Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej Wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Wymagana jest możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

I. Firewall.
II. Ochrony w warstwie aplikacji.
III. Protokołów routingu dynamicznego.

2. Redundancja, monitoring i wykrywanie awarii

2.1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – wymagana jest możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach wymagana jest funkcja synchronizacji sesji firewall.
2.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2.3. Monitoring stanu realizowanych połączeń VPN.
2.4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Wymagana jest możliwość tworzenia interfejsów redundantnych.

3. Interfejsy, Dysk, Zasilanie:

3.1. System realizujący funkcję Firewall musi dysponować minimum:
a) 8 portami Gigabit Ethernet RJ-45.
b) 8 gniazdami SFP 1 Gbps.
c) 2 gniazdami SFP+ 10 Gbps.

3.2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3.3. W ramach systemu Firewall wymagana jest możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

3.4. System musi umożliwiać w przyszłości rozbudowę o redundantny zasilacz hot-swap.

4. Parametry wydajnościowe:

4.1. W zakresie Firewall'a obsługa nie mniej niż 7 mln. jednoczesnych połączeń oraz 400 tys. nowych połączeń na sekundę.

4.2. Przepustowość Stateful Firewall: nie mniej niż 35 Gbps dla pakietów 512 B.

4.3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 13 Gbps.

4.4. Wydajność szyfrowania IPSec VPN nie mniej niż 15 Gbps.

4.5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 9 Gbps.

4.6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps.

4.7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7 Gbps.

5. Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

5.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

5.2. Kontrola Aplikacji.

5.3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.

5.4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.

5.5. Ochrona przed atakami - Intrusion Prevention System.

5.6. Kontrola stron WWW.

5.7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.

5.8. Zarządzanie pasmem (QoS, Traffic shaping).

5.9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).

5.10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania Zamawiający wymaga dostarczenia co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

5.11. Analiza ruchu szyfrowanego protokołem SSL.

5.12. Analiza ruchu szyfrowanego protokołem SSH.

6. Polityki, Firewall

6.1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

6.2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

a) Translację jeden do jeden oraz jeden do wielu.
b) Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

6.3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

6.4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

a) Amazon Web Services (AWS).
b) Microsoft Azure
c) Cisco ACI.
d) Google Cloud Platform (GCP).
e) OpenStack.
f) VMware vCenter (ESXi).

7. Połączenia VPN

7.1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

a) Wsparcie dla IKE v1 oraz v2.
b) Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
c) Obsługa protokołu Diffie-Hellman grup 19 i 20.
d) Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
e) Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
f) Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
g) Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
h) Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
i) Mechanizm „Split tunneling” dla połączeń Client-to-Site.

7.2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

a) Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.

b) Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
c) Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

8. Routing i obsługa łączy WAN

W zakresie routingu rozwiązanie musi zapewniać obsługę:

a) Routingu statycznego.
b) Policy Based Routingu.
c) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

9. Zarządzanie pasmem

9.1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnego możliwego i minimalnego gwarantowanego pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

9.2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

9.3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

10. Ochrona przed malware

10.1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).

10.2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

10.3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).

10.4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

10.5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

11. Ochrona przed atakami

11.1. Ochrona IPS musi opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.

11.2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.

11.3. Baza sygnatur ataków musi zawierać minimum 4500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

11.4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.

11.5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.

11.6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

11.7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

12. Kontrola aplikacji

12.1. Funkcja Kontroli Aplikacji musi umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.

12.2. Baza Kontroli Aplikacji musi zawierać minimum 1900 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

12.3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) muszą być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

12.4. Baza musi zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.

12.5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

13. Kontrola WWW

13.1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

13.2. W ramach filtra www muszą być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.

13.3. Filtr musi mieć możliwość blokowania stron typu Hazard wg własnej bazy danych (nie ręcznie wprowadzanych).

13.4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

13.5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

13.6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

13.7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

14. Uwierzytelnianie użytkowników w ramach sesji

14.1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

a) Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
b) Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
c) Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

14.2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

14.3. Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

15. Zarządzanie

15.1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i musi mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

15.2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

15.3. Musi istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

15.4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

15.5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

15.6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

15.7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

16. Logowanie

16.1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

16.2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

16.3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

16.4. Musi istnieć możliwość logowania do serwera SYSLOG.

17. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać ICSA lub EAL4 lub równoważne dla funkcji Firewall.

18. Serwisy i licencje

W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Muszą one obejmować: kontrolę aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

19. Gwarancja oraz wsparcie

19.1. System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

19.2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim w trybie 8x5 (od poniedziałku do piątku w godzinach pracy Zamawiającego tj. 9-17). W tym celu Wykonawca zobowiązany jest zapewnić świadczenie usług przez co najmniej dwóch inżynierów z aktualnym certyfikatem technicznym oferowanego rozwiązania (jeżeli producent oferuje stopniowy system certyfikacji to co najmniej jedna z tych osób musi posiadać najwyższy dostępny stopień).

20. Wdrożenie

W ramach dostawy Wykonawca musi przeprowadzić wdrożenie dostarczonego systemu. Wdrożenie musi być wykonane przez inżyniera z aktualnym certyfikatem technicznym oferowanego rozwiązania (jeżeli producent oferuje stopniowy system certyfikacji to wymagany jest najwyższy dostępny stopień).

21. Termin realizacji przedmiotu zamówienia

Zamawiający wymaga realizacji przedmiotu zamówienia w terminie 14 dni kalendarzowych licząc od dnia podpisania umowy.