Załącznik nr 3 A do SIWZ

Warunki techniczne - część pierwsza zamówienia

1. Przedmiotem pierwszej części zamówienia jest urządzenie typu Unified Threat Management (UTM), którego przeznaczeniem będzie ochrona jednej z podsieci lokalnej Urzędu na styku z siecią Internet. Dostarczone rozwiązanie musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład sprzedawanego rozwiązania były zrealizowane w postaci osobnych zamkniętych platform sprzętowych lub w postaci komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

2. Dla elementów rozwiązania Unified Threat Management (UTM), Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

- kontrola dostępu – zapora ogniowa klasy Stateful Inspection,
- ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS,
- poufność transmisji danych – połączenia szyfrowane IPSec VPN oraz SSL VPN,
- ochrona przed atakami – Intrusion Prevention System,
- kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM,
- kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP,
- kontrola pasma oraz ruchu [QoS, Traffic shaping] – co najmniej określanie maksymalnej i gwarantowanej ilości pasma,
- kontrola aplikacji – system powinien rozpoznawać aplikacje typu: P2P, botnet (C&C – ta komunikacja może być rozpoznawana z wykorzystaniem również innych modułów),
- możliwość analizy ruchu szyfrowanego protokołem SSL,
- mechanizmy ochrony przed wyciekiem poufnej informacji (DLP),
- w przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive,
- monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych,
- monitoring stanu realizowanych połączeń VPN,
- system realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: routera z funkcją NAT lub transparentnym,
- system realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/1000 Base-TX,
- system powinien umożliwiać zdefiniowanie co najmniej 240 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q,
- w zakresie Firewall'a obsługa nie mniej niż 400 tysięcy jednoczesnych połączeń oraz 4 tys. nowych połączeń na sekundę,
- przepustowość Firewall'a: nie mniej niż 1,5 Gbps dla pakietów 512 B,
- wydajność szyfrowania VPN IPSec: nie mniej niż 1 Gbps,
- system powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony system logowania i raportowania w postaci odpowiednio zabezpieczonej platformy sprzętowej lub programowej,

- wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 200 Mbps,
- wydajność skanowania ruchu z włączoną funkcją Antywirus - minimum 30 Mbps,
- w zakresie funkcji IPSec VPN, wymagane jest nie mniej niż:
    - tworzenie połączeń w topologii Site-to-site oraz Client-to-site,
    - monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
    - praca w topologii Hub and Spoke oraz Mesh,
    - możliwość wyboru tunelu przez protokół dynamicznego routingu, np. OSPF,
    - obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth,
- w ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem,
- rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM,
- możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a,
- translacja adresów NAT adresu źródłowego i docelowego,
- polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci,
- możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ,
- silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021),
- ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 4500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos,
- funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP,
- baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxy avoidance. Administrator powinien mieć możliwość nadpisywania kategorii lub tworzenia wyjątków i reguł omijania filtra WWW,
- automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL,
- elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i mieć możliwość współpracy z platformami dedykowanymi do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Ponadto powyższy system musi umożliwiać weryfikację tożsamości użytkowników z wykorzystaniem nie mniej niż:
- haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu,
- haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP,
- haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych,

- rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory.

4. Poszczególne elementy oferowanego rozwiązania powinny posiadać następujące certyfikaty:
   - ICSA lub EAL4 dla funkcji Firewall,
   - ICSA lub NSS Labs dla funkcji IPS,
   - ICSA dla funkcji: SSL VPN, IPSec VPN.
5. **Serwisy i licencje** – Wykonawca, którego oferta zostanie wybrana, zobowiązany jest do dostarczenia licencji aktywacyjnych dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 1 roku.
6. **Gwarancja** – system powinien być objęty serwisem gwarancyjnym producenta lub Autoryzowanego Partnera Serwisowego przez okres minimum 12 miesięcy, realizowanym na terenie Rzeczpospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Wykonawca winien przedłożyć oświadczenie, w którym potwierdzi wymagany serwis gwarancyjny (zawierające numer modułu internetowego i infolinii telefonicznej producenta lub Autoryzowanego Partnera Serwisowego) na terenie Rzeczpospolitej Polskiej.