960X
7. Konfiguracja aktualnie pracującego firewalla firmy Palo Alto PA-500 jako urządzenia zastępczego na wypadek awarii urządzenia podstawowego
8. Podłączenie 4 urządzeń wielofunkcyjnych do system Centralnego Wydruku znajdującego się w siedzibie głównej MRiRW (zapewnienie komunikacji sieciowej pomiędzy urządzeniami a serwerem Centralnego Wydruku)
9. Stworzenie procedury, instrukcji zastąpienia urządzenia podstawowego na firewall zastępczy w sytuacji awarii urządzenia podstawowego
10. Instalacja rekomendowanej przez producenta wersji systemu operacyjnego firewalla na urządzeniach znajdujących się w siedzibie głównej MRiRW przy ul. Wspólnej 30
11. Zapewnienie wsparcia technicznego przez Wykonawcę w ilości 30 godzin w okresie obowiązywania umowy:
 - wsparcie inżyniera w czasie: pon-pt, godz. 8-17, aż do wyczerpania puli godzin
 - rozliczanie godzin miesięczne, raportowane do Zamawiającego
 - po wykonanej konsultacji raport do Zamawiającego odnośnie pracochłonności
12. Przeprowadzenie przeszkolenia dla 2 administratorów wskazanych przez Zamawiającego w formie trzy dniowych warsztatów po min 5 godzin każdego dnia z zakresu konfiguracji i zarządzania rozwiązaniem klasy NGFW wdrożonym przez Wykonawcę
13. Zagwarantowanie usługi serwisowej wraz z dostępem telefonicznym do serwisu w trybie 7/24/NBD (następny dzień roboczy) dla dostarczonego urządzenia.
14. Sporządzenie i przekazanie Zamawiającemu dokumentacji powykonawczej w terminie 5 dni od dnia podpisania protokołu odbioru. Dokumentacja powykonawcza ma zostać dostarczona w formie papierowej i elektronicznej.

III. Wykonawcy ubiegający się o zamówienie publiczne muszą spełniać niżej wymienione warunki udziału w postępowaniu:

1. Wykonać w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie – minimum 2 zamówienia, których przedmiotem były lub są dostawa i wdrożenie systemu bezpieczeństwa sieciowego, o wartości zamówienia przekraczającej równowartość 200.000,00 zł netto każde.
2. Dysponować osobami, które będą uczestniczyć w wykonywaniu zamówienia, legitymującymi się kwalifikacjami zawodowymi i doświadczeniem, odpowiednimi do funkcji, jakie zostaną im powierzone. Osoby te muszą spełniać następujące wymagania:
 - co najmniej jedna osoba posiadająca ważny certyfikat na poziomie profesjonalisty o specjalizacji bezpieczeństwo, wydany przez producenta lub zewnętrzne jednostki certyfikujące autoryzowane przez producenta sprzętu w oparciu o który, zostanie zbudowany proponowany w ofercie system bezpieczeństwa,
 - co najmniej jedna osoba, która realizowała prace instalacyjno-konfiguracyjne przy minimum dwóch zamówieniach obejmujących łącznie dostawę wraz z wdrożeniem proponowanego w ofercie systemu bezpieczeństwa.

- co najmniej jedna osoba posiadająca ważny certyfikat na poziomie profesjonalisty (Routing and Switching) o specjalizacji w zakresie instalacji, konfiguracji i zarządzania sieciami komputerowymi, wydany przez producenta lub zewnętrzne jednostki certyfikujące autoryzowane przez producenta sprzętu.

Zamawiający dopuszcza przedstawienie jednej osoby spełniającej łącznie warunki określone powyżej.

Dokumenty potwierdzające spełnianie ww. warunków należy dołączyć do oferty.

IV. Podstawowe wymagania techniczne dotyczące zapory sieciowej:

Wymagania podstawowe
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.
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.
System zabezpieczeń firewall musi być wyposażony w co najmniej 4 porty Ethernet 10/100/1000, 8 portów 1Gbps SFP.
Interfejsy sieciowe systemu zabezpieczeń firewall muszą 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.
Tryb pracy musi być ustalany w konfiguracji interfejsu sieciowego, a system zabezpieczeń firewall musi umożliwiać pracę we wszystkich wymienionych powyżej trybach jednocześnie na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
System zabezpieczeń firewall musi obsługiwać protokół Ethernet z obsługą sieci VLAN poprzez znakowanie zgodne z IEEE 802.1q. Interfejsy sieciowe pracujące w trybie transparentnym, L2 i L3 muszą pozwalać na tworzenie subinterfejsów VLAN. Urządzenie musi obsługiwać 4094 znaczników VLAN.
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.
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).
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).
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.
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.

<p>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.</p>
<p>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 definiowanie aplikacji przez dodatkowe profile). Nie jest dopuszczalna kontrola aplikacji w modułach innych jak firewall (np. w IPS lub innym module UTM).</p>
<p>Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.</p>
<p>Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.</p>
<p>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.</p>
<p>System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.</p>
<p>Wymagania podstawowe identyfikacja użytkowników</p>

<p>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.</p>
<p>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.</p>
<p>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 sesję w przypadku gdy analizowany ruch przechodzi wcześniej przez serwer Proxy ukrywający oryginalne adresy IP zanim dojdzie on do urządzenia.</p>
<p>Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.</p>
<p>Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day</p>
<p>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.</p>
<p>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).</p>
<p>System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.</p>
<p>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.</p>
<p>System zabezpieczeń firewall musi posiadać moduł inspekcji antywirusowej uruchamiany per aplikacja oraz wybrany dekodery taki jak http, smtp, imap, pop3, ftp, smb kontrolującego ruch bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-wirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p>
<p>System zabezpieczeń firewall musi posiadać moduły inspekcji antywirusowej uruchamiany per reguła polityki bezpieczeństwa firewall. Nie jest dopuszczalne, aby moduły inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).</p>
<p>System zabezpieczeń firewall musi posiadać moduły 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 przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p>
<p>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).</p>
<p>System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.</p>
<p>System zabezpieczeń firewall musi posiadać moduł anty-spyware bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-spyware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.</p>

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).
System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
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).
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.
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.
System zabezpieczeń firewall musi umożliwiać zdefiniowanie stron WWW i serwisów do których użytkownicy mogą wysłać swoje poświadczenia. W przypadku próby wysłania poświadczeń do niezaufanej strony lub serwisu ruch musi zostać zablokowany.
System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
System zabezpieczeń firewall musi posiadać możliwość przechwytywania i przesyłania do zewnętrznych systemów typu „Sand-Box” plików różnych typów (exe, dll, pdf, msoffice, java, jpg, swf, apk) przechodzących przez firewall z wydajnością modułu anty-wirus czyli nie mniej niż 600 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.
Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielanie plików, przesyłanych konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".
Administrator musi mieć możliwość konfiguracji rodzaju pliku (exe, dll, pdf, msoffice, java, jpg, swf, apk), użytej aplikacji oraz kierunku przesyłania (wysyłanie, odbieranie, oba) do określenia ruchu poddanego analizie typu „Sand-Box”.
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
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.
System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
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.

<p>System zabezpieczeń firewall musi umożliwiać zestawianie zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Konfiguracja VPN musi odbywać się w oparciu o ustawienia routingu (tzw. routing-based VPN). Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN. Wykorzystanie funkcji VPN (IPSec i SSL) nie wymaga zakupu dodatkowych licencji.</p>
<p>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.</p>
<p>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.</p>
<p>System zabezpieczeń firewall musi pozwalać na budowanie polityk uwierzytelniania definiujący rodzaj i ilość mechanizmów uwierzytelniających (MFA - multi factor authentication) 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.</p>
<p>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.</p>
<p>System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.</p>
<p>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.</p>
<p>Wymagania zarządzanie i raportowanie</p>
<p>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.</p>
<p>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.</p>
<p>System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.</p>
<p>System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.</p>
<p>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).</p>
<p>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.</p>
<p>System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.</p>
<p>System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).</p>
<p>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.</p>

System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
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.
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.
System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
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 łącz sieciowych.
Pomoc techniczna produktu muszą być dostępne w Polsce.