

Minimalne wymagania techniczne dla systemu:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony 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.

Dla elementów systemu bezpieczeństwa obsługujących Urząd Miejski w Giżycku wraz z jednostkami podległymi, Wykonawca zapewni wszystkie poniższe funkcje i parametry pracy:

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - możliwość łączenia w klaster Active-Active lub Active-Passive.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym.
5. System realizujący funkcję Firewall powinien dysponować minimum 10 portami Ethernet 10/100/1000 Base-TX oraz 8 gniazdami SFP 1Gbps.

Po stronie Wykonawcy jest również dostawa 8 par jednomodowych modułów SFP (miniGBIC) do realizacji połączeń na odległość min. 10 km. kompatybilnych z dostarczonym sprzętem.

6. System powinien umożliwiać zdefiniowanie co najmniej 254 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
7. W zakresie Firewall'a obsługa nie mniej niż 6 milionów jednoczesnych połączeń oraz 190 tys. nowych połączeń na sekundę
8. Przepustowość Firewall'a: nie mniej niż 16 Gbps
9. Wydajność szyfrowania VPN IPSec: nie mniej niż 14 Gbps
10. System powinien mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub producenci poszczególnych elementów systemu muszą oferować systemy logowania i raportowania w postaci odpowiednio zabezpieczonych platform sprzętowych lub programowych.
11. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcji. Mogą one być realizowane w postaci osobnych platform sprzętowych lub programowych:

- Kontrola dostępu - zaporą ogniową 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)
12. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych.
13. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) - minimum 4,5 Gbps
14. Wydajność skanowania ruchu z włączoną funkcją Antywirus - minimum 1,7 Gbps
15. 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
16. W ramach funkcji IPSec VPN, SSL VPN – producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem.
17. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
18. Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSec VPN'a Antywirus'a, IPS'a.

19. Translacja adresów NAT adresu źródłowego i docelowego.
20. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci.
21. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ.
22. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2121)
23. 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.
24. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
25. 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.
26. Automatyczne aktualizacje sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
27. System zabezpieczeń musi umożliwiać weryfikację 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
28. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:
 - ICSA lub EAL4 dla funkcji Firewall
 - ICSA lub NSS Labs dla funkcji IPS
 - ICSA dla funkcji: SSL VPN, IPSec VPN
 - NSS Labs Firewall NGFW
 - NSS Labs Data Center IPS

- Common Criteria
- FIPS

29. Preferowane są urządzenia o najlepszej pozycji w testach :

- Miejsce w kwadrancie liderów w raporcie „Magic Quadrant for Unified Threat Management” z 2015 roku;
- Miejsce w kwadrancie liderów w raporcie „Magic Quadrant for Enterprise Network Firewalls” z 2015 roku;

<http://innetworktech.com/wp-content/uploads/2015/04/Magic-Quadrant-for-Enterprise-Network-Firewalls.pdf>
- Skuteczność i wartość zabezpieczeń, zgodnie z raportem „NSS Labs Firewall NGFW” z roku 2014;

30. 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.

31. Serwisy i licencje

- W ramach postępowania powinny zostać dostarczone licencje aktywacyjne dla wszystkich wymaganych funkcji ochronnych, upoważniające do pobierania aktualizacji baz zabezpieczeń przez okres 12 miesięcy.

32. Gwarancja oraz wsparcie:

- a) System powinien być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku gdy producent nie posiada na terenie Rzeczypospolitej Polskiej własnego centrum serwisowego, oferent winien przedłożyć dokument producenta, który wskazuje podmiot uprawniony do realizowania serwisu gwarancyjnego na terenie Rzeczypospolitej Polskiej.
- b) Gwarancja/AHB/SOS: System powinien być objęty rozszerzonym serwisem gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym /w ciągu 24 godzin/, realizowanym przez producenta rozwiązania lub autoryzowanego przedstawiciela producenta, w zakresie serwisu gwarancyjnego, mającego swoją siedzibę na terenie Polski.
- c) Zgłoszenia serwisowe będą przyjmowane w trybie 24/7/360 przez dedykowany serwisowy moduł internetowy oraz infolinię 24/7/360.

Oferent winien przedłożyć dokumenty:

- Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych,
 - oświadczenie Producenta lub Autoryzowanego Partnera Serwisowego o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające numer modułu internetowego i infolinii telefonicznej).
- d) W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument 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 (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

33. Pozostałe wymagania:

- a) Wykonywane czynności montażowe oraz konfiguracyjne nie mogą wpływać na pracę Urzędu i nie mogą powodować przestojów w pracy. Możliwe jest przygotowanie urządzenia w godzinach pracy tj. 7.30 – 15.30 w dni robocze, natomiast sama jego instalacja powinna odbyć się poza tymi godzinami,
- b) Wymaga się aby instalacja została przeprowadzona w siedzibie Zamawiającego (nie dopuszcza się podczas wdrożenia pracy zdalnej),
- d) W ramach obsługi serwisowej inżynier będzie dostępny do pomocy i konsultacji przez cały okres trwania umowy, a także raz na kwartał będzie możliwa wizyta serwisowa mająca na celu konserwację urządzenia,
- e) Po przeprowadzonej instalacji i konfiguracji urządzenia odbędzie się szkolenie obsługi informatycznej z konfiguracji i obsługi urządzenia w siedzibie zamawiającego minimum dwie sesje po 8 godzin.
- f) Wsparcie techniczne zapewnione przez wykonawcę na min. 12 miesięcy, max 2 godzinny czas reakcji od zgłoszenia usterki.
- g) W przypadku awarii i braku możliwości pracy zdalnej czas reakcji na zgłoszenie serwisowe nie powinien przekroczyć 2 godzin a naprawa musi być wykonana maksymalnie w ciągu kolejnych 12 godzin.
- h) Wymaga się aby wszelkie aktualizacje oprogramowania wykonywane były regularnie zgodnie z wypuszczaniem takich aktualizacji przez producenta urządzenia.