Załącznik Nr 1 do SIWZ

Szczegółowy opis przedmiotu zamówienia

Specyfikacja techniczna sprzętu

Szafa Rack 42U – 2 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Drzwi przednie stalowe perforowane z zamkiem, dwuskrzydłowe stalowe drzwi tylne perforowane uchylne, boczne stalowe demontowane na zatrzaskach z możliwością montażu zamka. W wyposażeniu znajdują się: cztery wentylatory, trzy półki, listwa zasilająca. - Drzwi przednie stalowe perforowane z zamkiem - Drzwi tylne stalowe perforowane dwuskrzydłowe uchylne z zamkiem - Drzwi boczne demontowane na zatrzaskach z możliwością montażu zamka - Wyposażenie: minimum 4 wentylatory, 3 półki, listwa zasilająca, 40 koszyków ze śrubami - Zgodność z normami ANSI/EIA RS-310-D, DIN41491 - Zgodność z normami PART1, IEC297-2, DIN41494 - Zgodność z normami PART7, GB/T3047.2-92 - Kompatybilne ze standardami: metrycznym, ETSI oraz międzynarodowym 19” - Stalowa blacha zimnowalcowana - Wykończenie pow.: odtłuszczanie, wytrawianie, fosfatowanie, malowanie proszkowe - Zabezpieczona przed rdzą, utlenianiem, porysowaniem, korozją - Dwa przepusty kablowe - jeden w suficie, drugi w podłodze - Grubość ramy: minimum 1.2 mm - Grubość szyn montażowych: minimum 2.0 mm - Grubość paneli bocznych: minimum 1.2 mm - Grubość przednich drzwi: minimum 1.2 mm - Regulowane nóżki i kółka - Gwarancja minimum 2 lata

Serwery (wersja I) – 2 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)	
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 12 dysków 3.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych

Procesor	Zainstalowane dwa procesory ośmiordzeniowe x86, dedykowane do pracy z serwerem osiągające w teście SPECrate2017_int_base wynik min. 83 dostępny na stronie www.spec.org dla konfiguracji dwuprocesorowej dla oferowanego serwera.
RAM	128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512Gb pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	- minimum pięć slotów generacji 3 w tym jeden FH.
Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 porty typu 1GbE Base-T oraz 2 porty 10 GbE BaseT Dodatkowa karta sieciowa dwuportowa 10 GbE SFP+.
Dyski twarde	Możliwość instalacji dysków SAS, SATA, SSD, NVMe. Zainstalowane: • 4 dyski NLSAS o pojemności min. 8TB. 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. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Wbudowane porty	Przednie: min. 1x VGA, min. 1x USB 2.0, min. 1x micro-USB dedykowane dla karty zarządzającej, Tylne: min. 1x VGA, min. 1x port szeregowy RS232, min. 2x USB 3.0, min. Port wewnętrzny: min. 1x USB 3.0.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 750W każdy z dedykowanymi przewodami zasilającymi.
System operacyjny/dodatkowe oprogramowani	Zainstalowany Windows Server 2019 Standard Zamawiający wymaga dostarczenia wymaganych licencji do uruchomienia 2 dodatkowych maszyn wirtualnych
Bezpieczeństwo	Możliwość zainstalowania moduł TPM 2.0 Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Diagnostyka	- Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury; - wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla dynamic DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania: - wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych; - możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta; - wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH; - możliwość oskryptowywania procesu wykrywania urządzeń; - możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram; - szczegółowy opis wykrytych systemów oraz ich komponentów; - możliwość eksportu raportu do CSV, HTML, XLS; - grupowanie urządzeń w oparciu o kryteria użytkownika; - automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń; - szybki podgląd stanu środowiska; - podsumowanie stanu dla każdego urządzenia; - szczegółowy status urządzenia/elementu/komponentu; - generowanie alertów przy zmianie stanu urządzenia; - filtry raportów umożliwiające podgląd najważniejszych zdarzeń; - integracja z service desk producenta dostarczonej platformy sprzętowej; - możliwość przejęcia zdalnego pulpitu; - możliwość podmontowania wirtualnego napędu; - kreator umożliwiający dostosowanie akcji dla wybranych alertów; - możliwość importu plików MIB; - przesyłanie alertów „as-is" do innych konsol firm trzecich; - aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania); - możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta; - możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;

	- moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2 x64, Microsoft Windows Server 2016, Microsoft Windows Server 2019.
Warunki gwarancji	Min. trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Serwery (wersja II) - 2 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)	
Obudowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory ośmiordzeniowe, min. 2.1 GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 8.4 w teście SPECspeed®2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.

RAM	128GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Funkcjonalność pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 porty typu 1GbE Base-T oraz 2 porty 10 GbE BaseT Dodatkowa karta sieciowa dwuportowa 10 GbE SFP+.
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 4 dyski min. 1.2TB SAS Hot-Plug 2,5" Możliwość instalacji wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash o pojemności minimum 16GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB oraz możliwość konfiguracji w RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy posiadający min. 2GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków SED.
System operacyjny/System wirtualizacji	Zainstalowany Windows Server 2019 Standard Zamawiający wymaga dostarczenia wymaganych licencji do uruchomienia 2 dodatkowych maszyn wirtualnych Zamawiający wymaga dostarczenia 40 licencji Windows Server 2019/2016 Device CALs
Wbudowane porty	min. 1 port USB 2.0, 1 port micro-USB oraz min. 3 porty USB 3.0, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x900
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug maksymalnie 550W.
Bezpieczeństwo	Możliwość zainstalowania moduł TPM 2.0 Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Diagnostyka	Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej; - zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); - szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; - możliwość podmontowania zdalnych wirtualnych napędów; - wirtualną konsolę z dostępem do myszy, klawiatury;

	- wsparcie dla IPv6; - wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; - integracja z Active Directory; - możliwość obsługi przez dwóch administratorów jednocześnie; - wsparcie dla dynamic DNS; - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. - możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera - możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE. 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.
Warunki gwarancji	3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Serwery NAS – 2 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)

Opis:	Serwer NAS - 4 wnęki - SATA 6Gb/s - RAID 0, 1, 5, 6, 10, JBOD, RAID 5 z rezerwą dynamiczną - RAM 2 GB - Gigabit Ethernet - iSCSI
Gwarancja producenta:	24 miesiące
Rodzaj urządzenia:	Serwer NAS
Połączenie z hostem:	Min Gigabit Ethernet
Pojemność całkowita pamięci:	Minimum 8 TB
Ilość zainstalowanych urządzeń / modułów:	Minimum 2
Rodzaj zainstalowanych dysków	4 TB 3,5" x 1/3H SATA 6Gb/s Wielkość bufora - 64 MB
Zainstalowane procesory:	1 x Intel Celeron 2 GHz
Ilość rdzeni:	Minimum 4
RAM:	Minimum 2 GB (zainstalowane) / 8 GB (obsługiwana) - DDR3L
Zainstalowana pamięć flash:	Minimum 512 MB
Kontroler pamięci masowej . Typ:	RAID
Kontroler pamięci masowej . Typ interfejsu:	Minimum SATA 6Gb/s
Kontroler pamięci masowej . Obsługiwane poziomy RAID:	Minimum RAID 0, RAID 1, RAID 5, RAID 6, RAID 10, JBOD, RAID 5 z rezerwą dynamiczną
Protokół warstwy Sieci / Transportu:	TCP/IP, PPTP, L2TP, IPSec, iSCSI, SMTP, FTP, DHCP, Bonjour, SMB, DDNS
Protokół zdalnego zarządzania:	SNMP 2, Telnet, SNMP 3, HTTP, HTTPS, TFTP, SSH
Zgodność z usługami sieciowymi:	Microsoft Active Directory (AD), Apple Bonjour Protocol, DHCP, DDNS, Microsoft CIFS, Network File System (NFS), FTP, FTPS, Server Message Block (SMB), Apple File Protocol (AFP), HTTP, HTTPS, Web-based Distributed Authoring and Versioning (WebDAV), SFTP
Algorytm kodowania:	FIPS 140-2, 256 bitów AES
Dodatkowe wnęki:	4 (całkowity) / 4 (wolna) x wymiana podczas pracy - 2.5" / 3.5"

Gniazda rozszerzeń:	2 (całkowity) / 1 (wolna) x SO-DIMM 204-pin
Interfejsy:	2 x Ethernet 1000Base-T - RJ-45 2 x USB 3.0 - Type A 2 x USB 2.0 - Type A 1 x
Dołączone przewody:	2 x kabel sieciowy
Cechy:	Slot blokady bezpieczeństwa (alarm dźwiękowy, pilot, wbudowany wentylator
Typ Gniazda Zabezpieczającego:	Wbudowany Kensington
Zasilanie	
Zasilacz:	Adapter zasilania zewnętrznego
Wymagane napięcie:	AC 120/230 V
Zużycie energii w trybie aktywności:	Max 34 wat

Zasilacze awaryjne do szaf rack (UPS) – 2 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)	
Moc wyjściowa (pozorna)	minimum 3000 VA
Moc wyjściowa (czynna)	minimum 3000 W
DANE OGÓLNE I ŚRODOWISKOWE	
Topologia	VI (line interactive)
Typ obudowy	Rack / Tower
Chłodzenie	Wymuszone, wewnętrzne wentylatory
WEJŚCIE	
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wejściowego (wartości skuteczne) i tolerancja	178 ÷ 281 V AC ± 2 %
Częstotliwość znamionowa napięcia wejściowego	50 Hz
Zakres częstotliwości i tolerancja	45 ÷ 55 Hz ± 1 Hz
Progi przełączania: sieć – UPS	178 ÷ 281 V AC ± 2 %
WYJŚCIE	
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa	195 ÷ 253 V AC ± 2 %

Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa	230 V AC ± 5 %
Automatyczna regulacja napięcia (AVR)	± 10 %
Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej)	Sinusoidalny / Tak jak na wejściu
Częstotliwość znamionowa napięcia wyjściowego	50 Hz
Filtracja napięcia wyjściowego	Filtr przeciwzakłóceniowy RFI/EMI, tłumik warystorowy
Progi przełączania: UPS – sieć	183 ÷ 276 V AC ± 2 %
Czas przełączenia na pracę rezerwową	< 3 ms
Czas powrotu na pracę sieciową	0 ms
Przeciążalność	> 105% - 15 s (wyłączenie UPS)
AKUMULATORY I CZASY PODTRZYMANIA	
Akumulatory wewnętrzne	minimum 12 V / 7 Ah VRLA
możliwość podłączenia zewnętrznego modułu bateryjnego	wymagane
Czas podtrzymania z baterii wewnętrznych lub przy wykorzystaniu zewnętrznego modułu bateryjnego (dla obciążenia 1820W)	minimum 21 min
Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza).	do 4 h
Maksymalny czas ładowania baterii wewnętrznych UPS + moduł bateryjny do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza).	do 12 h
PARAMETRY MECHANICZNE	
UPS wymiary – Rack (wys. X szer. X gł.)	nie większe niż 132 x 445 x 635 mm
Masa zasilacza	nie większa niż 45 kg
Moduł Bateryjny wymiary – Rack (wys. X szer. X gł.) - jeżeli jest oferowany	nie większe niż 88 x 445 x 435 mm

Masa modułu bateryjnego - jeżeli jest oferowany	nie większa niż 25 kg
ZABEZPIECZENIA	
Zabezpieczenie wejściowe	Przeciwzwarciowe – Bezpiecznik automatyczny
	16 A / 250 V AC
	Przeciwprzepięciowe
Zabezpieczenie wyjściowe	Elektroniczne – przeciwzwarciowe i przeciążeniowe
Zabezpieczenia wejścia DC (akumulatory wewnętrzne)	Zabezpieczenie nadprądowe
Zabezpieczenia DC (zewnętrzny moduł bateryjny)	Zabezpieczenie nadprądowe
WYPOSAŻENIE I FUNKCJE DODATKOWE	
Przyłącza wyjściowe (liczba i typ gniazd)	minimum 9 gniazd z podtrzymaniem bateryjnym (w tym minimum 2 gniazda w standardzie PL z bolcem uziemiającym)
Sygnalizacja	Akustyczno – optyczna; graficzny wyświetlacz LCD,
Interfejsy komunikacyjne	USB HID, SNMP/HTTP
Filtr teleinformatyczny (linii danych) – RJ45	LAN 1 Gbit/s
Wsporniki do montażu w szafie RACK	wymagane
Oprogramowanie monitorująco-zarządzające	oprogramamowanie w języku polskim do zarządzania i monitorowania pracy UPS .
	możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP)
	możliwość edycji nazw urządzeń na liście monitorowanych UPSów
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
Możliwość aktualizacji oprogramowania firmware przez użytkownika	wymagane
Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie napięcia sieciowego	wymagane
ZASTOSOWANE STANDARDY	
Deklaracje	CE
Normy	PN-EN 62040-1:2009, PN-EN 62040-2:2008
GWARANCJA / SERWIS	
Gwarancja	min 36 miesięcy na elektronikę i 24 miesiące na akumulatory;
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.

	serwis realizowany w systemie door to door
DODATKOWE OŚWIADCZENIA/DOKUMENTY	
	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań
	oświadczenie producenta o spełnieniu minimalnych wymaganych parametrów specyfikacji
	karta katalogowa oferowanego sprzętu, oraz wymaganego modułu bateryjnego.
	do oferty należy dołączyć oświadczenie producenta potwierdzające realizację gwarancji i przeglądów przez serwis producenta

Firewall sprzętowy (UTM) – 2 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. **Redundancja, monitoring i wykrywanie awarii** 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. **Interfejsy, Dysk, Zasilanie:** 1. System realizujący funkcję Firewall musi dysponować minimum: • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

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

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure
   - Cisco ACI.

- Google Cloud Platform (GCP).
- OpenStack.
- VMware vCenter (ESXi).

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.

5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

a) System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w ciągu 8 godzin od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy , w przypadku AHB 24x7x8 .
Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).

- Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych UTM

1. Opis przedmiotu zamówienia. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Przełącznik sieciowy – 4 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
W celu realizacji bezpiecznej infrastruktury teleinformatycznej, w której wymagane mechanizmy centralnego systemu bezpieczeństwa obejmują elementy warstwy dostępowej sieci, wymaganym jest dostarczenie przełącznika współpracującego z oferowanym systemem bezpieczeństwa (UTM), w zakresie opisanym w sekcjach: "Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC" oraz "Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa", o następujących parametrach:
Parametry fizyczne platformy • Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. • Zasilanie AC 230V. • Opcjonalny redundantny zasilacz. • Budżet mocy dla portów PoE min.: 370 W.

- Maksymalny pobór mocy bez budżetu dla PoE: 100 W.
- Minimalny zakres temperatury pracy: 0-50°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

- W tym porty PoE w ilości co najmniej: 24, zgodne ze standardem: 802.3af oraz 802.3at.

d) 4 porty GE, SFP.

Zarządzanie

- Dedykowany minimum 1 interfejs Ethernet RJ-45 do zarządzania.
- Wbudowany minimum 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów przy działających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Zarządzanie urządzeniami Switch musi odbywać się z poziomu wbudowanej konsoli graficznej funkcjonującej w ramach interfejsu zarządzania dostarczanego urządzenia bezpieczeństwa UTM; W ramach zarządzania musi być możliwe:

- kontrolowanie stanu zasilania portów PoE switcha;
- zarządzanie funkcjami bezpieczeństwa, kontroli ruchu, ochrony przez zapętlaniem (STP, ochrona przed zapętlaniem, snooping DHCP,
- tworzenie VLAN;
- konfiguracja portów i przypisywanie do nich VLAN;
- tworzenie i zarządzanie politykami bezpieczeństwa NAC na interfejsach (802.1x);
- graficzna wizualizacja połączeń i portów pozwalająca identyfikację w stopniu nie mniejszym niż:
- adres MAC hosta;
- adres IP hosta;
- nazwa hosta;
- nazwa użytkownika, jeśli mechanizmy uwierzytelniania są używane przez system bezpieczeństwa.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 104 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 155 Mpps.
- Tablica adresów MAC o pojemności co najmniej 16.000 wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
- Wsparcie dla Private VLAN.
- Obsługa routingu statycznego.
- Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Centralne zarządzanie sieciami VLAN.
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
   - Przenoszenie zidentyfikowanych urządzeń do właściwych sterf. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do sterfy odizolowanej.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
   - W przypadku gdy do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zaządzania lub NAC wymagane są licencje, producent zobowiązany jest je dostarczyć .
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

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

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe

1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym w ciągu 8 godzin

od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 12 miesięcy.

2. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7x8 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7 x8. Oferent winien przedłożyć dokumenty:
   - Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej).
   - Certyfikat ISO 9001 podmiotu serwisującego.

Opisy do wymagań ogólnych

3. Opis przedmiotu zamówienia. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
4. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Telefonia VOIP – 1 komplet

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)

Zakres dostawy i usług:

1. Dostawa urządzeń systemu telekomunikacyjnego:

1) <u>Centrala telefoniczna – Serwer IP PBX - 1 szt</u>

konfiguracja min. 80 linii wewnętrznych, - min. 30 szt. jednoczesnych kanałów rozmownych, z możliwością dalszej rozbudowy. Montaż w szafie RACK

Serwer:
- obudowa Rack 19" 2U
- procesor Intel i5
- pamięć RAM 8GB
- dysk HDD 1 TB klasy Enterprise
- system telekomunikacyjny (licencja bezterminowa)
- interfejs www dla administratora w języku polskim

*2) <u>telefon sekretarski – **5 szt**</u>*

Funkcje telefonu: 16 konta SIP, wstrzymanie/wyciszanie połączeń, DND, szybkie wybieranie, ponowne wybieranie, przekierowywanie, połączenia oczekujące, transfer połączeń, funkcja głośnomówiąca, SMS,

ponowne wybieranie, oddzwanianie, auto odpowiedź, lokalne 3-stronne konferencje, bezpośrednie połączenie IP bez SIP proxy, dzwonek: wybór/import/usuwanie, ręczne/automatyczne ustawianie czasu
plan numeracyjny, przeglądarka XML, RTCP-XR
Właściwości audio: dźwięk HD: w słuchawce, w głośniku, kodeki: G.722, G.711(A/μ), G.723, G.729AB, G.726, iLBC, DTMF: In-band, Out-of-band (RFC 2833) and SIP INFO, funkcja zestawu głośnomówiącego full duplex z AEC, VAD, CNG, AEC, PLC, AJB, AGC
Książka telefoniczna: lokalna książka telefoniczna do 1000 wpisów, czarna lista, zdalna książka telefoniczna XML/LDAP, inteligentne wyszukiwanie, wyszukiwanie/import/eksport, historia połączeń: wykonane/odebrane/nieodebrane/przekazane
Integracja z IP PBX: BLF, BLA, anonimowe wykonywanie/odrzucanie połączeń, Hot-desking, połączenia alarmowe, MWI, poczta głosowa, parkowanie połączeń, ściąganie połączeń, interkom, paging, muzyka na czekanie.
Klawisze funkcyjne: 10 klawiszy z podświetleniem, 10 klawiszy, w których można zaprogramować do 27 funkcji, 7 klawiszy funkcyjnych: wiadomość, zestaw słuchawkowy, wyciszenie, wstrzymanie, transfer, redial, głośnomówiący, 4 klawisze kontekstowe, 6 klawiszy nawigacji, klawisze kontroli głośności, podświetlany klawisz wyciszenia, podświetlany klawisz zestawu słuchawkowego, podświetlany klawisz funkcji zestawu głośnomówiącego.
Wyświetlacz i wskaźniki: podświetlany graficzny wyświetlacz 4.3" 480 x 272 pikseli, głębia koloru 16 bit, tapeta, wskaźnik LED dla oczekujących połączeń i wiadomości, dwukolorowy (czerwony lub zielony) wskaźnik LED statusu linii, intuicyjny interfejs użytkownika z ikonami i klawiszami funkcyjnymi, wybór języka (w tym język polski), identyfikacja dzwoniącego (ID) z nazwą i numerem.
Interfejs: 2 porty Gigabit Ethernet, wbudowany port USB obsługujący zestawy słuchawkowe Bluetooth (za pomoca adapter USB), PoE (IEEE 802.3af), klasa 0, 1 port RJ9 (4P4C) na słuchawkę ręczną, 1 port RJ9 (4P4C) na zestaw słuchawkowy, 1 port RJ12 (6P6C) EHS, 1 port RJ12 (6P6C) EXT: obsługa do 6 modułów rozszerzających.
Zarządzanie: konfiguracja: przeglądarka/telefon/auto-provision, auto-provision przez: FTP/TFTP/HTTP/HTTPS dla masowego wdrożenia, auto-provision z PnP, zarządzanie z poziomu urządzenia BroadSoft, zero sp-touch, TR-069, eksport śledzenia danych, logi systemowe, blokada telefonu dla ochrony prywatności, przywracanie ustawień fabrycznych.
Sieć i bezpieczeństwo: SIP v1 (RFC2543), v2 (RFC3261), IPV6, NAT Traversal: tryb STUN, tryb proxy i peer-to-peer SIP link, Przypisanie IP: statyczne/DHCP/PPPoE, serwer HTTP/HTTPS, synchronizacja daty I godziny poprzez SNTP, UDP/TCP/DNS-SRV (RFC 3263), QoS: 802.1p/Q tagging (VLAN), Layer 3 ToS DSCP, SRTP dla głosu, Transport Layer Security (TLS), zarządzanie certyfikatami HTTPS, szyfrowanie AES plików konfiguracyjnych, uwierzytelnianie przy pomocy MD5/MD5-sess, OpenVPN, IEEE802.1X.
Gwarancja 24 miesiące

3) **moduł sekretarski 1 szt**

Funkcje modułu: graficzny wyświetlacz LCD 160x320 pikseli, 20 klawiszy, każdy z dwukolorowym podświetleniem LED, 2 niezależne klawisze służące do przewijania stron, możliwość zaprogramowania współdzielonej linii, listy BLF, grupy BroadSoft, parkowania połączeń, konferencji, przekierowywania, odbierania połączeń w grupie, grupowego słuchania, przeglądarki XML, Zero-SP-Touch, do 6 łańcuchowo połączonych modułów, zasilanie z telefonu, 2 pozycje podstawki, możliwość montażu na ścianie.

4) **brama 32 porty, dla podłączenia telefonów wewnętrznych analogowych – 2 szt**

32 porty FXS, obsługa FAX, złącza Telco RJ21, konfiguracja przez www lub telnet, auto provisioning, Call Hold, Call Waiting, Call Forward, DND (Do Not Disturb- nie przeszkadzać), direct IP calling, blind Transfer, Attended Transfer.

5) brama 10 portów, **dla podłączenia telefonów wewnętrznych analogowych 1 szt**

dziesięć portów RJ-11 FXS do podłączenia telefonów analogowych do sieci danych opartych na protokole, jedno wieloportowe złącze 50-stykowe RJ-21, oferujące alternatywny wybór połączeń, jeden interfejs Ethernet 10/100 Base-T RJ-45 do podłączenia do routera lub przełącznika wielowarstwowego, obsługa funkcji głosowych i nośnych wysokiej jakości, zarządzanie wdrożeniami na dużą skalę, silne zabezpieczenia oparte na szyfrowaniu metodą komunikacji, inicjowanie obsługi administracyjnej i obsługi serwisowej.

4) Aparat VOIP - 45 szt

Funkcje telefonu:

- 3 konta SIP
- wstrzymanie/wyciszanie połączeń, DND
- szybkie wybieranie
- przekierowywanie, połączenia oczekujące, transfer połączeń
- funkcja głośnomówiąca, SMS
- ponowne wybieranie, oddzwanianie, auto odpowiedź
- lokalne 3-stronne konferencje
- bezpośrednie połączenie IP bez SIP proxy
- dzwonek: wybór/import/usuwanie
- ręczne/automatyczne ustawianie czasu
- plan numeracyjny
- przeglądarka XML
- zrzuty ekranu
- RTCP-XR

Właściwości audio:

- dźwięk HD: w słuchawce, w głośniku
- szerokopasmowy kodek: G.722
- wąskopasmowy kodek: G.711(A/μ), G.729AB, G.726, iLBC
- DTMF: In-band, Out-of-band (RFC 2833) and SIP INFO
- funkcja zestawu głośnomówićego full duplex z AEC
- VAD, CNG, AEC, PLC, AJB, AGC

Książka telefoniczna

- lokalna książka telefoniczna do 1000 wpisów
- czarna lista
- zdalna książka telefoniczna XML/LDAP
- inteligentne wyszukiwanie
- wyszukiwanie/import/eksport
- historia połączeń: wykonane/odebrane/nieodebrane/przekazane

Integracja z IP PBX

- BLF, BLA
- anonimowe wykonywanie/odrzucanie połączeń
- Hot-desking, połączenia alarmowe
- MWI
- poczta głosowa, parkowanie połączeń, ściąganie połączeń
- interkom, paging, muzyka na czekanie

Wyświetlacz i wskaźniki

- graficzny wyświetlacz LCD 132×64 piksele
- wskaźnik LED dla oczekujących połączeń i wiadomości
- dwukolorowy (czerowny lub zielony) wskaźnik LED statusu linii
- intuicyjny interfejs użytkownika z ikonami i klawiszami funkcyjnymi
- wybór języka (w tym język polski)
- identyfikacja dzwoniącego (ID) z nazwą i numerem

Interfejs

- 2 porty RJ45 Gigabit Ethernet
- PoE (IEEE 802.3af), klasa 2
- 1 port RJ9 (4P4C) na słuchawkę ręczną
- 1 port RJ9 (4P4C) na zestaw słuchawkowy

Zarządzanie:

- konfiguracja : przeglądarka/telefon/auto-provision
- auto-provision przez : FTP/TFTP/HTTP/HTTPS dla masowego wdrożenia
- auto-provision z PnP
- zero sp-touch, TR-069
- eksport śledzenia danych, logi systemowe
- blokada telefonu dla ochrony prywatności
- przywracanie ustawień fabrycznych

Sieć i bezpieczeństwo:

- SIP v1 (RFC2543), v2 (RFC3261), IPV6
- NAT Traversal: tryb STUN
- tryb proxy i peer-to-peer SIP link
- Przypisanie IP: statyczne/DHCP
- serwer HTTP/HTTPS
- synchronizacja daty I godziny poprzez SNTP
- UDP/TCP/DNS-SRV (RFC 3263)
- QoS: 802.1p/Q tagging (VLAN), Layer 3 ToS DSCP
- SRTP dla głosu
- Transport Layer Security (TLS)
- zarządzanie certyfikatami HTTPS
- szyfrowanie AES plików konfiguracyjnych
- uwierzytelnianie przy pomocy MD5/MD5-sess
- OpenVPN, IEEE802.1X
- LLDP/CDP/DHCP VLAN
- Gwarancja 24 miesiące

Brama ISDN

- 6 portów BRI (S0) ISDN (dostępnych przez BNTadpater)
- moduł 8 BRI ma zintegrowany zegar o wysokiej precyzji (HPC)
- Każdy port jest konfigurowalny w trybie NT lub TE z wymianą PIN
- Rezystory terminujące (100 Ohm) dla każdego portu oddzielnie konfigurowane
- TE / NT i terminacja na port przełączane programowo (bez zworek)
- Warstwa 2 to Q.921, a warstwa 3 jest zgodna z Q.931 (EuroISDN DSS1)
- Zestaw funkcji DSS1: CLIP / No-Screening, CLIR, COLP, UUS, MCID, CD, CNIP AOC-D
- Zestaw funkcji Q.SIG: CNIP
- Dostępność opcjonalna CAPI 2.0 (faks, głos)
- Kodeki: G.723.1 i załącznik A, G.729 a / b, G.726, (do 4 kanałów)
- G.711 i Echo Cancellation do 16 kanałów
- G.168 / G.165 Tłumienie echa z wykrywaniem zmiany ścieżki echa, do 128 ms
- Wykrywanie aktywności głosowej / generowanie hałasu komfortowego
- Wykrywanie i generowanie cyfr DTMF
- Przekaźnik faksu T.38 (V.27, V.29 i V.17) (do 4 kanałów)
- Agent użytkownika SIP zgodny z IETF RFC3261
- SIP przez UDP / TCP z opcjonalną obsługą TSL, SRTP
- „Mostkowanie TDM" dwóch urządzeń beroNet poprzez magistralę PCM

• Zasilanie: 110-230 V, działające 12 V DC przy 2 A • Zgodność: CE (EN55022, EN55024, EN60950)

Stworzenie i konfiguracja domeny lokalnej. Konfiguracja środowiska loklanego – 1 komplet

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
1. Utworzenie dwóch kontrolerów domeny Microsoft w postaci maszyn wirtualnych umieszczonych na każdym z dostarczonych serwerów. 2. Instalacja i konfiguracja ról i funkcji niezbędnych do działania MS AD. 3. Wdrożenie niezbędnych polityk GPO i przeszkolenie z ich obsługi; 4. Dodanie 10 wybranych stacji roboczych do domeny wraz z instruktażem; 5. Migracja danych Zamawiającego na nowe środowisko w formie dedykowanych maszyn wirtualnych - po potwierdzeniu zgodności systemów je obsługujących z nowym środowiskiem. 6. Licencje CAL na użytkownika – 50 szt.

Oprogramowanie backupu – 1 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Oprogramowanie powinno: 1. Być przeznaczone dla małych, średnich i dużych firm, które mają rozbudowane środowisko informatyczne, powinno oferować elastyczną architekturę (serwer zarządzający/media-serwer/klient) celem sprostania rozwojowi środowiska informatycznego 2. Cechować się efektywnym wykorzystaniem napędów taśmowych, tzn. system musi być zoptymalizowany do zapisywania informacji na jak najmniejszej ilości napędów taśmowych 3. Zapisywać na taśmach zoptymalizowane dane, bez konieczności wykonywania żadnych dodatkowych działań w celu ich optymalizacji. 4. Być skalowalne, umożliwiać łatwą rozbudowę w miarę rozrastania się infrastruktury informatycznej 5. Umożliwiać zmiany producenta sprzętu bez utraty funkcjonalności backupu. Nie powinno posiadać preferowanego dostawcy hardware dla którego dostępna jest bogatsza funkcjonalność (macierze, biblioteki taśmowe). 6. Być łatwe w instalacji, konfiguracji i zarządzaniu poprzez interface graficzny (GUI). 7. Posiadać zaawansowane funkcje monitoringu, generator raportów. 8. Umożliwiać backup po sieci LAN serwerów z Windows 2008/2008R2/2012/2012R2/2016/2019 i Linux. 9. Wykorzystywać bezobsługowe biblioteki taśmowe bądź lokalne dyski do przechowywania danych 10. Umożliwiać stosowanie go w środowisku Storage Area Network, zapewniając dużą szybkość wykonywanych backupów oraz współdzielenie napędów taśmowych pomiędzy serwery backupowe w sieci SAN. 11. Posiadać możliwość równoczesnego zapisu/ odczytu na wielu napędach taśmowych w tym samym czasie. 12. Umożliwiać backup online bazy danych (np. Oracle, Exchange, MS SQL). 13. Posiadać wbudowany mechanizm backupu otwartych plików 14. Wykorzystywać do backupu, mechanizm kopii migawkowych systemu Microsoft Windows (VSS). 15. Posiadać funkcje disaster–recovery dla systemu Windows umożliwiające proste i szybkie automatyczne odtworzenie serwera po awarii zapewniające integralność i spójność danych, opcja ta powinna być integralną częścią systemu backupowego. Funkcja disaster-recovery musi być dostępna dla systemów Windows

i oprócz odtwarzania systemu operacyjnego musi umożliwiać zmianę sterowników minimum do urządzeń pamięci masowych czy kart sieciowych tak by było możliwe odtworzenie systemu na innym fizycznym sprzęcie
16. Posiadać funkcję automatycznego backupu z możliwością programowania dowolnych cykli, bazując na kalendarzu. Oprogramowanie powinno umożliwiać backup typu: full, incremental, differential).
17. Umożliwiać wykonywania skryptów przed i po backupie (np. uruchamianych przed backupem bazy oraz po wykonaniu backupu off-line bazy, kasowanie redo logów)
19. Umożliwiać kompresję na kliencie backupowym przed wysłaniem danych przez sieć.
20. Umożliwiać pracę w klastrze serwerów z Microsoft Windows.
21. Umożliwiać wykonywanie backupów na urządzenia dyskowe, które następnie będą automatycznie powielane na nośniki taśmowe (D2D2T).
22. Umożliwiać przesyłanie altertuw poprzez email
23. Umożliwiać backup online danych z systemu SharePoint, wraz z odtwarzanie pojedynczych dokumentów z jednoprzebiegowego backupu.
24. Umożliwiać backup środwisk wirtualnych Vmware vSphere 6.0/6.5/6.7/7.0 z wykorzyatniem mechanizmu vstorage API w taki sposób by możliwe było odtwarzanie pojedynczych plików (zawartych w VMDK dla systemu Windows) z jednoprzebiegowego backupu całej maszyny wirtualnej.
26. Wspierać dla technologii wirtualizacyjnych firmy Microsoft (Hyper-V), odtwarzanie pojedynczych plików z maszyn wirtualnych Windows z jednoprzebiegowego backupu. Wsparcie powinno uwzględniać wersje oprogramowania Windows 2008/2008R2/2012/2012R2/2016/2019
27. Powinno posiadać (jako opcja) możliwość wykonania backupu Active Directory a następnie odzyskania pojedynczych obiektów AD bez restartu i resynchronizacji systemu. Backup ten powinien być wykonywany jednoprzebiegowo.
28. Umożliwiać centralne zarządzanie serwerami (Media Serwerami) systemu backupowego (jako opcja).
29. Umożliwiać backup zasobów z serwerów Linux poprzez sieć SAN, tak aby tylko metadane były wysyłane przez sieć LAN.
31. Wspierać najnowsze wersje aplikacji i serwerów takich jak: Windows 2019, Exchange 2019, Windows 10 oraz najnowsze wersje produktów takich jak: Microsoft SharePoint 2016, Microsoft Exchange 2019, Microsoft SQL Server 2019.
32. Posiadać jako opcję (komponent włączany, działający jako integralna część aplikacji backupowej) deduplikację danych. Funkcjonalność tego modułu powinna opierać się na blokowej deduplikacji danych wykonywanej on-line a więc w trakcie wykonywania zadania backupowego. Proces deduplikacji danych musi odbywać się na kliencie (serwerze z danymi, aplikacją) lub na media serwerze. Konfiguracja i zarządzanie całym procesem, przełączanie miejsca deduplikacji musi odbywać się za pomocą jednej konsoli zarządzającej systemem backupowym – jedna konsola dla konfigurowania i zarządzania całością procesów backupowych i odtwarzania danych.
33. Deduplikacja danych na kliencie (optymalizacja transferu danych przez siec LAN/WAN) powinna być dostępna dla systemów Windows i Linux i nie może wymagać instalacji dodatkowych komponentów czy agentów poza oprogramowaniem klienckim systemu backupowego.
34. Włączenie funkcjonalności deduplikacji danych nie powinno powodować konieczności instalacji dodatkowego oprogramowania nie tylko po stronie klienta backupu ale także media serwera (serwera systemu backupowego)
35. Posiadać otwarte API umożliwiające podłączanie urządzeń deduplikacyjnych innych firm.
36. Umożliwiać odtwarzanie pojedynczych elementów (maile, elementy AD, pliki czy bazy danych) z aplikacji Exchange, Active Directory, SharePoint i MS SQL zainstalowanych w środowiskach wirtualnych (Vmware, Hyper-V) poprzez backup całej maszyny wirtualnej.
37. Umożliwiać automatyczne i ręczne uruchamianie kopii zapasowej jako działającej maszyny wirtualnej na platformie MS Hyper-V lub VMware,
37. Umożliwiać szyfrowanie komunikacji pomiędzy klientem (serwerem produkcyjnym) a serwerem backupowym za pomocą protokołu SSL.
39. Umożliwiać konwersję P2V lub B2V systemów fizycznych (Windows) na maszyny wirtualne (Vmware i Hyper-V) w dwojaki sposób. P2V – powinien umożliwiać na równoczesny backup danych i jednoczesną konwersję do pełnej maszyny wirtualnej, natomiast B2V powinien umożliwiać konwersję po zakończeniu

zadania backupowego. Oba sposoby konwersji są wewnętrznymi komponentami systemu backupowego i nie powinny wymagać dodatkowych licencji czy instalacji dodatkowego oprogramowania.
40. Umożliwiać zarządzania systemem backupowym poprzez CLI (Command Line Interface) poprzez komponent Windows PowerShel.
41. Należy dostarczyć licencje oferujące backup środowiska wirtualnego składającego się z 1 serwera VMware vSphere wyposażonego w 2 procesory 8 core'owe z licencją na okres 12 miesięcy

Monitory telewizyjne (TV) – 3 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)	
Ekran	Minimum 43 cale / 108 cm, 16:9
Zgodność z HD	4K UHD, 3840 x 2160
HDR (High Dynamic Range) / Formaty HDR	tak / HDR10+, HLG (Hybrid Log-Gamma)
Optymalizacja ruchu / Częstotliwość odświeżania	Picture Quality Index 2800 / 50 Hz
Tuner	DVB-T2, DVB-S2, DVB-C, analogowy
Funkcje poprawy obrazu	UHD Dimming, Natural Mode Support, Contrast Enhancer, Dynamic Crystal Color, procesor Crystal 4K, Crystal Display, Dual LED
System dźwięku przestrzennego	tak
Moc głośników	Minium 2 x 10 W
Regulacja tonów wysokich / niskich	tak
Korektor dźwięku	tak
Smart TV	tak
Wi-Fi	tak
DLNA	tak
Przeglądarka internetowa	tak
Nagrywanie na USB	tak
Komunikacja dodatkowa	Bluetooth, Wi-Fi Direct
Menu w języku polskim	tak
Liczba złączy HDMI	Minimum 3
Liczba złączy USB	Minimum 2
Złącze Ethernet (LAN)	Min 1x 1 GbE
Cyfrowe wyjście optyczne	tak
Złącze CI (Common Interface)	1
Możliwość montażu na ścianie	tak -
Klasa energetyczna	Minimum A
Pobór mocy IEC 62087 Ed.2 (tryb włączenia)	Max 70 W
Rozdzielczość	Minimum 3840 x 2160
Zasilanie	220 - 240 V 50/60 Hz

Stacje robocze typu All-In-One – 30 szt.

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)	
Typ sprzętu	All-in-One
Typ obudowy	zintegrowana z ekranem
Procesor	
Model procesora	Minimum Intel Core i3 10100T lub równoważne 64-bit
Liczba rdzeni procesora	Minimum 4
Liczba wątków procesora	Minimum 8
Częstotliwość procesora [MHz]	Minimum 3000
Częstotliwość Turbo procesora [MHz]	Minimum 3800
Wielkość pamięci cache L2 lub L3 [KB]	Minimum 6144
Płyta główna	
Chipset	Minimum Intel Q470 lub równoważne
Pamięć	
Ilość pamięci [GB]	Minimum 8
Format pamięci	SODIMM
Typ pamięci	DDR4
Taktowanie pamięci [MHz]	Minimum 2666
Dyski twarde	
Liczba zainstalowanych dysków	1
Typ dysku nr 1	SSD
Kontroler dysku nr 1	M.2
Liczba zainstalowanych kart graficznych	1
Karta graficzna	zintegrowana
Liczba obsługiwanych wyświetlaczy	2
Ekran	
Wyświetlacz zintegrowany z obudową	
Przekątna ekranu [cale]	Minimum 23,8
Rozdzielczość	Minimum 1920 x 1080
Typ ekranu	Full HD
Rodzaj matrycy	IPS
Kontrast	700:1
Jasność [cd/m2]	250
Format obrazu	16:9
Wprowadzenie danych	
Mysz w zestawie	tak
Typ myszy	przewodowa

Klawiatura w zestawie	tak
Typ klawiatury	przewodowa
Opcje rozszerzeń	
Obsługiwane karty pamięci	SD, SDHC, SDXC
Multimedia	
Typ karty dźwiękowej	zintegrowana
Liczba obsługiwanych kanałów	2
HD Audio	tak
Liczba głośników	2
Typ głośników	zintegrowane
Wbudowany mikrofon	tak
Liczba wbudowanych mikrofonów	2
Wbudowana kamera	tak
Komunikacja	
Liczba kart sieciowych	2
Standard karty sieciowej	10/100/1000
Typ karty sieciowej	zintegrowana
WLAN	tak
Standard WLAN	ac/a/b/g/n
Bluetooth	tak
Standard Bluetooth	4.2
Złącza z tyłu obudowy	
Łączna liczba portów USB z tyłu	4
Liczba portów USB 2.0 z tyłu	2
Liczba portów USB 3.0 z tyłu	2
Liczba portów DisplayPort z tyłu	1
Liczba portów LAN z tyłu	1
Liczba wyjść audio z tyłu	1
Złącza z przodu lub boku obudowy	
Łączna liczba portów USB z przodu	2
Liczba portów USB 3.0 z przodu	1
Liczba wyjść audio z przodu	1 (combo)
Inne złącza z przodu	USB 3.1 Typ-C
Oprogramowanie	
System operacyjny	Windows 10 Pro lub równoważny preinstalowany

Bezpieczeństwo	
	Układ szyfrowania TPM, Blokada portów USB, Złącze Kensington
Zasilanie	
Moc zasilacza [W]	Minimum 155
Sprawność zasilacza [%]	Minimum 85
Gwarancja	
Czas gwarancji	Minimum 3 lata dla firm i instytucji
Typ gwarancji	on-site, next business day
Certyfikaty	
	Certyfikat Energy Star, Energy Star Qualified, EPEAT Compliant, Znak bezpieczeństwa CE, RoHS

Inne akcesoria, usługi – 1 komplet

PARAMETRY I CHARAKTERYSTYKA (WYMAGANIA MINIMALNE)
Montaż i instalacja sprzętu, rozszycie sieci, konfiguracja środowiska wg. wskazówek Zamawiającego. Wymagane akcesoria: Patchpanelle 19" 24xRJ45 STP (1U) do gniazd beznarzędziowych, ekranowany, keyston patch panel, organizatory kabli 19'', uchwyty kablowe 19" oraz inne niezbędne.

WÓJT
mgr Tomasz Stolarczyk