Załącznik nr 1c

Wymagania techniczne przedmiotu zamówienia

Część nr III

Dostawa urządzenia brzegowego 1szt.

1. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowych. Integralność systemu musi być zapewniona także w przypadku różnych dostawców dla poszczególnych lokalizacji. Dopuszcza się aby elementy wchodzące w skład systemu ochrony były zrealizowane w postaci zamkniętej platformy sprzętowej lub w postaci komercyjnej aplikacji instalowanej na platformie ogólnego przeznaczenia. W przypadku implementacji programowej dostawca powinien zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

2. Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

   2.1. System powinien być zaprojektowany w taki sposób aby możliwa była jego rozbudowa w celu wyeliminowania pojedynczego punktu awarii. W tym celu powinien zapewnić co najmniej:

      2.1.1. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
      2.1.2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
      2.1.3. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.

   2.2. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent
   2.3. System realizujący funkcję Firewall musi dysponować co najmniej 16 portami Ethernet 10/100/1000 Base-TX
   2.4. Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
   2.5. W zakresie Firewall'a obsługa nie mniej niż 1950 tys jednoczesnych połączeń oraz 3,5 tys. nowych połączeń na sekundę
   2.6. Przepustowość Firewall'a: nie mniej niż 3.2 Gbps dla pakietów 512B
   2.7. Wydajność szyfrowania 3DES: nie mniej niż 750 Mbps
   2.8. Wbudowany dysk twardy o pojemności co najmniej 30GB

2.9. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:

2.9.1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
2.9.2. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar
2.9.3. Poufność danych - IPSec VPN oraz SSL VPN
2.9.4. Oochrona przed atakami - Intrusion Prevention System [IPS/IDS]
2.9.5. Kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
2.9.6. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
2.9.7. Kontrola pasma oraz ruchu [QoS, Traffic shaping], co najmniej określenie maksymalnej i gwarantowanej ilości pasma
2.9.8. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
2.9.9. Ochrona przed wyciekiem poufnej informacji (DLP)
2.9.10. Możliwość analizy ruchu szyfrowanego protokołem SSL
2.9.11. Dwu-składnikowe uwierzytelnianie z wykorzystywaniem tokenów sprzętowych lub programowych

2.10. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 35 Mbps
2.11. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 250 Mbps
2.12. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:

2.12.1. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
2.12.2. Dostawca musi dostraczyć nielimitowanego klienta VPN współpracującego z proponowanym rozwiązaniem.
2.12.3. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
2.12.4. Praca w topologii Hub and Spoke oraz Mesh
2.12.5. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
2.12.6. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth

2.13. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM. Protokoły routingu powinny funkcjonować w ramach terminowanych na urządzeniu połączeniach IPSec VPN.
2.14. Możliwość budowy min 5 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.

2.15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.

2.16. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń i alarmowanie oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)

2.17. Możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ

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

2.19. Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać co najmniej 4000 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.

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

2.21. Baza filtra WWW o wielkości co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne (np. spyware, malware, spam, Proxy avoidance). Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.

2.22. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.

2.23. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:

2.23.1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu

2.23.2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP

2.23.3. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych

2.23.4. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.

2.23.5. Rozwiązanie musi integrować się z Citrix XenApp wersja 6.5 oraz 7.6 w zakresie autentykacji użytkowników.

2.23.6. Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty

2.23.6.1. ICSA lub EAL4 dla funkcji Firewall

2.23.6.2. ICSA lub NSS Labs dla funkcji IPS

2.23.6.3. ICSA dla funkcji: SSL VPN, IPSec VPN

2.24. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i

monitorowania platformami wchodzącymi w skład systemu. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

2.25. Rozwiązanie musi posiadać dedykowanego klienta IPSEC VPN dla systemów:

2.25.1. MS Windows 7/8/8.1
2.25.2. Android

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania, Dostawca winien przedłożyć dokument w j. polskim pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (tj. Dz.U. z 2013, poz. 134).

Zamawiający wymaga od Oferenta dostarczenia oświadczenia producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż rozwiązania objęte oferowanymi usługami serwisowymi producenta, w przypadku korzystania z tych usług, zostaną przyjęte do naprawy w autoryzowanym punkcie serwisowym producenta na terenie Polski oraz, że pochodzą one z oficjalnego kanału sprzedaży na terenie Polski.

Wymaga się aby dostawa obejmowała również:

- **Minimum 12 miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia dostawy całego systemu,**
- **Licencje producentów dla wszystkich funkcji bezpieczeństwa na okres minimum 12 m-ce liczoną od dnia zakończenia dostawy całego systemu,**
- **Minimum 12 miesięczny Serwis logistyczny na terenie Polski z dostawą urządzenia zastępczego na drugi dzień roboczy / 8x5xNBD gwarantujący udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy w następnym dniu roboczym.**

Dla zapewnienia wysokiego poziomu usług podmiot serwisujący powinien posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w trybie 8x5 przez dedykowany serwisowy moduł internetowy oraz infolinię 8x5.

Oferent winien przedłożyć dokumenty:

- oświadczenie producenta wskazujące podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczpospolitej Polskiej

- oświadczanie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej)

- certyfikat ISO 9001 podmiotu serwisującego lub równoważny

Termin wykonania zamówienia: **maksymalny** termin dostawy wynosi **7 dni** kalendarzowych licząc od dnia podpisania umowy.