Załącznik nr 1

Zadanie 1. Dostawa, instalacja i konfiguracja urządzeń aktywnych, zasilania awaryjnego, elementów pasywnych sieci.

Spis treści

Zakres wdrożenia

Wdrożenie obejmuje:

- dostawę oraz rozładunek wszystkich zamawianych elementów wraz z wniesieniem
- instalację szaf teleinformatycznych wraz z osprzętem w serwerowniach i montaż urządzeń według potrzeb Zamawiającego
- instalacja dodatkowego osprzętu (będącego częścią zamówienia) w punktach dystrybucyjnych wskazanych przez Zamawiającego
- montaż przełączników w punktach dystrybucyjnych, podłączenie przełączników zgodnie z przedstawionym przez Zamawiającego schematem sieci
- podstawowa konfiguracja przełączników, uruchomienie protokołów VRRP oraz STP, konfiguracja wskazanych przez Zamawiającego sieci wirtualnych VLAN
- montaż oraz konfiguracja zasilaczy awaryjnych w punktach dystrybucyjnych wskazanych przez Zamawiającego
- montaż oraz konfiguracja urządzenia UTM w zakresie wskazanym przez Zamawiającego
- wstępnej konfiguracja zamówionego sprzętu UTM
- integracja z dostarczoną infrastruktura sieciową
- konfiguracja IPSec VPN
- konfiguracja polityk Firewall
- konfiguracja profili UTM
- konfiguracja dynamicznego routingu (OSPF)
- testy urządzeń UTM
- montaż oraz konfiguracja posiadanego systemu zarządzania siecią Brocade Network Advisor w zakresie wskazanym przez Zamawiającego
- montaż oraz konfiguracja punktów dostępowych w miejscach wskazanych przez Zamawiającego
- konfiguracja protokołu routingu dynamicznego wskazanego przez Zamawiającego
- zabezpieczenie dostępu do urządzeń zgodnie z polityką bezpieczeństwa politechniki
- zintegrowanie dostępu do sieci z uwierzytelnianiem użytkowników w oparciu o serwer Radius
- konfiguracja urządzeń aby wysyłały logi na zewnętrzny serwer syslog
- uruchomienia raportów, alertów, i wykresów na serwerze logów
- przygotowanie administratorów co najmniej trzech pracowników wydelegowanych przez Zamawiającego
- wykonanie szczegółowej dokumentacji technicznej wdrożonego rozwiązania informatycznego

Wszystkie oferowane przełączniki sieciowe muszą spełniać takie wymagania:

Wspólne wymagana dla przełączników sieciowych	
Przełączniki, które obowiązują poniższe wymagania	• Przełącznik szkieletowy • Przełącznik dostępowy Typu A • Przełącznik dostępowy Typu B • Przełącznik dostępowy Typu C
Zarządzanie	• W celu zapewnienia jednolitej konsoli zarządzającej, wszystkie przełączniki muszą pochodzić od jednego producenta i być zgodne z posiadanymi przez Zamawiającego przełącznikami Brocade i oprogramowaniem zarządzającym Brocade Network Advisor
Gwarancja i serwis	• Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta, • Serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu, • Na dostarczany sprzęt musi być udzielona dożywotnia gwarancja (Gwarancja typu Limited Lifetime Warranty, czyli wspieranie urządzenia do 5 lat po zakończeniu produkcji danej linii produktowej), zapewniająca wymianę urządzenia w trybie NBD, potwierdzona pisemnie przez producenta urządzenia, • Gwarancja na oprogramowanie systemowe (firmware), czyli wsparcie urządzenia zapewniające możliwość aktualizacji i korekty błędów na okres 5 lat. Gwarancja potwierdzona pisemnie przez producenta urządzenia. • Wsparcie rozszerzone przez okres min. 60 miesięcy, obejmujące

		wymianę/tymczasową podmianę urządzenia w siedzibie zamawiającego w ciągu 4 godzin od momentu zgłoszenia usterki (8x5x4h)
		• Po upływie rozszerzonego wsparcia, czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych, diagnozę usterki i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego,
		• Po upływie rozszerzonego wsparcia, usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zdiagnozowania usterki,
		• Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (od poniedziałku do piątku, w godzinach 8-17), fax, e-mail i WWW (przez całą dobę);
		• Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań;
		• Po upływie rozszerzonego wsparcia w przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę, Zamawiający dopuszcza podstawienie na czas naprawy sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki. Dostarczony sprzęt zastępczy musi zostać skonfigurowany w sposób umożliwiający mu podjęcie pracy zgodnie z poprzednią funkcją jaką pełnił w infrastrukturze,
		• Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań od poniedziałku do piątku, w godzinach 8-17,
		• Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:
		  • bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres minimum 60 m-cy,
		  • dostęp do dokumentacji sprzętu i oprogramowania,
		  • dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
		  • dostęp do pomocy technicznej producentów.
		• Dostarczone dodatkowe moduły, tj. moduły światłowodowe, zasilacze, kable stackujące, nie mogą powodować ograniczenia gwarancji na zaoferowane switche,
		• Dodatkowo w okresie 60 miesięcy obowiązywać będzie dodatkowe wsparcie techniczne opisane w SIWZ.

Przełącznik szkieletowy		
Architektura	Porty	• Minimum 24 porty 100/1000 Mbps SFP • Minimum 4 porty 10 Gbps obsługujących moduły SFP+ • Możliwość rozbudowy o 4 porty 10 Gbps obsługujące moduły SFP+ poprzez aktywację licencyjną dodatkowych portów, nie zmniejszając tym samym liczby dostępnych opisanych powyżej portów SFP • Minimum 4 porty QSFP do stackowania o przepustowości minimum 40Gbps każdy • Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management (oba interface RJ-45)
	Wydajność	• Szybkość przełączania min. 395 Mpps • Przepustowość min. 525 Gbps
	Wentylacja	• Urządzenie musi posiadać dwa redundantne moduły wentylatorów, wymienialne w trakcie pracy urządzenia • Przepływ powietrza w kierunku przód-tył lub tył-przód
	Zasilanie	• Urządzenie musi posiadać zainstalowane dwa wewnętrzne zasilacze AC. Jeden zasilacz pełni funkcję redundantnego, wymienialnego w trakcie pracy urządzenia (hot-swap), redundancja zasilaczy typu 1+1

		• Pobór mocy – max 120W (przy jednym zasilaczu) • Wsparcie sprzętowe dla IEEE 802.3az (Energy-Efficient Ethernet; EEE)
	Obudowa	• Urządzenie przystosowane do montażu w szafie teletechnicznej 19 cali • Wysokość urządzenia 1RU
Stackowanie urządzenia	Ilość urządzeń	• Możliwość stackowania minimum 8 urządzeń w jednym stosie
	Interfejs stackowania	• Minimum 4 porty QSFP do stackowania, każdy o szybkości min. 40Gbps
	Wydajność w stosie	• Przepustowość min. 320Gbps (full duplex)
	Funkcje dodatkowe	• Hitless failover w przypadku awarii przełącznika typu master w stosie • Możliwość dodania i usunięcia urządzenia ze stosu bez przerywania pracy stosu
Funkcjonalność warstwy II	Tablica MAC	• Urządzenie musi obsługiwać min. 32000 adresów MAC
	Ilość VLAN	• Urządzenie musi obsługiwać min. 4096 sieci VLAN
	Obsługiwane protokoły	• Wsparcie dla 802.1s Multiple Spanning Tree oraz PVST/PVST+/PVRST • Wsparcie dla 802.1x • Obsługa IGMP snooping (v1/v2/v3) • Obsługa Dynamic Voice VLAN Assignment • Obsługa Link Fault Signaling (LFS) • Obsługa MLD Snooping (v1/v2) • Obsługa Multi-device Authentication • Obsługa mechanizmu MAC Address Locking; Port Security • Port-based Access Control Lists • Single-instance Spanning Tree • Single-link LACP • Uni-Directional Link Detection (UDLD) • Minimalny rozmiar obsługiwanych ramek typu Jumbo – 9000 bajtów • Obsługa do 254 instancji STP
	Trunking	• Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad • Minimalna liczba portów dla jedno logiczne połączenie: 8 • Minimalna liczba jednoczesnych grup trunkowych: 120
Funkcjonalność warstwy III	Obsługiwane protokoły	• Statyczny routing dla IPv4 i IPv6 • Obsługa routingu multicastów, PIM (PIM–DM i PIM-SM, PIM-SSM) • Obsługa Policy Based Routing • Obsługa protokołu RIP v2 i RIPng • Obsługa protokołu OSPF v2, OSPF v3(IPv6) • Obsługa protokołu VRRP, VRRPv3 dla IPv6 • ECMP
	Możliwość rozbudowy	• Opcjonalna możliwość obsługi protokołu BGP (po wykupieniu licencji, bez wymiany sprzętu)
	Tablica routingu	• Obsługa do 16000 wpisów routingu w urządzeniu
	DHCP	• DHCP relay • DHCP server

Mechanizmy bezpieczeństwa	Listy dostępowe	• Limitowanie ruchu wejściowego na każdym porcie w oparciu o listy ACL • Obsługa ACL zarówno dla IPv4 jak i dla IPv6 • Możliwość konfiguracji mirroringu w oparciu o listy ACL MAC Filter-based i VLAN-based
	Inne	• Obsługa Private VLAN • Limitowanie ruchu dla pakietów typu Broadcast/Multicast/ unknown traffic • Wsparcie sprzętowe dla MacSec
Zarządzanie ruchem	QOS	• Obsługa co najmniej 8 kolejek QoS na jednym porcie fizycznym • Obsługa algorytmu Weighted Round Robin (WRR) • Obsługa algorytmu Strict Priotity (SP) • Mapowanie za pomocą ACL do kolejki priorytetowej • Mapowanie na podstawie adresu MAC do kolejki priorytetowej • Limitowanie pasma na wejściu w oparciu o ACL • Limitowanie pasma na wyjściu na porcie fizycznym dla określonej kolejki • Wsparcie dla DHCP Relay • Wsparcie dla Diffserv oraz DSCP
Wyposażenie dodatkowe		• 4 modułów 10GBase-SR, SFP+ LC, MMF • 2 moduły 1000Base-SX, SFP LC, MMF • kabel do łączenia urządzenia w stos, tego samego producenta, co urządzenie
UWAGA:		• W miejsce stosu przełączników (dwóch zamawianych urządzeń) Zamawiający dopuszcza zastosowanie urządzenia typu modularnego z dwoma kartami typu management oraz modułami: • 2 x minimum 24 porty 100/1000 Mbps SFP • 2 x minimum 8 portów 10 Gbps SFP+ • Urządzenie musi posiadać również dwie matryce przełączające oraz dwa zasilacze. Wysokość urządzenia nie może przekraczać 6RU. Pozostałe wymagania pozostają bez zmian

Przełącznik dostępowy Typu A		
Architektura	Porty	• Minimum 48 portów 10/100/1000 Mbps RJ-45 • Minimum 4 porty typu combo (pracujące jako porty 10/100/1000 RJ-45 lub jako porty światłowodowe 1Gbps) • Minimum 2 porty 10 Gbps obsługujące moduły XFP lub SFP+ • Minimum 2 porty CX4 do stackowania o przepustowości minimum 16 Gbps każdy • Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management
	Wydajność	• Szybkość przełączania min. 150 Mpps • Przepustowość min. 200 Gbps
	Wentylacja	• Urządzenie musi posiadać moduł wentylacji • Przepływ powietrza w kierunku przód-tył lub tył-przód • Urządzenie musi posiadać automatyczną kontrolę szybkości wentylatorów w zależności od temperatury • Wymienny moduł wentylatorów

	Zasilanie	• Urządzenie musi posiadać możliwość zainstalowania dwóch wewnętrznych zasilaczy redundantnych, wymienialnych w trakcie pracy urządzenia - hot-swap, redundancja zasilaczy typu 1+1 • Minimum jeden zainstalowany zasilacz AC • Maksymalny pobór mocy (przy jednym zasilaczu) – 125W
	Obudowa	• Urządzenie przystosowane do montażu w szafie teletechnicznej 19 cali • Wysokość urządzenia 1RU
Stackowanie urządzenia	Ilość urządzeń	• Możliwość stackowania minimum 8 urządzeń w jednym stosie
	Interfejs stackowania	• Minimum 2 porty CX4 do stackowania, każdy o szybkości min. 16 Gbps
	Wydajność w stosie	• Przepustowość min. 64 Gbps (full duplex)
	Funkcje dodatkowe	• Hitless failover w przypadku awarii przełącznika typu master w stosie • Możliwość dodania i usunięcia urządzenia ze stosu bez przerywania pracy stosu
Funkcjonalność warstwy II	Tablica MAC	• Urządzenie musi obsługiwać min. 32000 adresów MAC
	Ilość VLAN	• Urządzenie musi obsługiwać min. 4096 sieci VLAN
	Obsługiwane protokoły	• Wsparcie dla 802.1s Multiple Spanning Tree oraz PVST/PVST+/PVRST • Wsparcie dla 802.1x • Obsługa IGMP snooping (v1/v2/v3) • Obsługa Dynamic Voice VLAN Assignment • Obsługa Link Fault Signaling (LFS) • Obsługa MLD Snooping (v1/v2) • Obsługa Multi-device Authentication • Obsługa MAC Address Locking • Port-based Access Control Lists • Single-instance Spanning Tree • Single-link LACP • Uni-Directional Link Detection (UDLD) • Minimalny rozmiar obsługiwanych ramek typu Jumbo – 9000 bajtów • Obsługa do 254 instancji STP • Obsługa protokołu CDP (Cisco Discovery Protocol)
	Trunking	• Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad • Minimalna liczba portów na jedno logiczne połączenie: 8 • Minimalna liczba jednoczesnych grup trunkowych: 56
Funkcjonalność warstwy III	Routing	• Statyczny routing dla IPv4 • Statyczny routing dla IPv6
	Tablica routingu	• Obsługa do 16000 wpisów routingu w urządzeniu
	Wspierane protokoły	• Obsługa routingu multicastów, PIM (PIM–DM i PIM-SM, PIM-SSM) • Obsługa Policy Based Routing • Obsługa protokołu RIP v2 oraz RIPng • Obsługa protokołu OSPF v2 i OSPFv3 • Obsługa protokołu VRRP • ECMP
	Możliwość rozbudowy	• Opcjonalna możliwość obsługi protokołu BGP (po wykupieniu licencji, bez wymiany sprzętu)

	DHCP	• DHCP relay • DHCP server
Mechanizmy bezpieczeństwa	Listy dostępowe	• Limitowanie ruchu wejściowego na każdym porcie w oparciu o listy ACL • Możliwość konfiguracji mirroringu w oparciu o listy ACL MAC Filter-based i VLAN-based
	Inne	• Obsługa Private VLAN • Limitowanie ruchu dla pakietów typu Broadcast/Multicast/ unknown traffic
Zarządzanie ruchem	QOS	• Obsługa co najmniej 8 kolejek QoS na jednym porcie fizycznym • Algorytm Weighted Round Robin (WRR) • Algorytm Strict Priotity (SP) • Mapowanie za pomocą ACL do kolejki priorytetowej • Mapowanie na podstawie adresu MAC do kolejki priorytetowej • Limitowanie pasma na wejściu w oparciu o ACL • Limitowanie pasma na wyjściu na porcie fizycznym dla określonej kolejki • Obsługa DHCP Relay • Obsługa Diffserv oraz DSCP
Dodatkowa funkcjonalność		• Wsparcie dla SNMPv2c/v3, SSHv2 oraz RADIUS, TACACS i TACACS+ • Funkcjonalność sFlow zgodnie z RFC 3176 umożliwiająca monitorowanie ruchu w warstwach 2 do 4 modelu OSI • Funkcjonalność sFlow wspomagana sprzętowo (sprzętowy agent protokołu sFlow)
Wyposażenie dodatkowe		• 2 moduły 10GBase-SR, XFP/SFP+ LC, MMF • Minimum jeden dedykowany kabel do łączenia urządzenia w stos, tego samego producenta, co urządzenie

Przełącznik dostępowy Typu B		
Architektura	Porty	• Minimum 48 portów 10/100/1000Mbps RJ-45 • Minimum 4 porty combo (pracujące jako porty 10/100/1000 RJ-45 lub jako porty światłowodowe 1Gbps) • Minimum 2 porty CX4 do stackowania o przepustowości minimum 16 Gbps każdy • Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management • Możliwość rozbudowy o minimum 2 porty 10 Gbps obsługujące moduły XFP lub SFP+
	Wydajność	• Szybkość przełączania min. 150 Mpps • Przepustowość min. 200 Gbps
	Wentylacja	• Urządzenie musi posiadać moduł wentylacji • Przepływ powietrza w kierunku przód-tył lub tył-przód • Urządzenie musi posiadać automatyczną kontrolę szybkości wentylatorów w zależności od temperatury • Wymienny moduł wentylatorów
	Zasilanie	• Minimum jeden zainstalowany zasilacz AC dostarczony przez producenta

		urządzenia • Urządzenie musi posiadać możliwość zainstalowania dwóch wewnętrznych zasilaczy redundantnych, wymienialnych w trakcie pracy urządzenia - hot-swap, redundancja zasilaczy typu 1+1 • Maksymalny pobór mocy (przy jednym zasilaczu) – 125W
	Obudowa	• Urządzenie przystosowane do montażu w szafie teletechnicznej 19 cali • Wysokość urządzenia 1RU
Stackowanie urządzenia	Ilość urządzeń	• Możliwość stackowania minimum 8 urządzeń w jednym stosie
	Interfejs stackowania	• Minimum 2 porty CX4 do stackowania, każdy o szybkości min. 16 Gbps
	Wydajność w stosie	• Przepustowość min. 64 Gbps (full duplex)
	Funkcje dodatkowe	• Hitless failover w przypadku awarii przełącznika typu master w stosie • Możliwość dodania i usunięcia urządzenia ze stosu bez przerywania pracy stosu
Funkcjonalność warstwy II	Tablica MAC	• Urządzenie musi obsługiwać min. 32000 adresów MAC
	Ilość VLAN	• Urządzenie musi obsługiwać min. 4096 sieci VLAN
	Obsługiwane protokoły	• Wsparcie dla 802.1s Multiple Spanning Tree oraz PVST/PVST+/PVRST • Wsparcie dla 802.1x • Obsługa IGMP snooping (v1/v2/v3) • Obsługa Dynamic Voice VLAN Assignment • Obsługa Link Fault Signaling (LFS) • Obsługa MLD Snooping (v1/v2) • Obsługa Multi-device Authentication • Obsługa MAC Address Locking • Port-based Access Control Lists • Single-instance Spanning Tree • Single-link LACP • Uni-Directional Link Detection (UDLD) • Minimalny rozmiar obsługiwanych ramek typu Jumbo – 9000 bajtów • Obsługa do 254 instancji STP • Obsługa protokołu CDP (Cisco Discovery Protocol)
	Trunking	• Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad • Minimalna liczba portów na jedno logiczne połączenie: 8 • Minimalna liczba jednoczesnych grup trunkowych: 56
Funkcjonalność warstwy III	Routing	• Statyczny routing dla IPv4 • Statyczny routing dla IPv6
	Tablica routingu	• Obsługa do 16000 wpisów routingu w urządzeniu
	Wspierane protokoły	• Obsługa routingu multicastów, PIM (PIM–DM i PIM-SM, PIM-SSM) • Obsługa Policy Based Routing • Obsługa protokołu RIP v2 oraz RIPng • Obsługa protokołu OSPF v2 i OSPFv3 • Obsługa protokołu VRRP • ECMP
	Możliwość rozbudowy	• Opcjonalna możliwość obsługi protokołu BGP (po wykupieniu licencji, bez wymiany sprzętu)

	DHCP	• DHCP relay • DHCP server
Mechanizmy bezpieczeństwa	Listy dostępowe	• Limitowanie ruchu wejściowego na każdym porcie w oparciu o listy ACL • Możliwość konfiguracji mirroringu w oparciu o listy ACL MAC Filter-based i VLAN-based
	Inne	• Obsługa Private VLAN • Limitowanie ruchu dla pakietów typu Broadcast/Multicast/ unknown traffic
Zarządzanie ruchem	QOS	• Obsługa co najmniej 8 kolejek QoS na jednym porcie fizycznym • Algorytm Weighted Round Robin (WRR) • Algorytm Strict Priotity (SP) • Mapowanie za pomocą ACL do kolejki priorytetowej • Mapowanie na podstawie adresu MAC do kolejki priorytetowej • Limitowanie pasma na wejściu w oparciu o ACL • Limitowanie pasma na wyjściu na porcie fizycznym dla określonej kolejki • Obsługa DHCP Relay • Obsługa Diffserv oraz DSCP
Dodatkowa funkcjonalność		• Wsparcie dla SNMP v2c/v3, SSHv2 oraz RADIUS, TACACS i TACACS+ • Funkcjonalność sFlow zgodnie z RFC 3176 umożliwiająca monitorowanie ruchu w warstwach 2 do 4 modelu OSI • Funkcjonalność sFlow wspomagana sprzętowo (sprzętowy agent protokołu sFlow)
Wyposażenie dodatkowe		• 4 moduły 1000Base-SX, SFP LC, MMF • Minimum jeden dedykowany kabel do łączenia urządzenia w stos, tego samego producenta, co urządzenie

Przełącznik dostępowy Typu C PoE		
Architektura	Porty	• Minimum 24 portów 10/100/1000Mbps RJ-45 PoE+ • Minimum 4 porty 1 GbE SFP z możliwością licencyjnego upgrade'u dwóch z nich do portów 10 GbE SFP+ • Przełącznik musi posiadać dedykowany port konsoli oraz dedykowany port typu out-of-band management
	Wydajność	• Szybkość przełączania min. 95 Mpps • Przepustowość min. 120 Gbps
	Zasilanie	• Minimum jeden zainstalowany zasilacz AC dostarczony przez producenta urządzenia • Maksymalny pobór mocy (przy jednym zasilaczu) – 400W
	Obudowa	• Urządzenie przystosowane do montażu w szafie teletechnicznej 19 cali • Wysokość urządzenia 1RU
Stackowanie urządzenia	Ilość urządzeń	• Możliwość stackowania minimum 8 urządzeń w jednym stosie
	Wydajność w stosie	• Przepustowość min. 40Gbps (full duplex)
	Funkcje dodatkowe	• Hitless failover w przypadku awarii przełącznika typu master w stosie • Możliwość dodania i usunięcia urządzenia ze stosu bez przerywania pracy stosu

Funkcjonalność warstwy II	Tablica MAC	• Urządzenie musi obsługiwać min. 16000 adresów MAC
	Ilość VLAN	• Urządzenie musi obsługiwać min. 4096 sieci VLAN
	Obsługiwane protokoły	• Wsparcie dla 802.1s Multiple Spanning Tree oraz PVST/PVST+/PVRST • Wsparcie dla 802.1x • Obsługa IGMP snooping (v1/v2/v3) • Obsługa Dynamic Voice VLAN Assignment • Obsługa Link Fault Signaling (LFS) • Obsługa MLD Snooping (v1/v2) • Obsługa Multi-device Authentication • Obsługa MAC Address Locking • Port-based Access Control Lists • Single-instance Spanning Tree • Single-link LACP • Uni-Directional Link Detection (UDLD) • Minimalny rozmiar obsługiwanych ramek typu Jumbo – 9000 bajtów • Obsługa do 250 instancji STP • Obsługa protokołu CDP (Cisco Discovery Protocol)
	Trunking	• Urządzanie musi wspierać wielokrotne połączenia w oparciu o standard IEEE 802.3ad • Minimalna liczba portów dla jedno logiczne połączenie: 8 • Minimalna liczba jednoczesnych grup trunkowych: 56
Funkcjonalność warstwy III	Routing	• Statyczny routing dla IPv4 • Statyczny routing dla IPv6
	Tablica routingu	• Obsługa do 10000 wpisów routingu w urządzeniu
	Możliwość rozbudowy	• Opcjonalna możliwość obsługi protokołów BGP, RIP v1/v2, OSPF v2, VRRP (po wykupieniu licencji, bez wymiany sprzętu)
	DHCP	• DHCP relay • DHCP server
Mechanizmy bezpieczeństwa	Listy dostępowe	• Limitowanie ruchu wejściowego na każdym porcie w oparciu o listy ACL • Możliwość konfiguracji mirroringu w oparciu o listy ACL MAC Filter-based i VLAN-based
	Inne	• Obsługa Private VLAN • Limitowanie ruchu dla pakietów typu Broadcast/Multicast/unknown traffic
Zarządzanie ruchem	QOS	• Obsługa co najmniej 8 kolejek QoS na jednym porcie fizycznym • Algorytm Weighted Round Robin (WRR) • Algorytm Strict Priotity (SP) • Mapowanie za pomocą ACL do kolejki priorytetowej • Mapowanie na podstawie adresu MAC do kolejki priorytetowej • Limitowanie pasma na wejściu w oparciu o ACL • Limitowanie pasma na wyjściu na porcie fizycznym dla określonej kolejki • Obsługa DHCP Relay • Obsługa Diffserv oraz DSCP

Dodatkowa funkcjonalność		• Wsparcie dla SNMPv2c/v3, SSHv2 oraz RADIUS, TACACS i TACACS+ • Funkcjonalność sFlow zgodnie z RFC 3176 umożliwiająca monitorowanie ruchu w warstwach 2 do 4 modelu OSI • Funkcjonalność sFlow wspomagana sprzętowo (sprzętowy agent protokołu sFlow) • 24 porty PoE Class 3 lub 12 portów PoE+
Wyposażenie Dodatkowe		• 4 moduły 1000Base-SX, SFP LC, MMF

Punkt Dostępowy WLAN
• musi być zasilany poprzez kabel sygnałowy Ethernet zgodnie ze standardem IEEE 802.3af lub 802.3at
• musi posiadać dwa moduły radiowe w standardzie 802.11a/b/g/n/ac
• musi posiadać fabryczną możliwość zastosowania linki zabezpieczającej przed kradzieżą
• musi być zarządzany z dedykowanego kontrolera bezprzewodowego, tego samego producenta
• musi wspierać tryb, w którym z punktu widzenia użytkownika grupa access-pointów rozgłaszająca daną sieć bezprzewodową jest widziana jako pojedyncze urządzenie (BSSID) dla pasma 2,4 GHz lub 5GHz
• interfejsy radiowe muszą mieć możliwość pracy w trybie MIMO 3x3, z 3 strumieniami przestrzennymi i prędkością transmisji na poziomie do 1300 Mbps przy wykorzystaniu standardu 802.11ac i kanału o szerokości 80 MHz
• musi posiadać dookólne zewnętrzne anteny dwu-zakresowe o wzmocnieniu minimum 3 dBi dla 2,4GHz i 5 GHz.
• musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji.
Ze względu na rozbudowę istniejącej infrastruktury, która pozwala na uzyskanie dostępu do sieci bezprzewodowej i przewodowej bez konieczności kontaktowania się z lokalnymi administratorami, instytucje biorące udział w projekcie zobowiązują się do przestrzegania wspólnej polityki bezpieczeństwa i do ufania informacjom przekazywanym z innych instytucji włączonych w system. Zamawiający wymaga dostarczenia urządzenia zgodnego z MERU AP832e.

System Zabezpieczeń UTM
Minimalne wymagane parametry
System zabezpieczeń musi być dostarczony jako dedykowane urządzenie zabezpieczeń sieciowych (appliance).
System zabezpieczeń nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
System zabezpieczeń firewall musi dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub bridge.
Urządzenie zabezpieczeń musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/1000 oraz 4 portami 10 GbE SFP+.
Musi istnieć możliwość rozbudowy urządzenia o minimum 8 interfejsów optycznych 1 GbE (SFP) za pomocą instalowanego modułu.
System zabezpieczeń musi umożliwiać tworzenie minimum 230 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q.
W ramach dostarczonego systemu zabezpieczeń muszą być realizowane wszystkie z poniższych funkcjonalności: – Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. – Ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS). – Poufność danych - IPSec VPN oraz SSL VPN. – Ochrona przed atakami - Intrusion Prevention System [IPS/IDS]. – Kontrola stron Internetowych – Web Filter [WF]. – Kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP). – Kontrola pasma oraz ruchu [QoS i Traffic shaping]. – Kontrola aplikacji oraz rozpoznawanie ruchu P2P.

– Możliwość analizy ruchu szyfrowanego SSL'em. Musi istnieć możliwość rozbudowy systemu o ochronę przed atakami na serwery webowe i aplikacji [WAF].
Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż 22 Gbps dla kontroli firewall.
Urządzenie zabezpieczeń musi obsługiwać nie mniej niż 2 500 000 jednoczesnych połączeń oraz 120 000 nowych połączeń na sekundę.
Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż 3.1 Gbps dla kontroli antywirus.
Urządzenie zabezpieczeń musi posiadać przepływność nie mniej niż 6.5 Gbps dla kontroli IPS.
Wydajność szyfrowania AES, nie mniej niż 2 Gbps.
W zakresie realizowanych funkcjonalności VPN, wymagane jest nie mniej niż: – Tworzenie połączeń w topologii Site-to-site oraz możliwość definiowania połączeń Client-to-site. – Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. – Rozwiązanie powinno wspierać lokalne i zewnętrzne centra certyfikacji. – Praca w topologii Hub and Spoke oraz Mesh. – Obsługa mechanizmów: IPSec NAT Traversal, DPD.
System zabezpieczeń musi zapewniać: obsługę Policy Routingu, routing statyczny i dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP.
System zabezpieczeń musi zapewniać translację adresów NAT adresu źródłowego i NAT adresu docelowego.
Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględniać adresy IP, adresy MAC, interfejsy, protokoły, usługi sieciowe, użytkowników, rejestrowanie zdarzeń oraz zarządzanie pasmem sieci (m.in. pasmo gwarantowane i maksymalne, priorytety).
System zabezpieczeń musi wspierać obsługę modemów 3G/4G. Modemy powinny pochodzić od dowolnie wybranych producentów.
System zabezpieczeń musi umożliwiać tworzenie wydzielonych stref bezpieczeństwa Firewall np. DMZ.
System musi umożliwiać automatyczne przełączanie na inne łącze w przypadku awarii podstawowego łącza. System musi wspierać podłączenie co najmniej trzech niezależnych łącz.
W ramach ochrony IPS system musi: – Opierać się, co najmniej na analizie protokołów i sygnatur. Baza wykrywanych ataków musi zawierać, co najmniej 4000 wpisów. – Pozwalać na definiowanie własnych wyjątków lub sygnatur. – Wykrywać anomalie protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos. – Pozwalać administratorowi na włączanie i wyłączanie określonych sygnatur w celu zminimalizowania opóźnień w przesyłaniu pakietów. – Generować alerty w przypadku prób ataków.
W zakresie kontroli aplikacji oraz rozpoznawania ruchu P2P wymagane jest co najmniej: – Kontrola ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. – Baza rozpoznawanych aplikacji musi zawierać co najmniej 2000 wpisów. – Blokowanie komunikatorów internetowych przynajmniej: GG (dawne Gadu-Gadu) w wersji klienckiej i webowej, Skype, Gmail Web Chat, Facebook Chat). – Blokowanie mediów strumieniowych przynajmniej: YouTube, Vimeo, radio internetowe. – Blokowanie uruchamiania aplikacji i gier w serwisie Facebook. – Blokowanie aplikacji proxy przynajmniej: TOR, Ultrasurf, JAP. – Blokowanie aplikacji P2P przynajmniej: Gnutella, BitTorrent, uTorrent, eMule. – Przydzielanie polityki QoS dla kategorii aplikacji np. komunikatory i dla konkretnej aplikacji np. Skype.
W zakresie kontroli stron internetowych system musi: – Zapewniać bazę filtra WWW o wielkości, co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne – minimum 46 kategorii. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków i reguł omijania filtra WWW. – Umożliwiać definiowanie polityk dostępu do stron internetowych w oparciu o harmonogramy czasowe dla użytkowników i grup użytkowników. – Wyświetlać komunikat użytkownikom wyjaśniający powód zablokowania dostępu do strony internetowej. Administrator musi mieć możliwość personalizacji treści komunikatu i dodania logo organizacji. – Umożliwiać przydzielanie polityki QoS dla kategorii stron internetowych np. portale społecznościowe.
System zabezpieczeń w ramach funkcji Antyspam musi udostępniać kwarantannę antyspamową, która jest obsługiwana przez użytkowników (co najmniej w zakresie zwalniania wiadomości).
System zabezpieczeń musi zapewniać automatyczne ściąganie sygnatur ataków, aplikacji, szczepionek antywirusowych.
System zabezpieczeń musi umożliwiać wykonywanie uwierzytelniania tożsamości użytkowników za pomocą nie mniej niż: – Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. – Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. – Rozwiązanie musi umożliwiać budowę architektury uwierzytelniania typu Single Sign On w środowisku Active Directory. – Rozwiązanie musi zapewniać wsparcie dla uwierzytelniania w środowiskach Microsoft Terminal Server i Citrix.
Poszczególne elementy oferowanego systemu zabezpieczeń muszą posiadać następujące certyfikaty:

– ICSA lub EAL4 – dla funkcjonalności Firewall. – ICSA lub Checkmark – dla wszystkich wymienionych funkcjonalności: antywirus, antyspam, IPS, Web Filter, VPN.
Elementy systemu muszą mieć możliwość zarządzania lokalnego (HTTPS, SSH) jak i współpracować z dedykowanymi do centralnego zarządzania i monitorowania platformami. Komunikacja systemów zabezpieczeń z platformami zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
System zabezpieczeń firewall musi posiadać wbudowany twardy dysk do przechowywania logów i raportów o pojemności nie mniejszej niż 120 GB. Wszystkie narzędzia monitorowania, analizy logów i raportowania muszą być dostępne lokalnie na urządzeniu zabezpieczeń. Nie jest wymagany do tego celu zakup zewnętrznych urządzeń, oprogramowania ani licencji.
System zabezpieczeń musi zawierać moduł logowania zdarzeń i raportowania. W ramach modułu raportowania system musi zapewniać: – Składowanie oraz archiwizację logów – Gromadzenie informacji o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz powiązanie ich z nazwami użytkowników – Monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników – Przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących – Generowanie raportów na zgodność z normami: HIPAA, SOX, PCI – Eksport raportów do plików PDF i HTML – Eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych)
W ramach zarządzania system zabezpieczeń musi: – Umożliwiać tworzenie kont administracyjnych o różnych uprawnieniach. – Automatycznie wylogować administratora po określonym czasie bezczynności. – Umożliwiać określanie złożoności polityk hasłowych dla administratorów. – Wspierać SNMP v1, v2 i v3. – Monitorować na bieżąco stan urządzenia (obciążenie interfejsów sieciowych, CPU, pamięć RAM). – Przechowywać przynajmniej dwie wersje firmware. – Wykonywać automatycznie kopie zapasowe konfiguracji systemu.
Dostawca musi dostarczyć licencje aktywacyjne dla wszystkich opisanych funkcji bezpieczeństwa na okres 60 miesięcy
System zabezpieczeń musi być objęty gwarancją producenta na okres 60 miesięcy, z czasem reakcji do 6h.
Wyposażenie dodatkowe: 4 moduły 10GBase-SR, XFP/SFP+ LC, MMF
Ze względu na rozbudowę istniejącej infrastruktury, Zamawiający wymaga dostarczenia urządzenia zgodnego z CR750iNG-XP.

Zasilacze awaryjne UPS

UPS'y muszą współpracować z posiadanym przez zamawiającego oprogramowaniem do wirtualizacji (VMware vSphere 5) na poziomie, który umożliwi w wyniku zaniku napięcia na wyłączenie wirtualnych hostów i fizycznych maszyn – wymagane skonfigurowanie w/w funkcjonalności na wszystkich serwerach fizycznych w farmie (3 szt.). Funkcjonalność ta musi być zrealizowana za pomocą sieci Ethernet.

Wszystkie zaoferowane i dostarczone UPS'y muszą posiadać takie cechy wspólne:
• UPS w technologii on-line
• Automatyczny wewnętrzny tor obejściowy. Zasilanie sieciowe dla podłączonego obciążenia na wypadek przeciążenia lub usterki zasilacza UPS.
• W razie potrzeby pozwala na szybkie rozszerzenie o dodatkowy zestaw baterii, wydłużający czas podtrzymania.
• Maksymalizacja wydajności, czasu eksploatacji i niezawodności akumulatorów dzięki inteligentnemu ładowaniu precyzyjnemu.
• Zasilanie bezprzerwowe. Akumulatory wymienialne przez użytkownika "na gorąco" bez przerywania pracy systemu
• Automatyczne włączenie UPS-a po powrocie zasilania. Automatycznie uruchamia podłączony sprzęt w momencie wznowienia zasilania z sieci miejskiej.
• Wydłużenie czasu eksploatacji akumulatorów przez regulację napięcia ładowania w zależności od temperatury

akumulatora.
• Zdalne zarządzanie UPS-em przez sieć Ethernet.
• Scentralizowane zarządzanie UPS-ami poprzez specjalistyczne oprogramowanie dołączone wraz z urządzeniami.
• Gniazdo kart do zarządzania.
• Szybkie raportowanie stanu urządzenia i zasilania za pomocą wizualnych wskaźników LED.
• Zarządzanie zasilaczem UPS przez port szeregowy.
• Akumulatory zewnętrzne typu plug-and-play umożliwiające niezakłócone, nieprzerwane zasilanie urządzeń podczas operacji wydłużania czasu pracy zasilacza UPS.
• Szyny do montażu w szafie przemysłowej 19”
• Oprogramowanie sprzętowe w pamięci flash z możliwością uaktualniania. Uaktualnienia oprogramowania sprzętowego mogą być instalowane zdalnie przy użyciu FTP.
• Automatyczny test akumulatora.
• Wczesne ostrzeganie o nieprawidłowościach umożliwia proaktywną wymianę komponentów.
• Powiadomienie o rozłączeniu akumulatora.
• Alarmy dźwiękowe, które zapewniają powiadamianie o zmieniających się warunkach zasilania z sieci miejskiej i z UPS-a.
• Regulacja częstotliwości i napięcia realizowana dzięki funkcji korygowania stanów nieprawidłowej częstotliwości i napięcia bez użycia akumulatorów.
• Filtrowanie napięcia chroniące podłączone urządzenia przed przepięciami, impulsami elektrycznymi, uderzeniami pioruna i innymi zakłóceniami zasilania.
• Korekcja wejściowego współczynnika poboru mocy.
• Kompatybilny z generatorem.
• Możliwość zimnego startu.
• Wyłącznik obwodu z możliwością resetu, bez potrzeby wymieniania bezpieczników.
• Do każdego UPS-a dołączone zostanie: CD z oprogramowaniem, wsporniki montażowe do szaf przemysłowych, kabel do sygnalizacji RS-232, Podręcznik użytkownika, oprogramowanie zarządzające.
• Potwierdzenia zgodności: Znak C,CE,EN 50091-1,EN 50091-2,EN 55022 klasa A,EN 60950,EN 61000-3-2,GOST,VDE

• **Gwarancja realizowana w miejscu instalacji sprzętu:**
  • 36 miesięcy serwisu obejmującego naprawę lub wymianę zasilacza
  • 24 miesiące serwisu obejmującego naprawę lub wymianę akumulatora

Szczególne wymagania:

Zasilacz awaryjny UPS 5000 VA		
Architektura	Typ urządzenia	Zasilacz typu on-line
	Montaż	Szyny do montażu w szafie teletechnicznej 19 cali
Wyjście	Moc wyjściowa	Minimum 3500W / 5000 VA
	Napięcie wyjściowe	Konfigurowalne dla 220 : 230 lub 240
	Częstotliwość na wyjściu	50/60 Hz +/-3 Hz z regulacją w zakresie +/-0,1
	Współczynnik szczytu	3:1
	Typ przebiegu	sinusoida
	Gniazda wyjściowe	• Minimum 8 x IEC 320 C13 • Minimum 2 x IEC 320 C19 • Minimum 4 x IEC Jumpers
	Układ obejściowy (bypass)	Wewnętrzny bypass (automatyczny i manualny)
	Wydajność przy pełnym obciążeniu	min. 92%
	Zniekształcenia napięcia wyjściowego	max 3%
Wejście	Napięcie wejściowe	230V
	Częstotliwość na wejściu	50/60 Hz +/- 5 Hz (autodetekcja)

	Typ gniazda wejściowego	Hard Wire 3-wire (wymagane podłączenie do przygotowanego przyłącza)
	Zakres napięcia wejściowego	160 - 280V
	Zmienny zakres napięcia wejściowego	100 - 280V
Akumulator	Typ akumulatora	Bezobsługowe baterie
	Typowy czas pełnego ładowania akumulatora	Maksymalnie 2,5 godziny
Zarządzanie	Port komunikacyjny	DB9 RS-232, RJ-45 10/100 Base-T Gniazdo montażu kart rozszerzeń
	Zainstalowane karty zarządzające	Tak. Zarządzająca karta sieciowa wraz z możliwością monitorowania warunków z urządzeń zewnętrznych
	Panel przedni	Diody LED wskazujące pracę z sieci : pracę z baterii : stan wymiany baterii : stanu przeciążenia oraz pracy w trybie "Bypass"
	Alarm dźwiękowy	Alarm podczas pracy na baterii sygnalizujący: znaczny stan wyczerpania baterii, ciągły sygnał dźwiękowy w stanie przeciążenia
	Awaryjny wyłącznik zasilania	Tak
Wymiary	Maksymalna głębokość	670 mm
	Maksymalna szerokość	432 mm
	Wysokość w szafie przemysłowej	Max. 3U
	Ciężar netto	Max. 55 kg
	Poziom hałasu	W odległości 1 m od powierzchni urządzenia max 55 dBA
Środowisko	Odprowadzanie ciepła	max. 1100 BTU/godz
	Zgodność środowiskowa	RoHS 7b Exemption

Zasilacz awaryjny UPS 6000 VA		
Architektura	Typ urządzenia	Zasilacz typu on-line
	Montaż	Szyny do montażu w szafie teletechnicznej 19 cali
Wyjście	Moc wyjściowa	Minimum 4200W / 6000 VA
	Napięcie wyjściowe	Konfigurowalne dla 220 : 230 lub 240
	Częstotliwość na wyjściu	50/60 Hz +/-3 Hz z regulacją w zakresie +/-0,1
	Współczynnik szczytu	3:1
	Typ przebiegu	sinusoida
	Gniazda wyjściowe	• Minimum 8 x IEC 320 C13 • Minimum 2 x IEC 320 C19 • Minimum 4 x IEC Jumpers
	Układ obejściowy (bypass)	Wewnętrzny bypass (automatyczny i manualny)
	Wydajność przy pełnym obciążeniu	min. 92%
	Zniekształcenia napięcia wyjściowego	max 3%
Wejście	Napięcie wejściowe	230V
	Częstotliwość na wejściu	50/60 Hz +/- 5 Hz (autodetekcja)
	Typ gniazda wejściowego	Hard Wire 3-wire (wymagane podłączenie do przygotowanego przyłącza)

	Zakres napięcia wejściowego	160 - 280V
	Zmienny zakres napięcia wejściowego	100 - 280V
Akumulator	Typ akumulatora	Bezobsługowe baterie
	Typowy czas pełnego ładowania akumulatora	Maksymalnie 2,5 godziny
Zarządzanie	Port komunikacyjny	DB9 RS-232, RJ-45 10/100 Base-T Gniazdo montażu kart rozszerzeń
	Zainstalowane karty zarządzające	Tak. Zarządzająca karta sieciowa wraz z możliwością monitorowania warunków z urządzeń zewnętrznych
	Panel przedni	Diody LED wskazujące pracę z sieci : pracę z baterii : stan wymiany baterii : stanu przeciążenia oraz pracy w trybie "Bypass"
	Alarm dźwiękowy	Alarm podczas pracy na baterii sygnalizujący: znaczny stan wyczerpania baterii, ciągły sygnał dźwiękowy w stanie przeciążenia
	Awaryjny wyłącznik zasilania	Tak
Wymiary	Maksymalna głębokość	670 mm
	Maksymalna szerokość	432 mm
	Wysokość w szafie przemysłowej	Max. 3U
	Ciężar netto	Max. 55 kg
	Poziom hałasu	W odległości 1 m od powierzchni urządzenia max 55 dBA
Środowisko	Odprowadzanie ciepła	max. 1250 BTU/godz
	Zgodność środowiskowa	RoHS 7b Exemption

Dodatkowy moduł baterii		
Architektura	Typ urządzenia	Dodatkowy moduł baterii kompatybilny z UPS 5000VA i 6000VA
	Montaż	Szyny do montażu w szafie teletechnicznej 19 cali
Akumulator	Wstępnie zainstalowane baterie	4
	Typ akumulatora	• Bezobsługowe baterie ołowiowo-kwasowe • Autonomiczny zestaw akumulatorów
	Pojemność akumulatora	Minimum 1900 VAh
Wymiary	Maksymalna głębokość	670 mm
	Maksymalna szerokość	432 mm
	Wysokość w szafie przemysłowej	Max. 3U
	Ciężar netto	Max. 110 kg
Środowisko	Zgodność środowiskowa	ROHS 7b Exemption

Wyposażenie dodatkowe – 1 komplet		
Szafa teleinformatyczna wraz z osprzętem	Ilość	**4 szt. z wyposażeniem każda**
	Opis	• Wysokość szafy: 42U • Szerokość: 800 mm • Głębokość 1000 mm

		• Drzwi przednie blaszane z perforacją oraz zamkiem trzypunktowym • Drzwi tylne blaszane z perforacją • Osłony boczne blaszane pełne • Dach z otworem pod zaślepki • Dwie pary belek nośnych w rozstawie 19” + jedna para belek nośnych środkowych • Cokół o wysokości 100 mm w konfiguracji: przód łącznik pełny, boki perforowane, tył przepust szczotkowy, • Dwie półki 19” montowane na 2 parach belek nośnych 1U, głębokość regulowana • Patch panel POE UTP 6 12p 1U 19"rack, wykrywanie mocy (30W max), ochrona przeciwprzeciążeniowa (650mA +15%-10%) • Termostat sterujący panele wentylatorów • Panel wentylacyjny dachowy, 4 wentylatory sterowany dostarczonym panelem sterowania • Panel wentylacyjny dachowy, 2 wentylatory sterowany dostarczonym panelem sterowania • Zintegrowany czujnik temperatury i wilgotności obsługiwany przez dostarczony panel sterowania
Patch Cord UTP	Ilość	• 5 metrowe – 100 szt. • 3 metrowe – 100 szt. • 2 metrowe – 100 szt. • 1 metrowe – 100 szt.
	Opis	• Kat. 6 S-FTP, złącza RJ-45 • Kolorystyka do ustalenia z Zamawiającym na etapie realizacji zamówienia.
Patch Cord LC-LC	Ilość	• 2 metrowe – 36 szt. • 3 metrowe – 20 szt.
	Opis	Wielomodowe, Kabel krosowy LC/LC duplex OM3 1,8mm
Litwa zasilająca, długa	Ilość	4
	Opis	• Sposób montażu: 19" • 18 gniazd z uziemieniem
Listwa zasilająca, krótka	Ilość	8
	Opis	• Sposób montażu: 19" • 9 gniazd z uziemieniem
Prowadnica kabli	Ilość	60
	Opis	• Prowadnica poprzeczna • Szerokość 19” • Wysokość 1RU • Liczba uchwytów: 5 • Kolor: ciemny, stonowany
Uchwyty kablowe boczne	Ilość	80
	Opis	• Materiał: Stal ocynkowana. • Rozmiar: min. 65x85 mm
Elementy Montażowe	Ilość	700
	Opis	• Wkręt M6x16

		• Nakrętka klatkowa M6 • Podkładka z tworzywa sztucznego

Szczególne warunki gwarancji i serwisu.

Wsparcie konsultacyjne:

Wymaga się aby Wykonawca wraz z dostawą sprzętu i oprogramowania zapewnił bezpłatne wsparcie konsultacyjne w wymiarze nie większym niż 300 osobo-godzin w okresie 36 miesięcy. Specjaliści wydelegowani do udzielenia wsparcia konsultacyjnego po otrzymaniu zgłoszenia od Zamawiającego muszą być dostępni w siedzibie Zamawiającego nie później niż 5 godzin od momentu zgłoszenia. Wsparcie konsultacyjne musi być dostępne codziennie, 24 godziny na dobę, 7 dni w tygodniu.

Wsparcie konsultacyjne będzie udzielane przez minimum 2 osobowy zespół konsultantów specjalistów, wskazanych w wykazie osób dołączonym do oferty.

Wsparcie dotyczyć będzie następujących obszarów :

- Uruchomienie i konfiguracja dostarczonych urządzeń sieciowych,
- Konfiguracja przełączników Ethernet z wykorzystaniem VLAN'ów,
- Instalacja i konfiguracja serwera logów,
- Instalacja i konfiguracja serwera bazodanowego dla potrzeb serwera logów,
- Wymiana i rekonfiguracja urządzeń sieciowych w razie ich uszkodzenia.

Wymagania ogólne dla dostarczanych rozwiązań :

- całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski,
- zamawiający wymaga, by dostarczone urządzenia były fabrycznie nowe,
- całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie wymaganym w SIWZ,
- zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień dostawy,
- całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna,
- Wykonawca przed podpisaniem umowy na realizację zamówienia winien przedłożyć Zamawiającemu oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Warunki gwarancji i serwisu :

- o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona min. 60-miesięczna gwarancja; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była naprawa lub wymiana urządzeń lub ich części, na części nowe i oryginalne, zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań,
- o ile wymagania szczegółowe nie specyfikują inaczej, serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych, diagnozę usterki i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego; usunięcie usterki (naprawa lub wymiana wadliwego podzespołu lub urządzenia) ma zostać wykonana w przeciągu następnego dnia roboczego od momentu zdiagnozowania usterki; Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (od

poniedziałku do piątku, w godzinach 8-17), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla wszystkich dostarczanych rozwiązań,

- W przypadku Sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający dopuszcza podstawienie na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 14 dni roboczych od momentu zgłoszenia usterki. Dostarczony sprzęt zastępczy musi zostać skonfigurowany w sposób umożliwiający mu podjęcie pracy zgodnie z poprzednią funkcją jaką pełnił w infrastrukturze,
- o ile wymagania szczegółowe nie specyfikują inaczej, Zamawiający otrzyma dostęp do pomocy technicznej Wykonawcy (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach 8-17
- o ile wymagania szczegółowe nie specyfikują inaczej, Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:
    - bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres minimum 60 m-cy,
    - dostęp do dokumentacji sprzętu i oprogramowania,
    - dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
    - dostęp do pomocy technicznej producentów.

Przygotowanie administratorów do obsługi urządzeń i systemu zarządzania siecią:
Wykonawca zapewni przygotowanie 3 administratorów sieci Zamawiającego trwające minimum 4 dni po 6 godzin. Instruktarz będzie prowadzony przez doświadczonego inżyniera technicznego znającego zagadnienia sieciowe, który posiada umiejętność konfigurowanie urządzeń dostarczonych przez Wykonawcę.
Zakres przygotowania będzie obejmował podstawową i zaawansowaną konfigurację urządzeń sieciowych dostarczonych przez Wykonawcę. Konfigurację sieci VLAN na tych urządzeniach. Konfiguracja poszczególnych portów, konfiguracja połączeń pomiędzy urządzeniami, stackowanie urządzeń, rozwiązywania prostych i skomplikowanych problemów w sieci, rekonfiguracja infrastruktury, diagnostyka.
W wyniku przeprowadzonego instruktarzu, każdy z administratorów powinien posiadać umiejętności:

- Analizowanie projektu sieci
- Implementacja sieci VLAN
- Implementacja Spanning-Tree Protocol
- Implementacja routingu pomiędzy sieciami wirtualnymi
- Zapewnienie niezawodności Implementacja niezawodności w warstwie sieciowej (L3)
- Mechanizmy bezpieczeństwa w sieciach LAN
- konfiguracji dostępu użytkownika do zasobów sieci
- konfiguracji usługi DHCP
- konfiguracji list ACL
- konfiguracji statycznego routingu dla IPv4
- szybkiego przełączenia urządzeń w przypadku awarii jednego z nich przełączenia
- konfigurowania UTM,
- czytania i interpretowania logów systemowych,
- przygotowania spersonalizowanych raportów z serwera logów SMTP.

Ilości:

Przełącznik szkieletowy – 1 szt.
Przełącznik dostępowy Typu A – 2 szt.
Przełącznik dostępowy Typu B – 9 szt.
Przełącznik dostępowy Typu C – 2 szt.
Punkt Dostępowy WLAN – 3 szt.
System ochrony sieci UTM – 2 szt.
Zasilacz awaryjny UPS 6000 VA – 2 szt.
Dodatkowy moduł baterii – 2 szt.
Wyposażenie dodatkowe – 1 kpl.