SZCZEGÓŁOWA SPECYFIKACJA OFEROWANEGO SPRZĘTU

**UTM DUŻE**

MARKA: ………………………………..

MODEL: ………………………………..

|  |  |
| --- | --- |
| **Wyszczególnienie** | **Potwierdzenie spełnienia warunku** |
| OBSŁUGA SIECI  |
| 1. Urządzenie posiada wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
 | Tak/Nie\* |
| ZAPORA KORPORACYJNA (Firewall) |
| 1. Urządzenie jest wyposażone w Firewall klasy Stateful Inspection.
 | Tak/Nie\* |
| 1. Urządzenie obsługuje translacje adresów NAT n:1, NAT 1:1 oraz PAT.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).
 | Tak/Nie\* |
| 1. Interface (GUI) do konfiguracji firewall umożliwia tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.
 | Tak/Nie\* |
| 1. Administrator ma możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
 | Tak/Nie\* |
| 1. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
 | Tak/Nie\* |
| 1. Edytor reguł firewall posiada wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
 | Tak/Nie\* |
| 1. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
 | Tak/Nie\* |
| 1. System umożliwia budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
 | Tak/Nie\* |
|  INTRUSION PREVENTION SYSTEM (IPS)  |
| 1. System detekcji i prewencji włamań (IPS) jest zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
 | Tak/Nie\* |
| 1. Moduł IPS jest opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
 | Tak/Nie\* |
| 1. Moduł IPS zabezpiecza przed co najmniej 10 000 ataków i zagrożeń.
 | Tak/Nie\* |
| 1. Administrator ma możliwość tworzenia własnych sygnatur dla systemu IPS.
 | Tak/Nie\* |
| 1. Moduł IPS nie tylko wykrywa, ale również usuwa szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
 | Tak/Nie\* |
| 1. Administrator ma możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
 | Tak/Nie\* |
| 1. Po zakupie stosownej licencji moduł IPS zapewnia analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose & SV).
 | Tak/Nie\* |
| 1. Urządzenie zapewnia automatyczną aktualizację sygnatur kontekstowych.
 | Tak/Nie\* |
| KSZTAŁTOWANIE PASMA (Traffic Shapping)  |
| 1. Urządzenie umożliwia kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
 | Tak/Nie\* |
| 1. Ograniczenie pasma lub priorytetyzacja reguły firewall jest możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
 | Tak/Nie\* |
| 1. Urządzenie umożliwia kształtowanie pasma na podstawie aplikacji generującej ruch.
 | Tak/Nie\* |
| OCHRONA ANTYWIRUSOWA  |
| 1. Urządzenie umożliwia zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
 | Tak/Nie\* |
| 1. Co najmniej jeden z dwóch skanerów antywirusowych jest dostarczany w ramach podstawowej licencji.
 | Tak/Nie\* |
| 1. Administrator ma możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
 | Tak/Nie\* |
| 1. Administrator ma możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
 | Tak/Nie\* |
| OCHRONA ANTYSPAM  |
| 1. Urządzenie posiada mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
 | Tak/Nie\* |
| 1. Ochrona antyspam działa w oparciu o:
* białe/czarne listy,
* DNS RBL,
* Skaner heurystyczny.
 | Tak/Nie\* |
| 1. W przypadku ochrony w oparciu o DNS RBL administrator ma możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
 | Tak/Nie\* |
| 1. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam jest w formacie zgodnym z formatem programu Spamassassin.
 | Tak/Nie\* |
| WIRTUALNE SIECI PRYWATNE (VPN)  |  |
| 1. Urządzenie umożliwia stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
 | Tak/Nie\* |
| 1. Urządzenie wspiera co najmniej następujące typy sieci VPN:
* PPTP VPN,
* IPSec VPN,
* SSL VPN.
 | Tak/Nie\* |
| 1. SSL VPN działa co najmniej w trybach tunelu i portalu.
 | Tak/Nie\* |
| 1. Producent urządzenia umożliwia pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
 | Tak/Nie\* |
| 1. Klient SSL VPN jest dostępny z poziomu portalu uwierzytelniania (captive portal)
 | Tak/Nie\* |
| 1. Urządzenie umożliwia funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
 | Tak/Nie\* |
| 1. Urządzenie umożliwia wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia tworzenie tuneli IPSec Policy Based oraz Route Based.
 | Tak/Nie\* |
| UWIERZYTELNIANIE  |
| 1. Urządzenie umożliwia uwierzytelnianie użytkowników co najmniej w oparciu o:
* lokalną bazę użytkowników (wewnętrzny LDAP),
* zewnętrzną bazę użytkowników (zewnętrzny LDAP),
* usługę katalogową Microsoft Active Directory.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia równoczesne użycie co najmniej 5 różnych baz LDAP.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
* SSL,
* Radius,
* Kerberos.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
 | Tak/Nie\* |
| 1. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta.
 | Tak/Nie\* |
| 1. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
 | Tak/Nie\* |
| 1. Rozwiązanie ma możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta wspiera co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
 | Tak/Nie\* |
| 1. Urządzenie posiada wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
 | Tak/Nie\* |
| 1. Wbudowany moduł 2FA musi daje możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
 | Tak/Nie\* |
| ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)  |
| 1. Urządzenie umożliwia wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
 | Tak/Nie\* |
| 1. Mechanizm równoważenia obciążenia łącza internetowego działa w oparciu o następujące dwa mechanizmy:
* równoważenie względem adresu źródłowego,
* równoważenie względem połączenia.
 | Tak/Nie\* |
| 1. Mechanizm równoważenia obciążenia uwzględnia wagi przypisywane osobno dla każdego z łączy do Internetu.
 | Tak/Nie\* |
| 1. Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
 | Tak/Nie\* |
| 1. Urządzenie wspiera mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
 | Tak/Nie\* |
| 1. W zakresie SD-WAN urządzenie zapewnia obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
 | Tak/Nie\* |
| 1. Monitorowanie dostępności łącza jest możliwe w oparciu o ICMP oraz TCP.
 | Tak/Nie\* |
| ROUTING (TRASOWANIE)  |
| 1. Urządzenie umożliwia statyczne trasowanie pakietów.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
 | Tak/Nie\* |
| 1. Urządzenie umożliwia dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.
 | Tak/Nie\* |
| ADMINISTRACJA URZĄDZENIEM  |
| 1. Konfiguracja urządzenia jest możliwa z wykorzystaniem polskiego interfejsu graficznego.
 | Tak/Nie\* |
| 1. Interfejs konfiguracyjny jest dostępna poprzez przeglądarkę internetową, a komunikacja jest możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
 | Tak/Nie\* |
| 1. Administrator ma możliwość wskazania do komunikacji innego portu niż 443 TCP.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
 | Tak/Nie\* |
| 1. Urządzenie oferuje możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia zarządzenia z poziomu konsoli (SSH)
 | Tak/Nie\* |
| 1. Urządzenie umożliwia zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
 | Tak/Nie\* |
| 1. Interfejs konfiguracyjny platformy centralnego zarządzania jest dostępny poprzez przeglądarkę internetową, a komunikacja jest zabezpieczona za pomocą protokołu HTTPS.
 | Tak/Nie\* |
| 1. Wbudowany webowy, graficzny interfejs administracyjny urządzenia oferuje narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
 | Tak/Nie\* |
| 1. Wbudowany webowy, graficzny interfejs administracyjny oferuje narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
 | Tak/Nie\* |
| 1. Wbudowany webowy, graficzny interfejs administracyjny oferuje możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
 | Tak/Nie\* |
| 1. Wbudowany webowy, graficzny interfejs administracyjny oferuje możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
 | Tak/Nie\* |
| 1. System oferuje możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
 | Tak/Nie\* |
| 1. Urządzenie oferuje portal uwierzytelniania (captive portal) dla użytkowników.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia zapisywanie logów na wbudowanym dysku.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
 | Tak/Nie\* |
| 1. Urządzenie umożliwia eksportowanie logów za pomocą protokołu IPFIX.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
* manualnego eksportu do pliku w dowolnym momencie czasu,
* automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
 | Tak/Nie\* |
| 1. Rozwiązanie daje możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
 | Tak/Nie\* |
| RAPORTOWANIE  |
| 1. Urządzenie posiada wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
 | Tak/Nie\* |
| 1. System raportowania i przeglądania logów wbudowany w system nie wymaga dodatkowej licencji do swojego działania.
 | Tak/Nie\* |
| 1. System raportowania posiada predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
 | Tak/Nie\* |
| 1. System raportowania umożliwia wygenerowanie co najmniej 25 różnych raportów.
 | Tak/Nie\* |
| 1. System raportowania umożliwia edycję konfiguracji bezpośrednio z poziomu raportu.
 | Tak/Nie\* |
| 1. System raportowania umożliwia eksport wyników raportu do formatu CSV.
 | Tak/Nie\* |
| 1. Urządzenie posiada możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
 | Tak/Nie\* |
| POZOSTAŁE USŁUGI I FUNKCJE  |
| 1. Urządzenie umożliwia stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
 | Tak/Nie\* |
| 1. Urządzenie posiada wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
 | Tak/Nie\* |
| 1. Urządzenie pozwala na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
 | Tak/Nie\* |
| 1. Konfiguracja serwera DHCP jest niezależna dla IPv4 i IPv6.
 | Tak/Nie\* |
| 1. Urządzenie umożliwia stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
 | Tak/Nie\* |
| 1. Urządzenie posiada usługę DNS Proxy.
 | Tak/Nie\* |
| 1. Urządzenie posiada wsparcie dla Spanning-tree protocol (RSTP/MSTP).
 | Tak/Nie\* |
| 1. Urządzenie oferuje wsparcie dla IEEE 802.1Q VLAN.
 | Tak/Nie\* |
| 1. Urządzenie ma zaimplementowane Open API
 | Tak/Nie\* |
| 1. Urządzenie posiada dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu możliwe jest zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.
 | Tak/Nie\* |
| 1. Urządzenie oferuje możliwość zwiększenia wydajności takich parametrów jak przepustowości firewall, IPS, Antywirus, VPN. Zwiększenie wydajności odbywa się wyłącznie przez zmianę licencji i nie wymaga ingerencji w komponenty fizyczne urządzenia czy wymianę samego urządzenia.
 | Tak/Nie\* |
| GWARANCJA I SERWIS  |
| 1. Urządzenie jest objęte minimum 36-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
 | Tak/Nie\* |
| 1. W okresie obowiązywania gwarancji jest zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
 | Tak/Nie\* |
| 1. Urządzenie jest objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny.
 | Tak/Nie\* |
| PARAMETRY SPRZĘTOWE  |
| 1. Rozwiązanie będzie dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive
 | Tak/Nie\* |
| 1. Urządzenie jest wyposażone w dysk SSD o pojemności co najmniej 200 Gb.
 | Tak/Nie\* |
| 1. Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
 | Tak/Nie\* |
| 1. Liczba portów Ethernet 2,5Gbps – min. 8
 | Tak/Nie\* |
| 1. Liczba portów światłowodowych 10Gbps – min. 2
 | Tak/Nie\* |
| 1. Urządzenie wyposażone jest w dodatkowy moduł z 4 interfejsami światłowodowymi 10Gbps
 | Tak/Nie\* |
| 1. Urządzenie pozwala na instalację modułu rozszerzeń z poniższej listy, zamiennie do modułu, o którym mowa powyżej:
* Moduł z 8 interfejsami miedzianymi 10/100/1000Mbps
* Moduł z 4 interfejsami miedzianymi 10Gbps
* Moduł z 8 interfejsami światłowodowymi 1Gbps
 | Tak/Nie\* |
| 1. Urządzenie umożliwia dostęp do Internetem za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
 | Tak/Nie\* |
| 1. Urządzenie jest wyposażone w min. 2 różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.
 | Tak/Nie\* |
| 1. Przepustowość Firewall (1518 bajtów UDP) – min 18Gbps.
 | Tak/Nie\* |
| 1. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – min 10Gbps.
 | Tak/Nie\* |
| 1. Przepustowość filtrowania Antywirusowego – min 3Gbps.
 | Tak/Nie\* |
| 1. Przepustowość tunelu VPN przy szyfrowaniu AES-GCM – min 4Gbps.
 | Tak/Nie\* |
| 1. Liczba tuneli VPN IPSec – min 1 000.
 | Tak/Nie\* |
| 1. Liczba tuneli typu SSL VPN (tryb tunelu) – min 300.
 | Tak/Nie\* |
| 1. Liczba tuneli typu SSL VPN (tryb portalu) – min 300.
 | Tak/Nie\* |
| 1. Obsługa interfejsów 802.11q (VLAN) – min 1336.
 | Tak/Nie\* |
| 1. Liczba równoczesnych sesji – min 1 000 000 i nie mniej niż 50 000 nowych sesji/sekundę.
 | Tak/Nie\* |
| 1. Urządzenie jest wyposażone w moduł TPM
 | Tak/Nie\* |
| 1. Urządzenie nie ma limitu na liczbę użytkowników.
 | Tak/Nie\* |
| 1. Liczba reguł filtrowania – min 32 768.
 | Tak/Nie\* |
| 1. Liczba tras statycznego routingu – min 5 120.
 | Tak/Nie\* |
| 1. Liczba tras dynamicznego routingu – min 10 000.
 | Tak/Nie\* |
| 1. Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U.
 | Tak/Nie\* |

\* - należy skreślić niewłaściwe