OPIS PRZEDMIOTU ZAMÓWIENIA

I. NAZWA ZAMÓWIENIA

Dostawa i wdrożenie systemu zapór sieciowych wewnętrznych (tzw. firewall) wraz z usługą szkolenia.

II. DEFINICJE:

System informatyczny – system informatyczny rozumiany jako w pełni działające środowisko u Zamawiającego, w skład którego wchodzi Sprzęt teleinformatyczny, Infrastruktura teleinformatyczna, konfiguracja aplikacyjna, bazodanowa i sieciowa oraz działające w tych środowiskach oprogramowanie komputerowe;

Sprzęt teleinformatyczny – sprzęt telekomunikacyjny i informatyczny rozumiany jako wszelkie urządzenia służące do prawidłowego działania Systemu informatycznego Zamawiającego np. urządzenia sieciowe, urządzenia bezpieczeństwa teleinformatycznego, urządzenia transmisji głosu i wideo, macierze, biblioteki taśmowe, urządzenia służące do tworzenia i przechowywania kopii zapasowych danych oraz pozostałe urządzenia szeroko rozumianego sprzętu komputerowego;

System – Sprzęt oraz oprogramowanie zainstalowane, skonfigurowane oraz wdrożone przez Wykonawcę dla Zamawiającego, zgodnie z przygotowanym przez Wykonawcę i zatwierdzonym przez Zamawiającego Projektem Technicznym składający się na przedmiot zamówienia.

Dokumentacja - wszelka dokumentacja stworzona przez Wykonawcę na potrzeby realizacji zamówienia, w tym Projekt Techniczny oraz Dokumentacja Powykonawcza opisująca instalację oraz konfigurację Systemu, procedury operacyjne i eksploatacyjne Systemu;

Infrastruktura teleinformatyczna – infrastruktura sprzętowa posiadana i aktualnie użytkowana przez Zamawiającego rozumiana jako aktywne i pasywne urządzenia sieciowe, elementy okablowania strukturalnego budynku, elementy infrastruktury bezpieczeństwa (zapory sieciowe, IPS, urządzenia do szyfrowania transmisji danych itp.) oraz pozostałe urządzenia pracujące w sieci Zamawiającego;

Projekt Techniczny – część Dokumentacji, zawierający szczegółowy opis wdrażanego Systemu. W szczególności powinna zawierać architekturę techniczną, logiczną i funkcjonalną Systemu z opisem zastosowanych rozwiązań. Powinien uwzględniać i uwydatniać zastosowane licencje i urządzenia, warstwy logiczne, sieciowe i funkcjonalne oraz zawierać dobre praktyki budowy tego typu rozwiązań z uwzględnieniem bezpieczeństwa danych, monitoringu oraz ciągłości działania. Projekt Techniczny jest przedkładany Zamawiającemu do zatwierdzenia;

Dokumentacja Powykonawcza – część Dokumentacji zawierająca szczegółowy opis wykonanych lub wykonywanych czynności instalacyjnych oraz konfiguracyjnych wszystkich komponentów Systemu, zawierająca procedury operacyjne i eksploatacyjne;

Lokalizacja Zapasowa – pomieszczenie zlokalizowane w budynku znajdującym się pod adresem ul. Świętokrzyska 11/21, 00-049 Warszawa.

III. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest zrealizowanie przez Wykonawcę dostawy i wdrożenia do Systemu informatycznego Zamawiającego Systemu, tj. systemu wewnętrznych zapór sieciowych wraz z dodatkami zbudowany jako redundantny układ dwóch urządzeń typu firewall pracujących w trybie klastra niezawodnościowego (tzw. tryb HA – High Availability, active-passive), dostawy i konfiguracji subskrypcji/ licencji sygnatur ataków/ IPS/zagrożeń/antywirusowych wraz z usługą szkolenia oraz dostarczeniem Dokumentacji Powykonawczej.

   Dostawa sprzętu i subskrypcji/licencji na użytkowanie wdrażanego Systemu zostanie dokonana do siedziby Zamawiającego, tj. na adres ul. ks. Ignacego Jana Skorupki 4, 00-546 Warszawa.

   Wdrożenie Systemu zostanie wykonane w siedzibie Zamawiającego i Lokalizacji Zapasowej.

   Zamawiający wymaga aby wdrożony System posiadał możliwość filtracji URL oraz posiadał funkcje Sandbox. Dostawa Systemu nie obejmuje dostawy licencji/subskrypcji na wskazane funkcje tj. filtrowanie URL i Sandbox.

2. W ramach dostawy i wdrożenia Systemu Wykonawca zrealizuje dostawę i wdrożenie 8 wkładek 10Gbase-SR zgodnych z Systemem. Wkładki nie mogą w jakikolwiek sposób negatywnie wpływać na prawidłową pracę Systemu oraz warunki gwarancji na System. Wkładki składają się na System. Wykonawca zobowiązany jest do zapewnienia prawidłowego działania wdrożonego Systemu jako całości w Systemie informatycznym Zamawiającego, jak również każdego z elementów wdrożonego Sytemu oraz zobowiązany jest do zapewnienia gwarancji na cały System oraz na każdy z elementów wdrożonego Sytemu.

3. W ramach przedmiotu zamówienia zostanie:

   a. udzielona minimum 36-miesięczna gwarancja na dostarczony oraz wdrożony System – liczona od dnia podpisania przez obie strony bez zastrzeżeń protokołu odbioru końcowego przedmiotu zamówienia oraz

   b. zapewnione minimum 36-miesięczne wsparcie techniczne i subskrypcja - od dnia podpisania bez zastrzeżeń przez obydwie strony protokołu odbioru końcowego przedmiotu zamówienia.

4. Tryb świadczenia gwarancji:

   a. dostępność serwisu w okresie gwarancji – 24 godziny na dobę przez 7 dni w tygodniu,

   b. zgłoszenia będą przyjmowane przez Wykonawcę telefonicznie lub na adres mailowy.

   c. czas naprawy (przywrócenie stanu funkcjonowania systemu sprzed awarii) – następny dzień roboczy następujący po dniu zgłoszenia (Next Business Day - NBD),

   d. serwis w okresie gwarancji musi być świadczony w miejscu wdrożenia systemu firewall, czyli w siedzibie Zamawiającego oraz Lokalizacji Zapasowej.

   e. usunięcie uszkodzenia nienaprawialnego nastąpi w terminie wskazanym w lit. c, poprzez wymianę na sprzęt sprawny o co najmniej takich samych walorach funkcjonalnych,

f. zapewniona naprawa lub wymiana urządzeń lub ich części na części nowe i oryginalne, zgodnie z metodyką z zaleceniami producenta sprzętu.

g. wymienione urządzenia lub elementy muszą być objęte takim samym zakresem usług serwisowych jakim objęte były urządzenia i elementy, które zostały wymienione.

h. wykonawca usługi gwarancyjnej ponosi wszystkie koszty napraw gwarancyjnych, włączając w to koszty części i transportu.

5. Wsparcie techniczne:

   a. powinno być świadczone przez producenta lub jego autoryzowanego polskiego przedstawiciela,
   b. będzie świadczone telefonicznie oraz drogą elektroniczną,
   c. obejmuje: dostęp do nowych wersji oprogramowania, aktualizację bazy aplikacji, sygnatur ataków IPS, definicji wirusów, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. Wsparcie techniczne dla oprogramowania rozumiane jest jako gotowość przystąpienia do rozwiązywania problemów technicznych związanych z oprogramowaniem systemu firewall w trybie 8 godzin na dobę, 5 dni roboczych w tygodniu

6. Termin realizacji zamówienia:

   Termin realizacji zamówienia wynosi, w zakresie:

   a. dostawy i wdrożenia Systemu oraz dostawy i konfiguracji subskrypcji/licencji sygnatur ataków/IPS/zagrożeń/antywirusowe, usługi szkolenia, dostarczenia Dokumentacji Powykonawczej – nie dłużej niż 8 tygodni liczonych od dnia zawarcia umowy,
   b. gwarancji oraz wsparcia technicznego – 36 miesięcy licząc od dnia podpisania protokołu odbioru końcowego przedmiotu zamówienia.

IV. WYMAGANIA W ZAKRESIE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Wszystkie elementy składowe dostarczonych urządzeń muszą być fabrycznie nowe, oryginalnie zapakowane i pochodzić z autoryzowanego źródła przeznaczonego do dystrybucji na terytorium Rzeczpospolitej Polskiej oraz wolne od wszelkich wad fizycznych i prawnych.
2. System musi współpracować z istniejącą infrastrukturą Zamawiającego, w szczególności z firewallami PaloAlto (PA-3020) oraz (PA-220).
3. Wykonawca dostarczy niezbędne elementy montażowe i połączeniowe do infrastruktury Zamawiającego.
4. Dostarczone urządzenia nie mogą być wyprodukowane przed dniem 1 czerwca 2018 roku.
5. Sprzęt teleinformatyczny musi być wyposażony w aktualną wspieraną wersję oprogramowania wewnętrznego (firmware), dostępną w dniu dostawy do Zamawiającego.

V. OPIS TECHNICZNY I WYMAGANIA FUNKCJONALNE PRZEDMIOTU ZAMÓWIENIA

1. WYMAGANIA PODSTAWOWE

1.1. System zabezpieczeń firewall musi być dostarczony jako specjalizowane urządzenia zabezpieczeń sieciowych (appliance). W architekturze systemu musi występować separacja

modułu zarządzania i modułu przetwarzania danych. Całość Systemu musi być dostarczona i wspierana przez jednego producenta.

1.2. 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.

1.3. System zabezpieczeń firewall musi być wyposażony w co najmniej 12 portów Ethernet 10/100/1000, 8 portów 1Gbps/10Gbps SFP/SFP+ oraz 8 wkładek 10Gbase-SR.

1.4. Interfejsy sieciowe systemu zabezpieczeń firewall muszą działać w trybie routera (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.

1.5. System zabezpieczeń firewall musi obsługiwać terminację tuneli GRE.

1.6. 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.).

1.7. 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.

1.8. 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.

1.9. 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).

1.10. 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).

1.11. 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.

1.12. 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.

1.13. 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.

1.14. 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).

1.15. Nie jest dopuszczalne, aby blokowanie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż firewall.
1.16. Nie jest dopuszczalne rozwiązanie, gdzie kontrola aplikacji wykorzystuje moduł IPS, sygnatury IPS ani dekodery protokołu IPS.
1.17. System zabezpieczeń firewall musi wykrywać co najmniej 1700 różnych aplikacji (takich jak Skype, Tor, BitTorrent, eMule, UltraSurf itp.) wraz z aplikacjami tunelującymi się w HTTP lub HTTPS. System zabezpieczeń musi obsługiwać inspekcję protokołu http/1.x oraz http/2.0.
1.18. System zabezpieczeń firewall musi wykonywać inspekcję danych przesyłanych wewnątrz tuneli VXLAN.
1.19. System zabezpieczeń firewall musi pozwalać na ręczne tworzenie sygnatur dla nowych aplikacji bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
1.20. 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.
1.21. 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.
1.22. 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.
1.23. 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.
1.24. 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.
1.25. 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.

1.26. 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.
1.27. System zabezpieczeń musi posiadać 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.
1.28. System zabezpieczeń firewall musi zapewniać inspekcję szyfrowanej komunikacji SSH (Secure Shell) dla ruchu wychodzącego w celu wykrywania tunelowania innych protokołów w ramach usługi SSH.

2. WYMAGANIA PODSTAWOWE IDENTYFIKACJA UŻYTKOWNIKÓW

2.1. 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.

2.2. System zabezpieczeń firewall musi posiadać możliwość zbierania i analizowania informacji Syslog z urządzeń sieciowych i systemów MS Windows oraz 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.

2.3. 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.
2.4. Po odczytaniu zawartości pola XFF z nagłówka http system zabezpieczeń musi usunąć odczytany źródłowy adres IP przed wysłaniem pakietu do sieci docelowej.

3. WYMAGANIA OCHRONY IPS, AV, ANTY-SPYWARE, URL, ZERO-DAY

3.1. 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.
3.2. 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).

3.3. System zabezpieczeń firewall musi zapewniać możliwość wykorzystania kategorii URL jako elementu klasyfikującego (nie tylko filtrującego) ruch w politykach bezpieczeństwa.
3.4. 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.
3.5. 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.
3.6. 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).
3.7. 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.
3.8. 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).
3.9. System zabezpieczeń firewall musi zapewniać możliwość ręcznego tworzenia sygnatur IPS bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
3.10. 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.
3.11. 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).
3.12. System zabezpieczeń firewall musi posiadać możliwość ręcznego tworzenia sygnatur anty-spyware bezpośrednio na urządzeniu bez użycia zewnętrznych narzędzi i wsparcia producenta.
3.13. System zabezpieczeń firewall musi posiadać sygnatury DNS wykrywające i blokujące ruch do domen uznanych za złośliwe.
3.14. 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).
3.15. 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.

3.16. 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.

3.17. 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.

3.18. System zabezpieczeń firewall musi posiadać funkcję wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.

3.19. 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.

3.20. Integracja z zewnętrznymi systemami typu "Sand-Box" musi pozwalać administratorowi na podjęcie decyzji i rozdzielenie plików, przesyłanych pomiędzy konkretnymi aplikacjami, pomiędzy publicznym i prywatnym systemem typu "Sand-Box".

3.21. 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".

3.22. 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.

4. WYMAGANIA DODATKOWE NAT, DOS, IPSEC VPN, SSL VPN, QOS

4.1. 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.

4.2. System zabezpieczeń firewall musi posiadać osobny zestaw polityk definiujący reguły translacji adresów NAT rozdzielny od polityk bezpieczeństwa.

4.3. 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.

4.4. 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 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.

4.5. 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.

4.6. 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.

4.7. 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.

4.8. System musi mieć możliwość kształtowania ruchu sieciowego (QoS) dla poszczególnych użytkowników.

4.9. 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.

5. WYMAGANIA DODATKOWE ŚRODOWISKO WIRTUALNE VMWARE

5.1. 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.

6. WYMAGANIA ZARZĄDZANIE I RAPORTOWANIE

6.1. 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.

6.2. 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.

6.3. System zabezpieczeń firewall musi umożliwiać edytowanie konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian których są autorami.

6.4. System zabezpieczeń firewall musi pozwalać na blokowanie wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji.

6.5. 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).
6.6. 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.
6.7. System zabezpieczeń firewall musi umożliwiać uwierzytelnianie administratorów za pomocą bazy lokalnej, serwera LDAP, RADIUS, TACACS+ i Kerberos.
6.8. System zabezpieczeń firewall musi umożliwiać stworzenie sekwencji uwierzytelniającej posiadającej co najmniej trzy metody uwierzytelniania (np. baza lokalna, LDAP i RADIUS).
6.9. 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.
6.10. System zabezpieczeń firewall musi pozwalać na usuwanie logów i raportów przetrzymywanych na urządzeniu po upływie określonego czasu.
6.11. System zabezpieczeń firewall musi umożliwiać sprawdzenie wpływu nowo pobranych aktualizacji sygnatur (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa.
6.12. System zabezpieczeń firewall musi pozwalać na konfigurowanie i wysyłanie logów do różnych serwerów Syslog per polityka bezpieczeństwa.
6.13. System zabezpieczeń firewall musi pozwalać na selektywne wysyłanie logów bazując na ich atrybutach.
6.14. System zabezpieczeń firewall musi pozwalać na generowanie zapytań do zewnętrznych systemów z wykorzystaniem protokołu HTTP/HTTPS w odpowiedzi na zdarzenie zapisane w logach urządzenia.
6.15. 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.
6.16. System zabezpieczeń firewall musi 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.
6.17. System zabezpieczeń firewall pozwalać na stworzenie raportu o aktywności wybranego użytkownika lub grupy użytkowników na przestrzeni kilku ostatnich dni.
6.18. 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.

VI. WDROŻENIE SYSTEMU

W zakresie wdrożenia Wykonawca zobowiązany jest do wykonania, w szczególności:

a. analizy (na podstawie informacji uzyskanych od Zamawiającego), w terminie 7 dni od dnia zawarcia umowy, której celem będzie opracowanie Projektu Technicznego z harmonogramem wdrożenia, zawierającego m. in. architekturę logiczną i fizyczną, architekturę logiczną,

komunikacyjną i innymi systemami i zaporami typu firewall stosowanymi u Zamawiającego, konfiguracje urządzeń, dostępy, protokoły i reguły konfiguracji systemu zapór sieciowych (ok. 50 reguł). Rozwiązanie musi zawierać mechanizmy niezawodnościowe w przypadku awarii pojedynczego urządzenia.

b. dostawy oraz montażu urządzeń i wszelkich komponentów sprzętowych systemu zapór sieciowych
   w szafach serwerowych w siedzibie Zamawiającego oraz Lokalizacji Zapasowej;
c. uruchomienia i konfiguracji systemu zapór sieciowych zgodnie z zatwierdzonym przez Zamawiającego Projektem Technicznym.
d. przeprowadzenia szkoleń zgodnie z wymaganiami określonymi w rozdziale VII.
e. Sporządzenia oraz dostarczenie Zamawiającemu Dokumentacji Powykonawczej.

VII. SZKOLENIA

Wykonawca zapewni szkolenia obejmujące zagadnienia związane z konfiguracją i zarządzaniem Systemem zapór sieciowych. Szkolenie będzie składało się z części teoretycznej oraz części praktycznej na środowisku szkoleniowym przygotowanym przez Wykonawcę. Szkolenie zostanie przeprowadzone dla 2 osób. Szkolenie będzie trwało minimum 40 godzin (5 dni roboczych), oraz będzie odbywało się w dni robocze od poniedziałku do piątku po min 8 godzin dziennie przez 5 następujących po sobie dni.

Szkolenia muszą być przeprowadzone w Warszawie. Usługi te muszą być świadczone w języku polskim w autoryzowanym ośrodku edukacyjnym

Szkolenie obejmie m.in. następującą tematykę:

1. Omówienie architektury firewalli;
2. Podstawową konfigurację urządzenia;
3. Konfigurację interfejsów sieciowych;
4. Polityki bezpieczeństwa;
5. Translacja NAT/PAT;
6. Mechanizmy ochrony antywirusowej, IPS, anty-spyware;
7. Filtrowanie URL;
8. Deszyfracja ruchu szyfrowanego SSL;
9. Sandbox;
10. Identyfikacja użytkowników;
11. Identyfikacja aplikacji
12. VPN – dostęp zdalny z komputerów, urządzeń mobilnych;
13. VPN – weryfikacja klientów wg wzorców zgodności;
14. VPN – site-to-site; IPsec
15. Klastry active-active, active-passive;
16. Obsługa przez CLI;
17. Integracja z AD, LDAP i inne
18. Monitorowanie firewalli;
19. Diagnostyka i rozwiązywanie problemów dla powyższych punktów;
20. Zrzuty ruchu sieciowego;
21. Logi diagnostyczne, konfiguracja;

VIII. DOKUMENTACJA POWYKONAWCZA, ODBIÓR KOŃCOWY WDROŻONEGO SYSTEMU

1. Po zakończeniu wdrożenia oraz przeprowadzenia szkolenia Wykonawca sporządzi i dostarczy Zamawiającemu 2 egzemplarze Dokumentacji Powykonawczej w wersji papierowej (2 egzemplarze) oraz elektronicznej (w formatach .doc i .pdf).

   Dokumentacja powykonawcza powinna zawierać, w szczególności zawierać architekturę logiczną, fizyczną, komunikacyjna oraz integracyjną z Systemami informatycznymi Zamawiającego, konfigurację szczegółową poszczególnych elementów, wykaz i szczegółową konfigurację zaimplementowanych polityk bezpieczeństwa, opis i szczegółową konfigurację zastosowanych zabezpieczeń typu IPS, antywirus oraz konfiguracje i adresacje interfejsów.
   Dokumentacja Powykonawcza powinna opisywać procedury eksploatacji/administracji, archiwizacji, odtworzenia, monitorowania oraz postępowania w przypadku wystąpienia awarii Systemu. Dodatkowo część opisowa powinna zawierać schemat graficzny architektury nowych/modyfikowanych elementów architektury sieci. Dokumentacja Powykonawcza będzie podlegała odbiorowi przez Zamawiającego.

2. Udokumentowanie wdrożenia nastąpi przez podpisanie dokumentu protokół odbioru końcowego przedmiotu zamówienia zgodnie z wymaganiami określonymi w umowie.