Załącznik nr 1 do OPZ

Znak sprawy: WAO.271.27.19

Specyfikacja techniczna urządzenia UTM

Urządzenie musi zapewniać wszystkie funkcje bezpieczeństwa oraz funkcjonalności niezależnie od dostawcy łącza, i być kompatybilne z obecnie używanymi urządzeniami przez Zamawiającego – t.j FortiGate 60D.
Urządzenie musi zapewniać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych, monitoring stanu realizowanych połączeń VPN.
Urządzenie powinno dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
Urządzenie powinno dysponować minimum 5 portami Ethernet 100/1000 BaseTX oraz 3 portami Ethernet 10/100 BaseTX.
Możliwość tworzenia min 250 interfejsów wirtualnych definiowanych jako VLAN-y w oparciu o standard 802.1Q.
W zakresie Firewall-a obsługa nie mniej niż 80 tys. jednoczesnych połączeń oraz 3 tys. nowych połączeń na sekundę.
Przepustowość Firewall-a: nie mniej niż 1 Gbps.
Wydajność szyfrowania AES lub 3DES: nie mniej niż 60 Mbps.
Urządzenie powinno być wyposażone w lokalny dysk o pojemności minimum 8 GB do celów logowania i raportowania. W przypadku kiedy urządzenie nie posiada dysku do poszczególnych lokalizacji musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
Poufność danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
Ochrona przed atakami - Intrusion Prevention System [IPS].
Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM uaktualniana nie rzadziej niż co 3 miesiące.
Kontrola pasma oraz ruchu [QoS, Traffic shaping].
Kontrola aplikacji oraz rozpoznawanie ruchu P2P.
Możliwość analizy ruchu szyfrowanego protokołem SSL.
Ochrona przed wyciekiem poufnej informacji (DLP) z funkcją archiwizowania informacji.
Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 50 Mbps.
Wydajność urządzenia (lub zestawu urządzeń) przy skanowaniu strumienia danych z włączoną funkcją:
Antivirus min. 30 Mbps.
Funkcjonalności w zakresie VPN:

- Możliwość spięcia wszystkich dostarczonych urządzeń z możliwością centralnego zarządzania lokalnego (poprzez HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami.
- 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 routiongu, np. OSPF,

Urządzenie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
Polityka bezpieczeństwa wszystkich urządzeń zabezpieczających musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
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 wykrywanych ataków powinna zawierać co najmniej 6500 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 oraz tworzenia wyjątków i reguł omijania filtra WWW.
Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
Dostarczone urządzenia muszą umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą 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 bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.