Szczegółowy opis przedmiotu zamówienia

I. Wymagania techniczne dla systemu bezpieczeństwa sieci (UTM)

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

System musi pełnić rolę kontrolera sieci bezprzewodowej dla posiadanych przez Zamawiającego Access Pointów:

a. Fortinet FortiAP-U421EV
b. Fortinet FortiAP-321C
c. Fortinet FortiAP-320B
d. Fortinet FortiAP-221B

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

- 16 portami Gigabit Ethernet RJ-45.
- 8 gniazdami SFP 1 Gbps.
- 8 gniazdami SFP+ 10 Gbps.
- 2 gniazdami QSFP+ 40 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie 2xAC.
5. Wraz z urządzeniami należy dostarczyć 4 szt. wkładek QSFP+ 40GBase-LR4
6. System musi być wyposażony w dwa dyski minimum 480 GB SSD

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 8 mln. jednoczesnych połączeń oraz 480 tyś. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 45 Gbps dla pakietów 64 B.
4. Przepustowość Stateful Firewall: nie mniej niż 80 Gbps dla pakietów 1518 B.
5. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 25 Gbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 46 Gbps.
7. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 12 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 7 Gbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 10 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.
   - Google Cloud Platform (GCP).
   - Nuage Networks VSP.
   - OpenStack.
   - VMware vCenter (ESXi).
   - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling” dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.

- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. Urządzenie musi posiadać licencje na możliwość utworzenia minimum 25 wirtualnych routerów (VDOM) z możliwością przypisania osobnych administratorów do każdego wirtualnego routera.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - 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.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), analiza typu Sandbox, antyspam, web filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy, oraz bezterminowo 25 wirtualnych routerów (VDOM).

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

II. Wymagania techniczne dla przełącznika sieciowego.

Wymagania podstawowe

1. Przełącznik posiadający 48 portów 1/10/25 Gbps SFP28
2. Przełącznik posiadający 8 portów 100 Gbps QSFP28

3. Wysokość urządzenia 1U
4. Nieblokująca architektura o wydajności przełączania min. 4 Tb/s
5. Szybkość przełączania min. 4270 Milionów pakietów na sekundę
6. Tablica MAC adresów min. 160 000
7. Pamięć operacyjna: minimum 16 GB pamięci DRAM
8. Pamięć SSD minimum 128 GB
9. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4059
10. Obsługa 802.1v VLAN Klasyfikacja per Protokół oraz port
11. Obsługa Q-in-Q IEEE 802.1ad
12. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
13. Przełącznik musi posiadać dwa redundantne zasilacze o mocy minimum 750 W. Zasilacze muszą wspierać możliwość wymiany w czasie działania przełącznika.
14. Przepływ powietrza w przełączniku: przód-tył
15. Moduł wentylatorów zapewniający ich redundancję
16. Wbudowany DHCP Serwer i klient
17. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
18. Wbudowany port konsolowy RJ-45 do zarządzania przełącznikiem
19. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
20. Port Micro-USB do podpięcia zewnętrznego storage

Obsługa Routingu IPv4

21. Sprzętowa obsługa routingu IPv4 - forwarding
22. Pojemność tabeli routingu min. 16 tys. wpisów
23. Routing statyczny
24. Obsługa routingu dynamicznego IPv4
25. RIP v1/v2
26. OSPFv2
27. BGP4, BGP+
28. IS-IS
29. Minimum 256 instancji VRF

Obsługa Routingu IPv6

30. Sprzętowa obsługa routingu IPv6 - forwarding
31. Pojemność tabeli routingu min. 7,5 tys. wpisów
32. Routing statyczny
33. Obsługa routingu dynamicznego dla IPv6
34. RIPng
35. OSPF v3
36. BGPv6
37. IS-IS
38. Ping dla IPv6
39. Obsługa MLDv1 (Multicast Listener Discovery version 1)
40. Obsługa MLDv2 (Multicast Listener Discovery version 2)
41. Minimum 256 instancji VRF

Obsługa Multicastów

42. Statyczne przyłączanie do grupy multicast
43. Obsługa PIM-SM
44. Obsługa PIM-SSM

45. Obsługa IGMP v1
46. Obsługa IGMP v2
47. Obsługa IGMP v3
48. Obsługa IGMP oraz MLD snooping
49. Obsługa IETF RFC1112 Host Extensions for IP Multicasting

Bezpieczeństwo

50. Obsługa RADIUS Authentication (RFC 2138)
51. Obsługa RADIUS Accounting (RFC 2139)
52. Obsługa IETF RFC5176 Dynamic Authorization Extensions to RADIUS
53. Obsługa 802.1AE Media Access Control Security
54. Obsługa SNMPv1/v2/v3
55. Obsługa 802.1X Port-based Network Access Control
56. Klient SSH2
57. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na
58. Obsługa DHCP Option 82
59. Ograniczanie przepustowości per port – w zakresie 1Mbps – 100 Gbps
60. Obsługa IETF RFC 2474

Bezpieczeństwo sieciowe

61. Obsługa redundancji routingu VRRP (dla IPv4 i IPv6)
62. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
63. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
64. Obsługa Link Aggregation LACP
65. Obsługa 802.1AX Link Aggregation

Zarządzanie

66. Obsługa IETF RFC5905 NTPv4: Protocol and Algorithms Specification
67. Zarządzanie przez SNMP v1/v2/v3
68. Zarządzanie przez przeglądarkę WWW – protokół http i https
69. Możliwość zarzadzania przełącznikiem z poziomu CLI
70. Zarządzanie z dedykowanej aplikacji zarządzającej
71. Telnet Serwer/Klient
72. SSH2 Serwer/Klient
73. Ping dla IPv4 / IPv6
74. Traceroute dla IPv4 / IPv6
75. Obsługa SYSLOG
76. Sprzętowa obsługa sFlow (minimum 3000 próbek per sec)
77. Sprzętowa obsługa IPFIX
78. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events

Inne

79. Obsługa VXLAN: IETF RFC7358
80. Obsługa standardów Shortest Path Bridging (SPB) IEEE 802.1aq oraz IETF RFC 6329
81. Obsługa VXLAN Gateway
82. Obsługa Distributed Virtual Routing (DvR)
83. Obsługa 802.1Qbp Equal-Cost Multi-Path (Shortest Path Bridging)
84. Obsługa 802.1Qcj Automatic Attachment to Provider Backbone Bridging (PBB) Services
85. Obsługa 802.1ag Connectivity Fault Management
86. Obsługa 802.1ah Provider Backbone Bridges

87. Obsługa 802.1aq Shortest Path Bridging (SPB) MAC-in-MAC
88. Obsługa IETF RFC 6329 IS-IS Extensions supporting IEEE 80 2.1aq SPB
89. Przełącznik musi umożliwiać wymianę zasilaczy i wentylatorów z posiadanym przez Zamawiającego przełacznikiem Extreme Networks VSP7400-48Y-8C-AC-F
90. Przełacznik musi umożliwiać budowę topologii Fabric z posiadanymi przez Zamawiającego przełączniki Extreme Networks VSP7400, x460-G2, x440-G2.
91. Przełacznik musi być objęty 3 letnim wsparciem technicznym obejmującym wymianę uszkodzonego urządzenia w trybie NBD, aktualizację oprogramowania, dostęp do bazy wiedzy technicznej.

III. Wymagania formalne

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.
2. Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.