



**Załącznik nr 1
do zapytania ofertowego**

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Oferowany sprzęt musi posiadać parametry nie gorsze niż podane w poniższym zestawieniu.

1. Serwer wraz z oprogramowanie systemowym – 1 szt.

L.p.	Parametr lub warunek	Minimalne wymagania
1	OBUDOWA	<ul style="list-style-type: none"> - Typu Rack, wysokość maksimum 2U; - Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack oraz ramieniem porządkującym ułożenie przewodów w szafie rack;
2	PŁYTA GŁÓWNA	<ul style="list-style-type: none"> - Dwuprocesorowa, wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów dwunastordzeniowych; - Minimum 6 złącz PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16 i 3 złącza o prędkości x8; - Wszystkie złącza PCI Express muszą być aktywne; - Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slotcie M.2 bez zajmowania klatek dyskowych serwera); - Zainstalowany w dedykowanym slotcie dysk SSD M.2 o pojemności minimum 150GB, DWPD minimum = 1,5;
3	PROCESORY	<ul style="list-style-type: none"> - Zainstalowany jeden procesor 8-rdzeniowy taktowany podstawowym zegarem 2,10Ghz; Musi istnieć możliwość dołożenia drugiego procesora;
4	PAMIĘĆ RAM	<ul style="list-style-type: none"> - Zainstalowane minimum 32GB typu DDR4 Registered, 2666Mhz; - Wsparcie dla technologii zabezpieczania pamięci w trybie kopii lustrzanej; - Minimum 12 gniazd pamięci RAM na płycie głównej;
5	KONTROLERY DYSKOWE, I/O	<ul style="list-style-type: none"> - Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 2GB pamięci podręcznej cache;
6	DYSKI TWARDE	<ul style="list-style-type: none"> - Zainstalowane 3 dysków 2TB 7200rpm oraz 2 SAS 12G 300GB 10K przeznaczonej do pracy ciągłej w serwerach, każdy o pojemności minimum 10TB; - Wszystkie dyski muszą być wymienne w trybie hot-plug;
7	KONTROLERY LAN	<ul style="list-style-type: none"> - Jedna dwuportowa karta 2x1Gbit/s, niezajmująca slotu PCI Express; - Dodatkowa osobna karta dwuportowa Ethernet 10Gbit/s Base-T (z negocjacją do 1Gbit/s);

8	KONTROLERY FC	Możliwość instalacji kart FC 16Gbit;
9	PORTY	<ul style="list-style-type: none"> - Zintegrowana karta graficzna ze złączem VGA; - 1x USB 3.0 dostępne na froncie obudowy; - 4x USB 3.0 dostępne z tyłu serwera; - 1x USB 3.0 wewnątrz serwera; <p>Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;</p>
10	ZASILANIE, CHŁODZENIE	<ul style="list-style-type: none"> - Redundantne zasilacze hotplug o mocy maksimum 800W, o sprawności 94% (klasa Platinum); - Redundantne wentylatory hotplug;
11	ZARZĄDZANIE	<ul style="list-style-type: none"> - Wbudowane diody informacyjne informujące o stanie serwera; - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: <ul style="list-style-type: none"> • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH); • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii; • Zarządzanie alarmami (zdarzenia poprzez SNMP); • Możliwość przejęcia konsoli tekstowej; • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM); • Sprzętowy monitoring serwera w tym stanu dysków twardej i kontrolera RAID (bez pośrednictwa agentów systemowych); • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.);
12	WSPIERANE OS	Windows 2016 Hyper-V, Windows 2012 R2 Hyper-V, VMWare, Suse, RHEL;
13	GWARANCJA	<ul style="list-style-type: none"> - Minimum 5 lat gwarancji producenta serwera w trybie onsite z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime); - Serwis musi obejmować opcję konfiguracji serwisu proaktywnego (tzw. AutoCall lub AutoHeal) – musi istnieć możliwość konfiguracji automatycznego bezpośredniego powiadomienia serwisu producenta i otwierania zgłoszenia serwisowego w przypadku usterki lub przewidywanej

		<ul style="list-style-type: none"> usterki serwera w trakcie całego okresu gwarancji; - Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; - Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera (również po zakończeniu wsparcia serwisowego producenta serwera) – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;
14	DOKUMENTACJA, INNE	<ul style="list-style-type: none"> - Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty); - Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce; - Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, (ogólnopolski numer o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardej, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji; - W celu zapewnienia odpowiedniego SLA jako element odbioru technicznego serwera wymaga się dostarczenia oświadczenia Producenta serwera iż odpowiednie dane kontaktowe uprawnionego przedstawiciela Zamawiającego zostały zgłoszone przez Wykonawcę do Producenta serwera celem możliwości konfiguracji i świadczenia proaktywnego wsparcia/kontakt w przypadku nastąpienia usterki w Polsce. (Dane zostaną podane przez Zamawiającego z minimum 14 dniowym wyprzedzeniem przed odbiorem sprzętu); - Wymagane jest oświadczenie Producenta oferowanego serwera, iż wymagany w postępowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta serwera na potrzeby oferty w niniejszym postępowaniu; - Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
15	OPROGRAMOWANIE	Microsoft Windows Server 2016 Essentials;

2. Urządzenie klasy UTM – 1 szt.

L.p.	Parametr lub warunek	Minimalne wymagania
------	----------------------	---------------------

1	OBSŁUGA SIECI	<ul style="list-style-type: none"> - Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP;
2	ZAPORA KORPORACYJNA (Firewall)	<ul style="list-style-type: none"> - Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection; - Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT; - Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge); - Interface (GUI) do konfiguracji firewalla 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 etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie; - Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia; - Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u; - Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów); - Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos);
3	INTRUSION PREVENTION SYSTEM (IPS)	<ul style="list-style-type: none"> - 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; - Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy; - Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń; - Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS; - Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej; - Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS; - Administrator urządzenia 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;
4	KSZTAŁTOWANIE PASMA (Traffic)	<ul style="list-style-type: none"> - Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma;



	Shapping)	<ul style="list-style-type: none"> - Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP; - Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring); - Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch;
5	OCHRONA ANTYWIRUSOWA	<ul style="list-style-type: none"> - Rozwiązanie ma zezwalać na zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania); - Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji; - Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym; - 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 odrzucenia;
6	OCHRONA ANTYSZPAM	<ul style="list-style-type: none"> - Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM); - Ochrona antyspam ma działać w oparciu o: <ul style="list-style-type: none"> • białe/czarne listy; • DNS RBL; • heurystyczny skaner; - W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL; - Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin;
7	WIRTUALNE SIECI PRYWANE (VPN)	<ul style="list-style-type: none"> - Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja); - Odpowiednio kanały VPN można budować w oparciu o: <ul style="list-style-type: none"> • PPTP VPN; • IPSec VPN; • SSL VPN; - SSL VPN musi działać w trybach Tunel i Portal; - W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem; - Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover); - Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf;



		- Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię Route Based;
8	FILTR DOSTĘPU DO STRON WWW	<ul style="list-style-type: none"> - Urządzenie ma posiadać wbudowany filtr URL; - Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych; - Administrator musi mieć możliwość dodawania własnych kategorii URL; - Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora; - Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST; - Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: <ul style="list-style-type: none"> • blokowanie dostępu do adresu URL; • zezwolenie na dostęp do adresu URL; • blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora; - Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony; - Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych; - Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS; - Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME; - Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane; - Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http;
9	UWIERZYTELNIANIE	<ul style="list-style-type: none"> - Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: <ul style="list-style-type: none"> • lokalną bazę użytkowników (wewnętrzny LDAP); • zewnętrzną bazę użytkowników (zewnętrzny LDAP); • usługę katalogową Microsoft Active Directory; - Rozwiązanie musi pozwalać na równoczesne użycie co najmniej 5 różnych baz LDAP; - Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia autoryzację w oparciu o protokoły: <ul style="list-style-type: none"> • SSL; • Radius; • Kerberos; - Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory; - Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta; - Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny;



10	ADMINISTRACJA ŁĄCZAMI DO INTERNETU (ISP)	<ul style="list-style-type: none"> - Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing); - Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy: <ul style="list-style-type: none"> • równoważenie względem adresu źródłowego; • równoważenie względem połączenia; - Mechanizm równoważenia łączy musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu; - Urządzenie ma posiadać mechanizm przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego; - Urządzenie ma posiadać mechanizm statycznego trasowania pakietów; - Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego; - Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP; - Rozwiązanie powinno zapewniać obsługę routingu dynamicznego w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP;
11	POZOSTAŁE USŁUGI I FUNKCJE ROZWIĄZANIA	<ul style="list-style-type: none"> - Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci; - Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay; - Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6; - Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS; - Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3; - Urządzenie musi posiadać usługę DNS Proxy;
12	ADMINISTRACJA URZĄDZENIEM	<ul style="list-style-type: none"> - Producent musi dostarczać w podstawowej licencji narzędzie administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia; - Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego; - Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https; - Komunikacja może odbywać się na porcie innym niż https (443 TCP); - Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami; - Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana; - Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https;

		<ul style="list-style-type: none"> - Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS); - Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX; - Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora; - Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora;
13	RAPORTOWANIE	<ul style="list-style-type: none"> - Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu; - System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania; - System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego; - System raportujący musi umożliwiać wygenerowanie co najmniej 5 różnych raportów; - System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu; - W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny; - Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy;
14	PARAMETRY SPRZĘTOWE	<ul style="list-style-type: none"> - Urządzenie musi być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać z wbudowanej pamięci flash; - Liczba portów Ethernet 10/100/1000Mbps – min. 8 w tym min. 3 routowalne; - Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta; - Przepustowość Firewalla – min.2 Gbps; - Przepustowość Firewalla wraz z włączonym systemem IPS – min. 1,6 Gbps; - Przepustowość filtrowania Antywirusowego – min. 300 Mbps; - Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 350 Mbps; - Maksymalna liczba tuneli VPN IPsec nie może być mniejsza niż 50; - Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż 20; - Obsługa min. VLAN 64; - Liczba równoczesnych sesji - min. 200 000 i nie mniej niż 15 000 nowych sesji/sekundę; - Urządzenie jest nielimitowane na użytkowników; - Urządzenie musi mieć wykupioną licencję Premium UTM Security Pack na 1 rok;

3. Switch – 1 szt.

Specyfikacja:

Standardy i protokoły	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE802.3z, IEEE 802.3ad, IEEE 802.3x, IEEE 802.1d, IEEE 802.1s, IEEE 802.1w, IEEE 802.1q, IEEE 802.1p, IEEE 802.1x
Porty	P-424 porty RJ45 10/100/1000Mb/s (Auto negocjacja/Auto MDI/MDIX) 4 gigabitowe sloty SFP
Okablowanie sieciowe	10BASE-T: Kabel UTP kat. 3, 4 lub 5 (do 100m) 100BASE-TX/1000Base-T: Kabel UTP kat. 5, 5e lub wyższej (do 100m) 1000BASE-X: MMF, SMF
Bezwentylatorowy	Nie - 2 wentylatory
Zasilanie	100~240VAC, 50/60Hz
Pobór mocy	Maksymalnie (PoE włączone): 264,8W (220V/50Hz) Maksymalnie (PoE wyłączony): 28,2W (220V/50Hz)
Porty PoE+ (RJ45)	Zgodność ze standardami: 802.3at/af Liczba portów PoE+: 24 Maksymalna łączna moc podłączonych urządzeń: 192W
WYDAJNOŚĆ	
Przepustowość	56Gb/s
Szybkość przekierowań pakietów	41,7Mp/s
Tablica adresów MAC	16K
Ramki jumbo	9KB
FUNKCJE OPROGRAMOWANIA	
Funkcja Quality of Service	Priorytetywanie ruchu CoS/DSCP w oparciu o standard IEEE 802.1p 8 kolejek priorytetowania Ustalenie kolejek priorytetów: SP, WRR, SP+WRR Limitowanie transmisji w zależności od portu/przepływu danych IPv6 QoS* Voice VLAN
Funkcje L2 i L2+	Routing statyczny DHCP Relay IGMP Snooping V1/V2/V3 Agregacja portów - LACP (Do 14 grup agregacji obejmujących do 8 portów każda)



PROGRAM REGIONALNY
NARODOWA STRATEGIA SPÓJNOŚCI



WOJEWÓDZTWO
WIELKOPOLSKIE



UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO



Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu państwa w ramach Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2007-2013

	STP/RSTP/MSTP LLDP, LLDP-MED Filtrowanie/ochrona BPDU Ochrona TC/Root Wykrywanie połączeń loopback Kontrola przepływu 802.3x
Sieci VLAN	jednoczesna obsługa do 4096 VLAN z 4096 identyfikatorów VLAN ID MAC/Protocol VLAN
Listy kontroli dostępu	Filtrowanie pakietów oparte o źródłowe i docelowe adresy MAC L2~L4 Adres IP, porty TCP/UDP IPv6 ACL*
Bezpieczeństwo transmisji	AAA Port Security DHCP Snooping IP-MAC-Port Binding ARP Inspection 802.1x and Radius Authentication SSH v1/v2 SSL v3/TLSv1 Broadcast/Multicast/Unknown-unicastStorm Control Dos Defend
IPv6	Podwójny stos IPv4/IPv6 MLD Snooping IPv6 ND Wykrywanie MTU ICMPv6 TCPv6/UDPv6
Zastosowania IPv6	Klient DHCPv6 Ping6 Tracert6 Telnet(v6) IPv6 SNMP IPv6 SSH IPv6 SSL Http/Https IPv6 TFTP
Zarządzanie	Interfejs przeglądarki internetowej GUI



Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu państwa w ramach Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2007-2013

	SNMP v1/v2c/v3, zgodne z publicznymi bibliotekami MIB i prywatnymi bibliotekami MIB TP-LINK RMON (grupy 1, 2, 3, 9) Monitorowanie CPU Port Mirroring Aktualizacja firmware: poprzez przeglądarkę internetową oraz TFTP Diagnostyka: test VCT Logi systemu, publiczne biblioteki MIB Dual Image
INNE	
Certyfikaty	CE, FCC, RoHS

4. UPS RACK – 1 szt.

Specyfikacja:

Zalecana wilgotność otoczenia	20,00 - 90,00 %
Długość	410,00 mm
Poziom hałas	50,00 dB
Napięcie baterii	12,00 V
Zakres częstotliwości wejściowej	- Hz
Czas ładowania baterii	4,00 H
Napięcie wejściowe	230,00 VAC
Maksymalny czas przełączania	0,00 ms
Szerokość	438,00 mm
Moc	1 600,00 W
Zalecana temperatura otoczenia	0,00 - 40,00 °C
Częstotliwość wyjściowa	50,00 Hz
Napięcie wyjściowe	230,00 V
Liczba gniazd rozszerzeń	1,00
Zakres napięcia wejściowego	- VAC
Pojemność baterii	9,00 Ah
Liczba baterii	4
Moc pozorna	2 000,00 VA
Regulacja częstotliwości wyjściowej	Sinusoida Hz
Gniazdo rozszerzeń	Tak
Oprogramowanie	ViewPower
Zabezpieczenie przeciwprzepięciowe	Tak

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu państwa w ramach Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2007-2013

Postać fali	Sinusoida
Awaryjne wyłączenie (EPO)	Tak
Zabezpieczenie przeciwprzepięciowe	Tak
Złącza USB	2.0
Obsługiwane systemy operacyjne	Windows/MAC/Linux/Unix
Gniazda wyjściowe	Tak, IEC C13 (10A)x4
CZAS ZASILANIA AWARYJNEGO	
OBCIĄŻENIE [W]	CZAS [min]
100	135
200	60
300	37
400	26
500	19
750	11,5
1000	7,8
1500	4,3
2000+	Overload

5. Urządzenie Typu NAS – 1 szt.

Specyfikacja:

Maksymalna obsługiwana pojemność	24 TB
Kieszenie na dyski	3,5" - 2 szt.
RAID	0 1 Basic Single Disk
Rodzaje wyjść / wejść	USB 3.0 - 1 szt. USB 2.0 - 2 szt. RJ-45 10/100/1000 (LAN) - 1 szt. DC-in (wejście zasilania) - 1 szt.
Procesor	Realtek RTD1295 (4 rdzenie, 1.4 GHz)
Pamięć RAM	1 GB (DDR4)
Protokoły sieciowe	AFP HTTP Klient protokołu BitTorrent Klient VPN Serwer CIFS/SMB Serwer DLNA Serwer FTP



Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu państwa w ramach Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2007-2013

	Serwer NFS Serwer VPN Serwer WWW
System plików dla dysków zewnętrznych	FAT32 NTFS HFS+ EXT3 EXT4
System plików	EXT4
Dodatkowe informacje	Dostęp przez sieć Web Licencja na 4 kamery IP Obsługa przechowywania kopii zapasowych w chmurze
Dołączone akcesoria	Zasilacz
Gwarancja	24 miesiące (gwarancja producenta)

6. Dysk Twardy – 2 szt.

Specyfikacja:

Pojemność	3000 GB
Format	3.5"
Interfejs	SATA III (6.0 Gb/s) - 1 szt.
Pamięć podręczna cache	64 MB
Prędkość obrotowa	5900 obr./min
Prędkość odczytu (maksymalna)	180 MB/s
Niezawodność MTBF	1 000 000 godz.
Dodatkowe informacje	Zgodność z systemami NAS
Gwarancja	36 miesięcy (gwarancja producenta)

7. UPS – 1 szt.

Specyfikacja:

Topologia	Online
Moc pozorna	3000 VA
Moc skuteczna	2400 W
Napięcie wejściowe	110 - 300 V
Kształt napięcia wyjściowego	Sinusoidalny
Gniazda wyjściowe	IEC - 4 szt.
Czas przełączania	4 ms
Średni czas ładowania	4 h
Interfejs komunikacyjny	RS232 USB

Projekt współfinansowany przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu państwa
w ramach Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2007-2013

Sygnalizacja pracy	Wyświetlacz LCD Dźwiękowa
Typ obudowy	Rack

8. Kabel Krosowy – 20 szt.

Specyfikacja:

Wtyk	2 x RJ45
Ośłona wtyku	zalewana
Kat.	5e, UTP
Typ połączenia	prosty 1:1 (według standardu 568B)
Żyły	26AWG x 4P linka
Izolacja i powłokazew.	PVC
Przepustowość	100-125 MHz

9. Windows 10 Pro – 7 szt.

Specyfikacja:

Wersja	Windows 10 Pro
Architektura	64-bitowa
Licencja	OEM
Liczba użytkowników	1
Liczba stanowisk	1
Wersja językowa	Polska
Nośnik	DVD

Produkty muszą zostać zainstalowane, zintegrowane i skonfigurowane zgodnie z wymaganiami Zamawiającego.