

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA  
„Dostawa serwera sieciowego, dostawa UTM”

## 1. Wstęp

Niniejszy dokument stanowi szczegółowy opis przedmiotu zamówienia na zakup oraz konfigurację sprzętu wraz z oprogramowaniem.

## 2. Przedmiot zamówienia

Przedmiotem zamówienia jest:

- 1) sprzedaż, dostarczenie sprzętu wraz z oprogramowaniem;
- 2) udzielenie przez Wykonawcę gwarancji i zapewnienie serwisu gwarancyjnego na dostarczony Sprzęt w okresach wymaganych w SWZ tj. : **minimum 36 m-cy na serwer, 12 m-cy na UTM.**
- 3) udzielenie licencji na oprogramowanie;
- 4) dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu.

## 3. Zakres zamówienia i termin realizacji

Zamawiający wymaga, aby dostawa do Zamawiającego nastąpiła w terminach określonych w poniższej tabeli.

LP	Przedmiot dostawy	Liczba sprzętu	Termin dostawy – liczba dni od podpisania umowy
1	Serwer sieci	1	60
2	UTM	1	60

## 4. Szczegółowa specyfikacja sprzętu – serwer.

Parametr	Charakterystyka (wymagania minimalne)
<b>Obudowa</b>	Obudowa Rack o wysokości max 2U z możliwością instalacji do 8 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych.  Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne.
<b>Płyta główna</b>	Płyta główna z możliwością zainstalowania minimum dwóch procesorów Intel 3rd Gen. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA  
„Dostawa serwera sieciowego, dostawa UTM”

<b>Chipset</b>	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
<b>Procesor</b>	Zainstalowane dwa procesory 8-rdzeniowe, klasy x86, dedykowane do pracy z zaoferowanym serwerem, taktowane zegarem min. 2.8 GHz (częstotliwość bazowa) umożliwiające osiągnięcie wyniku minimum 34 900 punktów w teście PassMark dla konfiguracji Dual CPU- CPU Mark dostępnym na stronie internetowej: <a href="https://www.cpubenchmark.net/multi_cpu.html">https://www.cpubenchmark.net/multi_cpu.html</a>
<b>RAM</b>	Minimum 64GB DDR4 RDIMM 3200MT/s w kościach 16GB, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
<b>Zabezpieczenia pamięci RAM</b>	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
<b>Gniazda PCI</b>	- minimum cztery sloty PCIe z czego przynajmniej trzy generacji 4
<b>Interfejsy sieciowe/FC/SAS</b>	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
<b>Dyski twarde</b>	<p>Możliwość instalacji dysków SAS, SATA, SSD</p> <p>Zainstalowane 2 dyski HDD NLSAS o pojemności min. 8TB, 12Gb/s, 7.2 tys. obr./min, Hot-Plug</p> <p>Zainstalowane 2 dyski HDD NLSAS o pojemności min. 2TB, 12Gb/s, 7.2 tys. obr./min, Hot-Plug</p> <p>Możliwość zainstalowania dwóch dysków M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1.</p> <p>Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.</p>
<b>Kontroler RAID</b>	Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.
<b>System operacyjny/System wirtualizacji</b>	<p>Licencja Windows Server 2022 Standard, licencja pokrywająca wszystkie fizyczne rdzenie w serwerze.</p> <p>System należy dostarczyć wraz z licencjami CAL na 35 użytkowników.</p>
<b>Wbudowane porty</b>	<p>Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej,</p> <p>Tylne: min. 1x VGA, min. 2x USB w tym 1x USB 3.0,</p>
<b>Video</b>	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
<b>Zasilacze</b>	Redundantne, Hot-Plug min. 800W każdy
<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>• Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.</li> <li>• Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.</li> <li>• Moduł TPM 2.0</li> <li>• Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem</li> </ul>
<b>Diagnostyka</b>	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**  
**„Dostawa serwera sieciowego, dostawa UTM”**

<b>Karta Zarządzania</b>	<p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <ul style="list-style-type: none"> <li>• zdalny dostęp do graficznego interfejsu Web karty zarządzającej;</li> <li>• zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);</li> <li>• szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika;</li> <li>• wsparcie dla IPv6;</li> <li>• wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;</li> <li>• możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;</li> <li>• integracja z Active Directory;</li> <li>• wsparcie dla dynamic DNS;</li> <li>• wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.</li> <li>• możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera</li> <li>• możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera</li> </ul>
<b>Certyfikaty</b>	<p>Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001.</p> <p>Serwer musi posiadać deklarację CE.</p> <p>Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022.</p>
<b>Warunki gwarancji</b>	<p>3 lata gwarancji producenta realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.</p> <p>Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.</p> <p>Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p> <p>Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.</p> <p>Możliwość rozszerzenia gwarancji przez producenta do 7 lat.</p> <p>Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera</p>
<b>Dokumentacja użytkownika</b>	<p>Zamawiający wymaga dokumentacji w języku polskim lub angielskim.</p> <p>Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.</p>

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA  
„Dostawa serwera sieciowego, dostawa UTM”

## 5. Szczegółowa specyfikacja sprzętu wraz z konfiguracją – UTM.

Dostawa urządzenia klasy UTM - formularz oferty	
PARAMETR	WYMAGANIA
Sprzęt wyprodukowany	Nie wcześniej niż 6 miesięcy przed datą publikacji ogłoszenia
Obudowa	do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn montażowych, lub półka montażowa. W ofercie należy podać sposób montażu
Porty	<ul style="list-style-type: none"> <li>✓ LAN: min 10 x 1GbE,</li> <li>✓ WAN: 1x1GbE</li> <li>✓ Port do podłączenia konsolowego</li> <li>✓ Port konsolowy: minimum 1xRJ-45</li> <li>✓ Port USB: minimum 1 port umożliwiający załadowanie konfiguracji dla przełącznika z pamięci flash USB</li> <li>✓ Urządzenie musi umożliwiać pełną rekonfigurację interfejsów wewnętrznych, wspierając m.in.: <ul style="list-style-type: none"> <li>➤ Stworzenie wirtualnego switch z interfejsów,</li> <li>➤ Stworzenie interfejsów typu bridge,</li> <li>➤ Agregacji interfejsów m.in. za pomocą LACP.</li> </ul> </li> </ul>
Wydajność urządzenia	<ul style="list-style-type: none"> <li>✓ Wymagane przepustowość urządzenia dla ruchu: IPS: min 1500 Mbps</li> <li>✓ Wymagane przepustowość urządzenia dla ruchu: Ruchu Firewall: min 7000 Mbps,</li> <li>✓ Liczba jednoczesnych sesji: min 400000</li> </ul>
Zarządzanie	<ul style="list-style-type: none"> <li>✓ Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.</li> <li>✓ Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.</li> <li>✓ Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.</li> <li>✓ Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.</li> <li>✓ Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH)</li> <li>✓ Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.</li> </ul>

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**  
**„Dostawa serwera sieciowego, dostawa UTM”**

	<ul style="list-style-type: none"> <li>✓ Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.</li> <li>✓ Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.</li> <li>✓ Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).</li> <li>✓ Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.</li> <li>✓ Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: <ul style="list-style-type: none"> <li>➤ manualnego eksportu do pliku w dowolnym momencie czasu,</li> <li>➤ automatycznego eksportu do chmury producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu</li> </ul> </li> <li>✓ Urządzenie ma umożliwiać odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.</li> <li>✓ Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.</li> </ul>
<b>Bezpieczeństwo</b>	<ul style="list-style-type: none"> <li>✓ Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection.</li> <li>✓ Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT.</li> <li>✓ Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge).</li> <li>✓ Interface (GUI) do konfiguracji firewall ma umożliwiać 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.</li> <li>✓ Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.</li> <li>✓ Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.</li> </ul>

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa serwera sieciowego, dostawa UTM”

	<ul style="list-style-type: none"> <li>✓ Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.</li> <li>✓ Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.</li> <li>✓ Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.</li> <li>✓ Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).</li> <li>✓ System detekcji i prewencji włamań (IPS) ma być 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.</li> <li>✓ Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.</li> <li>✓ Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.</li> <li>✓ Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.</li> <li>✓ Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.</li> <li>✓ Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS.</li> <li>✓ Administrator ma mieć 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.</li> <li>✓ Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.</li> <li>✓ Po zakupie stosownej licencji moduł IPS ma zapewniać 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 &amp; SV).</li> <li>✓ Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.</li> </ul>
--	--

## SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

## „Dostawa serwera sieciowego, dostawa UTM”

	<ul style="list-style-type: none"> <li>✓ Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.</li> <li>✓ Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).</li> <li>✓ Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.</li> <li>✓ Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).</li> <li>✓ Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.</li> <li>✓ Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.</li> <li>✓ Administrator ma mieć 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 być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.</li> <li>✓ Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).</li> <li>✓ Ochrona antyspam ma działać w oparciu o: <ul style="list-style-type: none"> <li>a. białe/czarne listy,</li> <li>b. DNS RBL,</li> <li>c. Skaner heurystyczny.</li> </ul> </li> <li>✓ W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.</li> <li>✓ Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.</li> <li>✓ Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).</li> <li>✓ Urządzenie ma wspierać co najmniej następujące typy sieci VPN: <ul style="list-style-type: none"> <li>a. PPTP VPN,</li> <li>b. IPSec VPN,</li> <li>c. SSL VPN.</li> </ul> </li> <li>✓ SSL VPN ma działać co najmniej w trybach tunelu i portalu.</li> <li>✓ Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.</li> <li>✓ Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łączy zapasowe na wypadek awarii łączy dostawcy podstawowego (VPN Failover).</li> <li>✓ Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf.</li> </ul>
--	--

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**  
**„Dostawa serwera sieciowego, dostawa UTM”**

	<ul style="list-style-type: none"> <li>✓ Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.</li> <li>✓ Urządzenie ma posiadać wbudowany filtr URL.</li> <li>✓ Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.</li> <li>✓ Administrator ma mieć możliwość dodawania własnych kategorii URL.</li> <li>✓ Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: <ul style="list-style-type: none"> <li>a. blokowanie dostępu do adresu URL,</li> <li>b. zezwolenie na dostęp do adresu URL,</li> <li>c. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.</li> </ul> </li> <li>✓ Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.</li> <li>✓ Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.</li> <li>✓ Filtr URL musi uwzględniać komunikację po protokole HTTPS.</li> <li>✓ Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.</li> <li>✓ Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.</li> <li>✓ Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: <ul style="list-style-type: none"> <li>a. lokalną bazę użytkowników (wewnętrzny LDAP),</li> <li>b. zewnętrzną bazę użytkowników (zewnętrzny LDAP),</li> <li>c. usługę katalogową Microsoft Active Directory.</li> </ul> </li> <li>✓ Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.</li> <li>✓ Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: <ul style="list-style-type: none"> <li>a. SSL,</li> <li>b. Radius,</li> <li>c. Kerberos.</li> </ul> </li> <li>✓ Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.</li> <li>✓ Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.</li> <li>✓ Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.</li> <li>✓ Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).</li> <li>✓ Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy:</li> </ul>
--	--



**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**  
**„Dostawa serwera sieciowego, dostawa UTM”**

	<ul style="list-style-type: none"> <li>a. równoważenie względem adresu źródłowego,</li> <li>b. równoważenie względem połączenia.</li> </ul> <ul style="list-style-type: none"> <li>✓ Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.</li> <li>✓ Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łączy podstawowego (tzw. Failover).</li> <li>✓ Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy.</li> <li>✓ W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów).</li> <li>✓ Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.</li> <li>✓ Urządzenie ma umożliwiać statyczne trasowanie pakietów.</li> <li>✓ Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łączy podstawowego.</li> <li>✓ Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).</li> <li>✓ Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.</li> </ul>
Inne wymagania	<ul style="list-style-type: none"> <li>✓ Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.</li> <li>✓ Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.</li> <li>✓ Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).</li> <li>✓ Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.</li> <li>✓ Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsiaci w zakresie określenia bramy, serwerów DNS, nazwy domeny.</li> <li>✓ Urządzenie ma posiadać usługę DNS Proxy.</li> <li>✓ Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).</li> <li>✓ Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.</li> <li>✓ Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.</li> </ul>

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**  
**„Dostawa serwera sieciowego, dostawa UTM”**

	<ul style="list-style-type: none"> <li>✓ System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.</li> <li>✓ System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.</li> <li>✓ System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.</li> <li>✓ System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.</li> <li>✓ W ramach posiadanej licencji urządzenie ma umożliwiać skorzystanie z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny.</li> <li>✓ Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.</li> <li>✓ Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).</li> </ul>
Warunki środowiskowe	<ul style="list-style-type: none"> <li>✓ Przystosowanie do pracy w temperaturze minimum w zakresie 0-45 stopni Celcjusza</li> <li>✓ Przystosowanie do pracy w wilgotności minimum w zakresie 10-90 procent wilgotności</li> </ul>
Gwarancja	<ul style="list-style-type: none"> <li>✓ Urządzenie ma być objęte minimum 12-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.</li> <li>✓ W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.</li> </ul>
Licencje i oprogramowanie	<ul style="list-style-type: none"> <li>✓ Dostarczone oprogramowanie do zarządzania Urządzeniem oraz wykonywaniem czynności administracyjnych (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.</li> <li>✓ W przypadku gdy realizacji funkcjonalności w zakresie ochrony i monitorowania sieci WAN/LAN niezbędne są licencje i/lub subskrypcje dostarczone subskrypcje muszą obejmować co najmniej 3 letni okres od momentu ich aktywacji po instalacji urządzenia u Zamawiającego.</li> <li>✓ Podać nazwę licencji/ subskrypcji:</li> <li>✓ W formularzu oferty należy podać okres obowiązywania danej licencji subskrypcji:</li> </ul>

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA  
„Dostawa serwera sieciowego, dostawa UTM”

Dostawa i odbiór sprzętu	<ul style="list-style-type: none"> <li>✓ Wykonawca dostarcza sprzęt do siedziby Zamawiającego w oryginalnie zapakowanych i zaplombowanych opakowaniach w ustalonym z Zamawiającym terminie.</li> <li>✓ Urządzenia po dostarczeniu podlegają przeglądowi i ocenie przez Zamawiającego w obecności przedstawiciela Wykonawcy w ustalonym z Zamawiającym terminie.</li> <li>✓ Zgodnie z ustalonym z Zamawiającym harmonogramem Wykonawca: <ul style="list-style-type: none"> <li>➤ rozmieszcza i podłącza sprzęt do wskazanych przez zamawiającego źródeł energii oraz punktów dostępowych sieci WAN/LAN znajdujących się w siedzibie Zamawiającego.</li> <li>➤ dokonuje uruchomienia, instalacji, oraz aktywacji licencji (o ile jest to wymagane).</li> </ul> </li> </ul>
Oświadczenia	<p>Zamawiający wymaga a Wykonawca oświadcza, że oferowane urządzenia sieciowe spełniają poniższe wymogi i standardy:</p> <ul style="list-style-type: none"> <li>✓ Są wyprodukowane z zachowaniem normy jakościowej ISO 9001 oraz ISO 14001 lub równoważnych środków zapewnienia jakości;</li> <li>✓ Posiadają deklarację zgodności CE;</li> <li>✓ Zamawiający wymaga a Wykonawca oświadcza, że w celu dokonania odbioru końcowego przez Zamawiającego Wykonawca złoży następujące dokumenty: <ul style="list-style-type: none"> <li>➤ Certyfikat ISO 9001:2000 producenta lub równoważny dokument zapewnienia jakości dla oferowanego urządzenia.</li> <li>➤ Certyfikat ISO 14001 producenta lub równoważny dokument zapewnienia ochrony środowiska.</li> </ul> </li> </ul>