ZAŁĄCZNIK NR 1.17 do PFU

UTM - Routery brzegowe i dostępowe

1. Router Typ-1 (Lokalizacja: GPD lub opcjonalnie BS01) – 1 szt.

Urządzenie lub zespół urządzeń klasy operatorskiej pełniące role routera brzegowego, swicha oraz systemu bezpieczeństwa, spełniające następujące wymogi:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 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.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
3. Elementy systemu przenoszące ruch użytkowników powinny dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent
4. System realizujący funkcję Firewall powinien dysponować minimum 16 interfejsami miedzianymi Ethernet 10/100/1000 oraz 2 portami SFP
5. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
6. W zakresie Firewall'a obsługa nie mniej niż 1,4mln jednoczesnych połączeń oraz 50 tys. nowych połączeń na sekundę.
7. System realizujący funkcję Firewall powinien być wyposażony w lokalny dysk o pojemności minimum 16 GB do celów logowania i raportowania. W przypadku kiedy system nie posiada dysku musi być dostarczony system logowania w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej.
8. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    b. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). System kontroli AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    c. Poufność danych - IPSec VPN oraz SSL VPN

   d. Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
   e. Kontrola stron Internetowych – Web Filter [WF]
   f. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
   g. Kontrola pasma oraz ruchu [QoS i Traffic shaping]
   h. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
   i. Możliwość analizy ruchu szyfrowanego SSL'em oraz funkcja SSH proxy
   j. Ochrona przed wyciekiem poufnej informacji (DLP)
9. Wydajność systemu Firewall min 2,5 Gbps
10. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 500 Mbps
11. Wydajność ochrony przed atakami (IPS) min 1,5 Gbps.
12. Wydajność IPSEC VPN, nie mniej niż 1,2 Gbps
13. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
   a. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
   b. Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
   c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
   d. Praca w topologii Hub and Spoke oraz Mesh
   e. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
   f. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
   g. bsługa ssl vpn w trybach portal oraz tunel
14. Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.
15. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
16. Możliwość budowy min 2 oddzielnych instancji systemów bezpieczeństwa (fizycznych lub logicznych) w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
17. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety)
18. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
19. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)

20. Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 6000 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.
21. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
22. Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 50 kategorii. W ramach filtra powinny być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
23. Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
24. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
25. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall powinien posiadać certyfikat ICSA dla rozwiązań kategorii Network Firewall
26. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

Uwaga 1: 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.

Uwaga 2: 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.

2. UTM - Router dostępowy - większe jednostki (Router Typ-2 – 7 szt.)

Urządzenie lub zespół urządzeń klasy operatorskiej pełniące role routera dostępowego, oraz systemu bezpieczeństwa, spełniające następujące wymogi:

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.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

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:
   a. Możliwość łączenia w klaster Active-Active lub Active-Passive każdego z elementów systemu.
   b. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   c. Monitoring stanu realizowanych połączeń VPN oraz automatyczne przekierowanie pakietów zgodnie z trasą definiowaną przez protokół OSPF.
2. System realizujący funkcję Firewall powinien dawać możliwość pracy w jednym z dwóch trybów: Routera z funkcją NAT lub transparent.
3. System realizujący funkcję Firewall musi dysponować co najmniej 10 portami Ethernet 10/100/1000 Base-TX
4. Możliwość tworzenia min 64 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
5. W zakresie Firewall'a obsługa nie mniej niż 450 tys jednoczesnych połączeń oraz 3 tys. nowych połączeń na sekundę

6. Przepustowość Firewall'a: nie mniej niż 1 Gbps
7. Wydajność szyfrowania 3DES: nie mniej niż 750 Mbps
8. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności:
   a. kontrola dostępu - zapora ogniowa klasy Stateful Inspection
   b. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar
   c. poufność danych - IPSec VPN oraz SSL VPN
   d. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
   e. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
   f. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
   g. kontrola pasma oraz ruchu [QoS, Traffic shaping]
   h. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
   i. Ochrona przed wyciekiem poufnej informacji (DLP)
9. Wydajność całego systemu bezpieczeństwa przy skanowaniu strumienia danych z włączonymi funkcjami: Stateful Firewall, Antivirus, WebFilter, min. 40 Mbps
10. Wydajność skanowania ruchu w celu ochrony przed atakami (IPS) min 150 Mbps
11. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    a. Tworzenie połączeń w topologii Site-to-site oraz Client-to-site
    b. Dostawca musi dostraczyć nielimitowanego klienta VPN współpracującego z propomownym rozwiązaniem.
    c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    d. Praca w topologii Hub and Spoke oraz Mesh
    e. Możliwość wyboru tunelu przez protokół dynamicznego routiongu, np. OSPF
    f. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
12. 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.
13. Możliwość budowy min 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie routingu, Firewall'a, Antywirus'a, IPS'a, Web Filter'a.
14. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.

15. 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)
16. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ
17. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
18. 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.
19. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
20. Baza filtra WWW o wielkości co najmniej 45 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.
21. Automatyczne aktualizacje sygnatur ataków, aplikacji , szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
22. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    b. haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    c. haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory bez konieczności instalowania jakiegokolwiek oprogramowania na kontrolerze domeny.
23. Funkcje bezpieczeństwa oferowanego systemu powinny posiadać certyfikaty ICSA dla funkcjonalności Firewall, IPS, Antywirus
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.

Uwaga 1: 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.

Uwaga 2: 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.

3. UTM - Router dostępowy - małe jednostki

Router Typ-3 (Lokalizacja: WN'y w których podłączany jest tylko 1 komputer) – 20 szt.

Urządzenie lub zespół urządzeń klasy operatorskiej pełniące role routera dostępowego, swicha oraz systemu bezpieczeństwa, spełniające następujące wymogi:

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 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.

Dla elementów systemu bezpieczeństwa wykonawca zapewni wszystkie poniższe funkcjonalności:

1. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
2. Elementy systemu przenoszące ruch użytkowników powinny dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent
3. System realizujący funkcję Firewall powinien dysponować minimum 5 interfejsami miedzianymi Ethernet 10/100/1000
4. Możliwość tworzenia min 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
5. W zakresie Firewall'a obsługa nie mniej niż 150tys jednoczesnych połączeń oraz 3 tys. nowych połączeń na sekundę.

6. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie z poniższych funkcjonalności. Poszczególne funkcjonalności systemu bezpieczeństwa mogą być realizowane w postaci osobnych platform sprzętowych lub programowych:
    a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection
    b. Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). System kontroli AV musi umożliwiać skanowanie AV dla plików typu: rar, zip.
    c. Poufność danych - IPSec VPN oraz SSL VPN
    d. Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
    e. Kontrola stron Internetowych – Web Filter [WF]
    f. Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
    g. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
    h. Możliwość analizy ruchu szyfrowanego SSL'em
    i. Ochrona przed wyciekiem poufnej informacji (DLP)
7. Wydajność systemu Firewall min 500 Mbps
8. Wydajność skanowania strumienia danych przy włączonych funkcjach: Stateful Firewall, Antivirus min. 20Mbps
9. Wydajność ochrony przed atakami (IPS) min 100 Mbps.
10. Wydajność IPSEC VPN, nie mniej niż 200 Mbps
11. W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż:
    a. Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site
    b. Producent oferowanego rozwiązania VPN powinien dostarczać klienta VPN współpracującego z proponowanym rozwiązaniem
    c. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności
    d. Praca w topologii Hub and Spoke oraz Mesh
    e. Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
    f. Obsługa ssl vpn w trybach portal oraz tunel
12. Rozwiązanie powinno zapewniać: routing statyczny oraz obsługę Policy Routingu
13. Translacja adresów NAT adresu źródłowego i NAT adresu docelowego.
14. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, interfejsy, protokoły, usługi sieciowe, użytkowników, reakcje zabezpieczeń, rejestrowanie zdarzeń
15. Możliwość tworzenia wydzielonych stref bezpieczeństwa Firewall np. DMZ

16. Silnik antywirusowy powinien umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021)
17. Ochrona IPS powinna opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków powinna zawierać, co najmniej 6000 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.
18. Funkcja kontroli aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP
19. Baza filtra WWW o wielkości, co najmniej 45 milionów adresów URL pogrupowanych w kategorie tematyczne – min 50 kategorii. W ramach filtra powinny być dostępne m.in. kategorie spyware, malware, spam, proxy avoidance, sieci społecznościowe, zakupy. Administrator powinien mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW.
20. Automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych oraz ciągły dostęp do globalnej bazy zasilającej filtr URL.
21. System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż:
    a. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu
    b. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP
    c. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych
    d. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory
22. Element oferowanego systemu bezpieczeństwa realizujący zadanie Firewall powinien posiadać certyfikat ICSA dla rozwiązań kategorii Network Firewall
23. Elementy systemu powinny mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi platformami do centralnego zarządzania i monitorowania. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
24. Wymaga się aby dostawa obejmowała również:
    - Minimum 36 miesięczną gwarancję producentów na dostarczone elementy systemu liczoną od dnia zakończenia wdrożenia całego systemu

Uwaga 1: 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.

Uwaga 2: 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.