



Szczegółowy opis przedmiotu zamówienia

1. System bezpieczeństwa Typ 1 – 6 kompletów w składzie:
urządzenie UTM (1 szt.) + przełącznik sieciowy Typ 1 (1 szt.)
2. System bezpieczeństwa Typ 2 – 5 kompletów w składzie:
urządzenie UTM (1 szt.) + przełącznik sieciowy Typ 2 (1 szt.)
3. System bezpieczeństwa Typ 3 – 5 kompletów w składzie:
urządzenie UTM (1 szt.)

I. Wymagania techniczne dla urządzenia UTM

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.

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 każdej instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie:

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

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. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. 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: 10 portami Gigabit Ethernet RJ-45.
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 AC.



Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6.2 Gbps.
5. 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 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 720 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniżej wymienione funkcje.

1. Kontrola dostępu - zaporą ogniową 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.

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).
- OpenStack.
- VMware vCenter (ESXi).

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

W zakresie routingu rozwiązanie powinno zapewniać obsługę:

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



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. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. 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:
 - Hasła statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
 - Hasła statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
 - Hasła dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
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 dwuskładnikowego 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 Firewall 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 zbieranie logów do aplikacji logowania i raportowania udostępnianej w chmurze.
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 certyfikacje ICASA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania przez okres 36 miesięcy 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.

II. Wymagania techniczne dla przełącznika sieciowego Typ 1

Parametry fizyczne platformy

1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
2. Zasilanie AC 230V.
3. Maksymalny pobór mocy: 10 W.
4. Minimalny zakres temperatury pracy: 0-40°C.



Interfejsy sieciowe - wymagania minimalne

Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w liczbie:

- 8 portów GE, RJ-45.
- 2 porty GE, SFP.

Zarządzanie

1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
3. Wsparcie dla SNMP w wersjach 1-3
4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
9. Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
10. Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

1. Przepustowość urządzenia - min. 20 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 14 Mpps.
2. Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
3. Opóźnienie wprowadzane przez przełącznik - poniżej 4 mikrosekund.

Wymagane funkcje

1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
2. Obsługa Jumbo Frames.
3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
4. Agregacja portów zgodna ze standardem 802.3ad.
5. Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
6. Wsparcie dla Private VLAN.
7. Port-mirroring.
8. Uwierzytelnianie 802.1x na poziomie portu.
9. Uwierzytelnianie 802.1x w oparciu o adres MAC.
10. W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.



III. Wymagania techniczne dla przełącznika sieciowego Typ 2

Parametry fizyczne platformy

1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
2. Zasilanie AC 230V.
3. Maksymalny pobór mocy: 20 W.
4. Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

Wymaganiem jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w liczbie:

- 24 porty GE, RJ-45.
- 4 porty GE, SFP.

Zarządzanie

1. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
2. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
3. Wsparcie dla SNMP w wersjach 1-3
4. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
5. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
6. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
7. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
8. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
9. Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
10. Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

1. Przepustowość urządzenia - min. 56 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 40 Mpps.
2. Tablica adresów MAC o pojemności co najmniej 8 k wpisów.
3. Opóźnienie wprowadzane przez przełącznik - poniżej 4 mikrosekund.

Wymagane funkcje

1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
2. Obsługa Jumbo Frames.



3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
4. Agregacja portów zgodna ze standardem 802.3ad.
5. Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
6. Wsparcie dla Private VLAN.
7. Port-mirroring.
8. Uwierzytelnianie 802.1x na poziomie portu.
9. Uwierzytelnianie 802.1x w oparciu o adres MAC.
10. W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
11. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
12. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.

IV. Integracja przełączników sieciowych z systemem centralnego zarządzania (wymagania dotyczą przełączników Typ 1 i Typ 2)

Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf).

Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:

- Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
- Centralne zarządzanie sieciami VLAN.
- Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
- Obsługa białych i czarnych list adresów MAC.
- Wykrywanie aplikacji komunikujących się w sieci.
- Musi być możliwe redundantne połączenie z elementami zarządzającymi.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

1. Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN.
2. Routing statyczny i dynamiczny (co najmniej OSPF).
3. Policy Based Routing.

Wymagane jest aby rola dedykowanego kontrolera była pełniona przez wyspecyfikowany UTM Typ 1 oraz posiadane przez Zamawiającego urządzenie Fortinet FortiGate-1500D.

V. Gwarancja oraz wsparcie

1. 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 8x5.
2. Serwis gwarancyjny musi być realizowany przez producenta urządzenia lub autoryzowanego partnera serwisowego.



VI. 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.