

1. Przedmiotem zamówienia jest dostawa dla Zamawiającego urządzeń infrastruktury informatycznej.

2. Realizacja przedmiotu zamówienia obejmuje:

- a. Dostawę sprzętu zgodnie ze specyfikacją określoną w pkt. 3
- b. Zapewnienie gwarancji zgodnie ze specyfikacją określoną w pkt. 4

3. Specyfikacja sprzętu:

Adaptowalne urządzenie chroniące sieć komputerową + **licencja 10 sesji SSL VPN** spełniające poniższe wymagania:

Architektura:

1. Powinno być urządzeniem modularnym pozwalającym na uzyskanie funkcji firewall, VPN (sprzętowe wsparcie szyfracji), sondy IPS.
2. Powinno być wyposażone w co najmniej cztery interfejsy Gigabit Ethernet 10/100/1000
3. Powinno być wyposażone w co najmniej jeden interfejs dla zarządzania pozapasmowego (OOB)
4. Powinno być wyposażone w moduł sprzętowego wsparcia szyfracji DES i AES
5. Powinno posiadać minimum dwa porty dedykowane dla zarządzania: port konsoli, port asynchroniczny dla przyłączenia modemu
6. Powinno posiadać co najmniej jeden port USB (tokeny, certyfikaty etc.)
7. Powinno posiadać co najmniej 64MB pamięci Flash
8. Powinno posiadać co najmniej 1024MB pamięci DRAM
9. Urządzenie powinno posiadać dodatkowy slot pozwalający na wykorzystanie modułów funkcjonalnych zwiększających standardową funkcjonalność urządzenia, a w szczególności
 - a. moduł umożliwiający osiągnięcie pełnej funkcjonalności systemu IPS (Intrusion Prevention System)
 - b. moduł umożliwiający osiągnięcie funkcjonalności ochrony antywirusowej, antyspyware, antyspamowej, filtrowania i blokowania odwołań do niepożądanych adresów URL oraz filtrowania zawartości poczty elektronicznej e-mail
 - c. moduł zwiększający ilość obsługiwanych interfejsów o co najmniej 4 porty Gigabit Ethernet

Zasilanie:

10. Urządzenie powinno posiadać zasilacz umożliwiający zasilanie prądem przemiennym 230V

Wydajność:

11. Urządzenie powinno posiadać wydajność co najmniej 650 Mbps ruchu poddanego inspekcji przez mechanizmy ściany ogniowej
12. Urządzenie powinno posiadać wydajność co najmniej 325 Mbps ruchu szyfrowanego

13. Urządzenie powinno umożliwiać terminowanie co najmniej 5000 jednoczesnych sesji VPN
14. Na urządzeniu powinna istnieć możliwość terminować jednocześnie 2500 sesji WebVPN
15. Urządzenie powinno obsługiwać co najmniej 400 000 jednoczesnych sesji/połączeń z prędkością 20 000 połączeń na sekundę
16. Na urządzeniu powinna istnieć możliwość obsługi do 50 wirtualnych instancji firewall
17. Urządzenie musi obsługiwać co najmniej 10 jednoczesnych sesji SSL VPN (w dostarczanej wersji)

Oprogramowanie – funkcjonalność:

18. Urządzenie powinno pełnić rolę ściany ogniowej śledzącej stan połączeń z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji
19. Urządzenie nie powinno posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej
20. Powinno być oparte o dedykowany system operacyjny – nie dopuszcza się rozwiązań gdzie platformą systemową jest otwarty system operacyjny np. UNIX (Linux, FreeBSD etc.) lub jego modyfikacja
21. Urządzenie powinno umożliwiać osiągnięcie docelowo pełnej funkcjonalności systemu IPS oraz Antivirus z pomocą dodatkowych modułów funkcjonalnych
22. Urządzenie musi posiadać zintegrowane sprzętowe wsparcie dla szyfrowania
23. Urządzenie powinno zostać dostarczone wraz z dedykowanym oprogramowaniem klienta VPN. Oprogramowanie powinno mieć możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows, Solaris i Linux, a także komputerów Mac. Oprogramowanie powinno umożliwiać zestawienie do urządzenia stanowiącego przedmiot postępowania połączeń VPN z komputerów osobistych PC. Oprogramowanie to powinno pochodzić od tego samego producenta, co oferowane urządzenie i powinno być objęte jego jednolitym wsparciem technicznym.
24. Urządzenie powinno mieć możliwość operowania jako transparentna ściana ogniowa warstwy drugiej ISO OSI
25. Powinno mieć możliwość routingu pakietów zgodnie z protokołami RIP, OSPF
26. Powinno obsługiwać mechanizmy związane z obsługą ruchu multicast
27. Powinno obsługiwać protokół NTP
28. powinno obsługiwać IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode
29. Powinno umożliwiać współpracę z serwerami CA
 - a. Baltimore UniCERT
 - b. Entrust Authority
 - c. iPlanet/Netscape CMS
 - d. Microsoft Certificate Services
 - e. RSA KEON
 - f. VeriSign OnSite
30. Powinno obsługiwać funkcjonalność Network Address Translation (NAT)
31. Urządzenie powinno zapewniać mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w modelu active/standby oraz active/active
32. Urządzenie powinno zapewniać funkcjonalność stateful Failover dla ruchu VPN

33. Urządzenie powinno posiadać mechanizmy inspekcji aplikacyjnej i kontroli następujących usług:
- Hypertext Transfer Protocol (HTTP),
 - File Transfer Protocol (FTP),
 - Extended Simple Mail Transfer Protocol (ESMTP),
 - Domain Name System (DNS),
 - Simple Network Management Protocol (SNMP),
 - Internet Control Message Protocol (ICMP),
 - SQL*Net,
 - Network File System (NFS),
 - H.323 (wersje 1-4),
 - Session Initiation Protocol (SIP),
 - Skinny Client Control Protocol (SCCP),
 - Media Gateway Control Protocol (MGCP),
 - Real-Time Streaming Protocol (RTSP),
 - Telephony Application Programming Interface (TAPI)
 - Java Telephony Application Programming Interface (JTAPI) over Computer Telephony Interface Quick Buffer Encoding (CTIQBE) protocol,
 - GPRS Tunneling Protocol (GTP),
 - Lightweight Directory Access Protocol (LDAP), Internet Locator Service (ILS),
 - Sun Remote Procedure Call (RPC)
34. Powinno dokonywać inspekcji ruchu voice w zakresie protokołów H.323, SIP, SCCP, MGCP, TAPI, JTAPI
35. Urządzenie powinno mieć możliwość blokowania aplikacji tunelowanych z użyciem portu 80 w tym:
- Blokowanie komunikatorów internetowych w tym AOL Instant Messenger, Microsoft Messenger, Yahoo Messenger
 - Blokowanie aplikacji typu peer-to-peer w tym KaZaA i Gnutella
 - Zapobieganie stosowaniu aplikacji typu GoToMyPC
36. Urządzenie musi zapewniać obsługę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP w tym:
- AUTH,
 - DATA,
 - EHLO,
 - ETRN,
 - HELO,
 - HELP,
 - MAIL,
 - NOOP,
 - QUIT,
 - RCPT,
 - RSET,
 - SAML,
 - SEND,
 - SOML,
 - VERFY

- 37. Urządzenie powinno mieć możliwość inspekcji protokołów HTTP oraz FTP na nie standardowych portach
- 38. Urządzenie powinno zapewniać wsparcie stosu protokołów IPv6 w tym:
 - a. dla list kontroli dostępu dla IPv6
 - b. Inspekcji aplikacyjnej co najmniej dla protokołów
 - i. HTTP,
 - ii. FTP,
 - iii. SMTP,
 - iv. ICMP,
- 39. Powinno obsługiwać mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu
- 40. Urządzenie powinno umożliwiać współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik, o wielkości przekraczającej 4KB

Zarządzanie i konfiguracja:

- 41. Powinno posiadać możliwość eksportu informacji przez syslog
- 42. Powinno posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołów RADIUS lub TACACS+
- 43. Powinno być konfigurowalne przez CLI oraz interfejs graficzny (oczekiwane są narzędzia dodatkowe w postaci kreatorów połączeń, etc.)
- 44. Dostęp do urządzenia powinien być możliwy przez SSHv1 i SSHv2
- 45. Urządzenie powinno obsługiwać funkcję SCP.
- 46. Plik konfiguracyjny urządzenia powinien być możliwy do edycji w trybie off-line. Tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej powinno być możliwe uruchomienie urządzenia z nową konfiguracją.
- 47. Urządzenie musi umożliwiać jednoczesne przechowywanie w pamięci nieulotnej co najmniej 3 niezależnych konfiguracji urządzenia

Obudowa:

- 48. Powinna być wykonana z metalu, nie dopuszcza się stosowania urządzeń w obudowie plastikowej
- 49. Powinno mieć możliwość montażu w racku 19"

Normy i certyfikacje:

- 50. Powinno spełniać następujące normy bezpieczeństwa i normy dla oddziaływania elektromagnetycznego:
 - a. EN 60950 IEC 60950
 - b. Znak CE
 - c. EN55022 Class A
 - d. EN61000-3-2,
 - e. EN61000-3-3
- 51. Powinno posiadać następujące certyfikacje branżowe
 - a. ICSA Firewall
 - b. ICSA IPSec
 - c. FIPS 140-2 Level 2
 - d. Common Criteria EAL4+

4. Gwarancja Producenta

- 1) Dostarczony sprzęt objęty będzie 36-cio miesięczną gwarancją Producenta, z oczekiwanym czasem wymiany sprzętu w trybie 8x5 NBD.
- 2) Na dostarczone urządzenia i oprogramowanie Wykonawca zobowiązany jest zapewnić serwis gwarancyjny w ramach wykupionego przez niego u producenta urządzeń i oprogramowania kontraktu serwisowego. Wykonawca Zobowiązany jest przedstawić Zamawiającemu, najpóźniej w dniu podpisania ostatniego protokołu zdawczo-odbiorczego, dokumenty potwierdzające zawarcie takiego kontraktu serwisowego (kopie dokumentów potwierdzone za zgodność z oryginałem).
- 3) Serwis gwarancyjny, o którym mowa w pkt. 1, obejmował będzie w szczególności subskrypcję upoważniającą do bezpłatnej aktualizacji zainstalowanego w urządzeniach oprogramowania.
- 4) Zgłoszenia awarii będą przyjmowane w dni robocze, w godz. 08.00 – 16.00
- 5) Gwarancja nie obejmuje uszkodzeń wynikających ze złej eksploatacji sprzętu, które nastąpiły z winy Zamawiającego, któremu dostarczono sprzęt.

5. Wymagania formalne od dostawców

- 1) Wykonawca musi być autoryzowanym partnerem producenta oferowanych rozwiązań, mogącym świadczyć serwis oparty na świadczeniach producenta – do oferty należy załączyć dokument potwierdzający autoryzację (certyfikat lub pisemne potwierdzenie producenta lub jego polskiego przedstawicielstwa).
- 2) Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek Unii Europejskiej - do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy
- 3) Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem),
- 4) całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie wymaganym w SIWZ - do oferty należy dostarczyć odpowiednie oświadczenia Wykonawcy
- 5) Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
- 6) W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:
 - a) zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), oraz

- b) pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów licencyjnych.

Jeżeli inspekcja, o której mowa w ust. 2 powyżej wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 30% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Strony w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych

- 7) Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający dzień składania ofert,
- 8) Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.