BDG-V.2610.7.2019.PS

Załącznik nr 3 do SIWZ

Szczegółowy Opis Przedmiotu Zamówienia

I. Przedmiot Zamówienia.

Przedmiotem Zamówienia, jest dostawa Systemu Zabezpieczeń typu Next Generation Firewall wraz z wdrożeniem i instruktażem oraz usługami wsparcia technicznego dla Ministerstwa Przedsiębiorczości i Technologii, zwanego dalej „Systemem"
Dostawa i wdrożenie Systemu Zabezpieczeń typu Next Generation Firewall zostanie zrealizowane w terminie do ……. dni od daty podpisania umowy.
Świadczenie usług wsparcia technicznego dla dostarczonego Systemu Zabezpieczeń typu Next Generation Firewall przez okres 12 miesięcy od daty odbioru Systemu.
W ramach realizacji przedmiotu zamówienia zostaną dostarczone urządzenia wraz z niezbędnymi elementami i licencjami oprogramowania składającego się na zaoferowany System Zabezpieczeń typu Next Generation Firewall.
Sprzęt będący przedmiotem niniejszego zamówienia zostanie dostarczony do siedziby Zamawiającego w Warszawie przy Pl. Trzech Krzyży 3/5, w obecności osób wyznaczonych przez Zamawiającego.
Zaoferowany sprzęt musi być fabrycznie nowy, przeznaczony do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz. U. z 2016 r., poz. 655 ze zm.) i z wydanymi na jej podstawie rozporządzeniami), wyprodukowany nie wcześniej niż w 2017 r. oraz objęty wymaganą przez Zamawiającego gwarancją w Polsce. Zamawiający nie dopuszcza produktów ,,odnawianych" (ang. Refurbished).
Zaoferowany sprzęt oraz oprogramowanie nie może być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
Wszystkie elementy dostarczone z urządzeniami, będą pochodziły od jednego producenta. Stosowane elementy muszą być wspierane przez producenta urządzeń i być objęte możliwością analizy potencjalnych błędów w trakcie potencjalnych zgłoszeń serwisowych. Muszą pochodzić z autoryzowanego kanału sprzedaży producentów Urządzeń na rynek polski lub Unii Europejskiej

II. Wymagana, minimalna funkcjonalność i parametry zaoferowanego Systemu Zabezpieczeń typu Next Generation Firewall:

L.p.	Wymagana minimalna funkcjonalność i parametry zaoferowanego Systemu
1	System zabezpieczeń firewall musi być dostarczony w architekturze wysokiej dostępności (klaster HA dwa urządzenia) 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.
2	System zabezpieczeń firewall musi posiadać przepływność w ruchu full-duplex nie mniej niż 6 Gbit/s dla kontroli firewall z włączoną funkcją kontroli aplikacji, nie mniej niż 3 Gbit/s dla kontroli zawartości (w tym kontrola anty-wirus, anty-spyware, IPS i web filtering) i obsługiwać nie mniej niż 2 000 000 jednoczesnych połączeń.
3	System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000, 8 portów 1Gbps/10Gbps SFP/SFP+
4	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.

5	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.).
6	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.
7	System zabezpieczeń firewall musi obsługiwać nie mniej niż 10 wirtualnych routerów posiadających odrębne tabele routingu i umożliwiać uruchomienie więcej niż jedna tablica routingu w pojedynczej instancji systemu zabezpieczeń. Urządzenie musi obsługiwać protokoły routingu dynamicznego, nie mniej niż BGP, RIP i OSPF.
8	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).
9	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).
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.
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.
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 6 Gbit/s.
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).
14	Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
15	Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
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.
17	System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
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.

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.
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.
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.
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.
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.
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.
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.
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.
27	System bezpieczeństwa musi umożliwiać konfiguracje parametrów połączenia – sesji TCP (session timeout) konfigurowane niezależnie dla każdego serwisu (TCP Timeout, Half Closed, Time Wait)
28	System bezpieczeństwa firewall musi umożliwiać eksportowanie konfiguracji wszystkich polityk i funkcji bezpieczeństwa do formatu CSV oraz PDF
39	Oferowany system bezpieczeństwa firewall musi posiadać możliwość integracji z systemem bezpieczeństwa na stacjach końcowych tego samego producenta co pozwoli na ochronę przed zaawansowanymi atkami typu APT w tym zagrożeniami typu *ransomware*
30	Proponowane rozwiązanie powinno plasować się w kwadracie Gartnera w kategorii Next Generation Firewalls przez minimum 4 ostatnie lata
31	Oferowany system bezpieczeństwa firewall musi dostarczać funkcjonalność ochrony poświadczeń użytkownika i umożliwiać monitorowanie i blokowanie wpisywanych wewnętrznych poświadczeń (np. z MS AD) na zewnętrzne serwisy Webowe

32	System bezpieczeństwa musi natywnie wspierać integrację z urządzeniami HP/Aruba oraz wspierać technologię Clearpass. W szczególności, proponowane rozwiązanie musi potrafić wymieniać z siecią HP informacje takie jak: Source IP, USername, User Role, Device type, domain name, machine name, machine OS

L.p.	Wymagania podstawowe identyfikacji użytkowników
1	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.
2	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.
3	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.
4	Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

L.p.	Wymagania ochrony IPS, AV, anty-spyware, URL, zero-day
1	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.
2	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).
3	System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
4	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.
5	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.
6	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).

7	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.
8	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).
9	System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
10	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.
11	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).
12	System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
13	System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
14	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).
15	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.
16	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.
17	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.
18	System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
19	System zabezpieczeń firewall musi zapewniać 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 3 Gbit/s w celu ochrony przed zagrożeniami typu zero-day. Systemy zewnętrzne, na podstawie przeprowadzonej analizy, muszą aktualizować system firewall sygnaturami nowo wykrytych złośliwych plików i ewentualnej komunikacji zwrotnej generowanej przez złośliwy plik po zainstalowaniu na komputerze końcowym.
20	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".

21	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”.
22	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.
23	System bezpieczeństwa firewall musi umożliwiać dodawanie zewnętrznych listy dostępu typu adresy IP, lista domen oraz list URL. Listy te pobierane co 5 minut z zewnętrznego serwera dostępnego po protokole http, https z kontrolą certyfikatu

L.p.	Wymagania dodatkowe NAT, DoS, IPSEC VPN, SSL VPN, QoS
1	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.
2	System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.
3	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.
4	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.
5	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.
6	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.
7	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.
8	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.
9	System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.
10	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.

11	System bezpieczeństwa firewall musi dostarczać funkcję tzw. Offloading SSL pracującą w trybie Layer3 i Transparent umożliwiającą przekierowanie ruchu rozszyfrowanego do innego rozwiązania bezpieczeństwa, które pracując w trybie prewencji zatrzymuje zagrożenia. Dopuszcza się zastosowanie zewnętrznego, dodatkowego rozwiązania umożliwiającego spełnienie tego wymagania
12	Proponowane rozwiązanie VPN w ramach dostarczanego sprzętu musi umożliwiać obsługę nielimitowanej ilości oprogramowania. Jedynym dopuszczalnym limitem może być wydajność samej platformy.

Wymagania dodatkowe środowisko wirtualne vmware
System zabezpieczeń firewall musi pozwalać na integrację w środowisku wirtualnym VMware w taki sposób, aby firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa firewalla.

L.p.	**Wymagania dotyczące zarządzania i raportowania**
1	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.
2	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.
3	System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.
4	System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.
5	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).
6	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.
7	System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
8	System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
9	System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 240 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
10	System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.

11	System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
12	System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
13	System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
14	System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
15	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.
16	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.
17	System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
18	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.
19	Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym.

L.p.	Wymagania podstawowe systemu zarządzania
1	System zarządzania, logowania i raportowania musi obsługiwać 25 firewalli.
2	System zarządzania, logowania i raportowania musi zapewniać przestrzeń dyskową o pojemności nie mniejszej niż 2 TB.
3	System zarządzania, logowania i raportowania musi umożliwiać dodanie dodatkowej przestrzeni dyskowej przeznaczonej na logowanie.
4	System zarządzania, logowania i raportowania musi posiadać taki sam Graficzny Interfejs Użytkownika jak zarządzane firewalle.
5	System zarządzania, logowania i raportowania musi umożliwiać import obecnej konfiguracji używanych firewalli.
6	System zarządzania, logowania i raportowania musi umożliwiać zbieranie logów zdarzeń z systemów firewall. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW.
7	System zarządzania, logowania i raportowania musi umożliwiać korelację logów zdarzeń z zarządzanych firewalli.
8	System zarządzania, logowania i raportowania musi umożliwiać łatwe przeszukiwanie skorelowanych logów zebranych z zarządzanych firewalli.
9	System zarządzania, logowania i raportowania musi umożliwiać tworzenie, zapisywanie i ponowne wykorzystywanie filtrów służących do wyszukiwania informacji w zebranych danych.

10	System zarządzania, logowania i raportowania musi umożliwiać tworzenie statycznych raportów dopasowanych do wymagań Zamawiającego. Musi istnieć możliwość zapisania stworzonych raportów i uruchamianie ich w sposób ręczny lub automatyczny w określonych przedziałach czasu oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób.
11	System zarządzania, logowania i raportowania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) dopasowanych do wymagań Zamawiającego z funkcjonalnością „drill-down”.
12	System zarządzania, logowania i raportowania musi umożliwiać centralne budowanie i dystrybucję polityk bezpieczeństwa o różnym zasięgu. Lokalnych (dla wybranych firewalli lub logicznych systemów firewalla) i globalnych (dla grup firewalli lub kilku systemów logicznych wybranych firewalli).
13	System zarządzania, logowania i raportowania musi umożliwiać grupowanie firewalli i systemów z poszczególnych firewalli w logiczne kontenery umożliwiające wspólne zarządzanie (konfigurowanie polityk bezpieczeństwa, konfigurowanie ustawień sieciowych, wykorzystanie tych samych obiektów).
14	System zarządzania, logowania i raportowania musi umożliwiać tworzenie raportów na podstawie zbudowanych kontenerów.
15	System zarządzania, logowania i raportowania musi umożliwiać przechowywanie i zarządzanie obiektami używanymi przez wszystkie firewalle w jednym, centralnym repozytorium.
16	System zarządzania, logowania i raportowania musi umożliwiać odseparowanie konfiguracji urządzeń i ich ustawień sieciowych od konfiguracji reguł bezpieczeństwa i obiektów w nich użytych.
17	System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych sygnatur.
18	System zarządzania, logowania i raportowania musi umożliwiać dystrybucję i zdalną instalację nowych wersji systemu oraz poprawek.
19	System zarządzania, logowania i raportowania musi umożliwiać tworzenie kopii zapasowych zarządzanych firewalli.
20	System zarządzania, logowania i raportowania musi pozwalać na przełączenie się w kontekst pojedynczego firewalla lub logicznego systemu na firewallu z poziomu konsoli zarządzającej.
21	System zarządzania, logowania i raportowania musi umożliwiać dzielenie obiektów pomiędzy firewallami i systemami logicznymi.
22	System zarządzania, logowania i raportowania musi umożliwiać tworzenie obiektów o różnym zasięgu (lokalne, globalne).
23	System zarządzania, logowania i raportowania musi umożliwiać tworzenie i używanie ról administracyjnych różniących się poziomem dostępu do danego urządzenia lub grupy urządzeń/logicznych systemów.
24	System zarządzania, logowania i raportowania musi informować o zmianach konfiguracji systemu.
25	System zarządzania, logowania i raportowania musi umożliwiać audytowanie/sprawdzanie poprawności konfiguracji urządzenia/logicznego systemu przed jej zatwierdzeniem.
26	System zarządzania, logowania i raportowania musi umożliwiać zapisywanie różnych wersji konfiguracji zarządzanych firewalli/logicznych systemów.
27	System zarządzania, logowania i raportowania musi umożliwiać wykonanie procedury wymiany uszkodzonego urządzenia na nowe tak aby System zarządzania, logowania i raportowania zrozumiał iż nowe urządzenie zastępuje urządzenie uszkodzone.

28	System zarządzania, logowania i raportowania musi być dostarczony jako maszyna wirtualna.
29	System zarządzania musi posiadać możliwość pracy w konfiguracji odpornej na awarie w trybie Active-Passive.
30	Proponowane rozwiązanie do centralnego zarządzania farmą firewalli nie może być w żaden sposób limitowane, jeśli chodzi o ilość danych. Może je jedynie ograniczać ilość zasobów dyskowych dedykowanych pod to rozwiązanie.

III. Dostawa i wdrożenie Systemu Zabezpieczeń typu Next Generation Firewall

W ramach dostawy i wdrożenia Systemu Wykonawca zrealizuje:

1. Dostawę fabrycznie nowych urządzeń wolnych od wad oraz pochodzących z oficjalnego kanału sprzedaży producenta na rynek polski lub Unii Europejskiej.
2. Wykonanie analizy przedwdrożeniowej, zaprojektowanie Systemu, utworzenie i przekazanie dokumentu (w języku polskim) – Projekt techniczny zawierającego co najmniej:
   a) architekturę rozwiązania,
   b) opis konfiguracji wstępnej i polityki bezpieczeństwa,
   c) opis konfiguracji mechanizmów bezpieczeństwa,
   d) testy akceptacyjne systemu bezpieczeństwa
3. Instalację i konfigurację Systemu zgodnie z projektem technicznym w zakresie:
   a) Montażu dostarczonych urządzeń w środowisku Zamawiającego,
   b) Instalacji i konfiguracji Systemu,
   c) Wykonanie testów akceptacyjnych.
4. Opracowanie i dostarczenie dokumentacji powdrożeniowej zawierającej w swojej treści co najmniej:
   a) Procedury i instrukcje dotyczące instalacji konfiguracji oraz parametryzacji wdrożonego Systemu,
   b) Procedury i instrukcje wykonania kopii bezpieczeństwa i ich odtworzenia,
   c) Procedury i instrukcje aktualizacji i wdrażania poprawek,
   d) Procedury postępowania w razie wystąpienia błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,

   Dokumentacja musi być dostarczona przed produkcyjnym uruchomieniem Systemu. Dokumentacja będzie podlegała akceptacji ze strony Zamawiającego.
5. Po wdrożeniu Systemu Wykonawca zobowiązany będzie do przeprowadzenia instruktażu na następujących zasadach:
   a) Instruktaż zostanie przeprowadzony na rzecz Zamawiającego dla minimum 4 pracowników, w wymiarze minimum 2 dni roboczych po 6 godzin zajęć efektywnych dziennie;
   b) Dokładny termin zostanie uzgodniony z Zamawiającym z co najmniej 3 dniowym wyprzedzeniem,
   c) Instruktaż zostanie przeprowadzony w siedzibie Zamawiającego,
   d) Wykonawca zapewni przeprowadzenie instruktażu przez kadrę wykwalifikowaną, posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu zamówienia, (wymagane posiadanie certyfikatu z oferowanej technologii przez inżyniera przeprowadzającego instruktaż),
   e) Przed ustalonym terminem instruktażu Wykonawca prześle Zamawiającemu zakres tematyczny/programu instruktażu. Zamawiający będzie miał prawo do weryfikacji zakresu tematycznego/programu instruktażu i zgłoszenia ew. dodatkowego zakresu tematycznego,
   f) Instruktaż swoją tematyką będzie obejmował co najmniej:
      – instalację dostarczonego Systemu,
      – konfigurację podstawowych funkcjonalności,
      – weryfikację ruchu (wykrywanie sytuacji niepożądanych),
      – tworzenie własnych sygnatur,
      – zarządzanie uprawnieniami,

- backup i odtworzenie konfiguracji.

6. Usługi wsparcia technicznego
   - Przedmiot zamówienia objęty będzie 12 miesięczną usługą wsparcia technicznego świadczoną w miejscu użytkowania Systemu,
   - W trakcie 12 miesięcy w ramach usługi wsparcia technicznego, Zamawiający będzie uprawniony do pobierania nowych wersji oprogramowania które zostanie zaoferowane w ramach Zamówienia,
   - Usługa wsparcia technicznego zapewni minimum:
     a) udzielanie odpowiedzi na podstawowe pytania dotyczące instalacji, używania i konfiguracji;
     b) bezpośrednie konsultacje telefoniczne z inżynierem producenta dotyczące bieżących problemów związanych z Oprogramowaniem i Systemem;
     c) analizę informacji diagnostycznych mającą na celu określenie przyczyny problemu, np. pomoc w interpretacji dokumentacji problemów związanych z instalacją lub kodem,
     d) w przypadku znanych defektów oprogramowania, przekazywanie informacji o sposobie ich usunięcia lub obejścia, a także udzielanie pomocy w uzyskaniu poprawek, do otrzymania których Zamawiający jest uprawniony w ramach posiadanej licencji,
     e) dostęp do telefonicznego wsparcia technicznego producenta oprogramowania w czasie podstawowego okresu dostępności centrum wsparcia dla systemu (w dni robocze w godzinach 8:00 - 17:00),
     f) naprawy błędu lub usunięcia zgłoszonej awarii Systemu, w ciągu 4 godzin od momentu zgłoszenia w przypadku awarii Systemu powodującej brak jego dostępności,
     g) naprawy błędu lub usunięcia zgłoszonej awarii Systemu , w ciągu 24 godzin od momentu zgłoszenia w przypadku pozostałych zgłoszeń,
     h) nieprzerwany i nieograniczony dostęp do zasobów elektronicznych, baz samopomocy, FAQ, baz wiedzy producenta oprogramowania.