Załącznik nr 3: Opis przedmiotu zamówienia
do Zapytania ofertowego nr 1/2023

OPIS PRZEDMIOTU ZAMÓWIENIA

Szczegółowy opis poszczególnych Części przedstawiony jest poniżej, są to wymagania minimalne.

CZĘŚĆ NR 1:

1. Zestaw komputerowy – 16 szt.

Komputery typu AiO

Matryca

Przekątna matrycy	23,8''
Standard matrycy	Full HD
Rozdzielczość matrycy	1920 x 1080
Powłoka matrycy	Matowa
Technologia ekranu	IPS
Jasność matrycy	250 nit
Kontrast	1000:1
Pokrycie palety barw	99% sRGB

Procesor

Liczba rdzeni procesora	czternaście
Liczba rdzeni performance	sześć
Liczba rdzeni efficient	osiem
Taktowanie rdzeni procesora	3,5 GHz (Max efficient core)
Taktowanie trybu turbo procesora	4,8 GHz (Max performance core)
Pamięć cache procesora	24 MB

Pamięć RAM

Zainstalowana pojemność pamięci RAM	16 GB
Ilość slotów pamięci RAM	2
Możliwość rozbudowy pamięci RAM do	64 GB
Częstotliwość pamięci RAM	4800 MHz
Technologia wykonania pamięci RAM	SODIMM DDR5

Dysk

Ilość zainstalowanych dysków	1 szt
Typ dysku	SSD
Pojemność dysku podstawowego	512 GB

Karta graficzna

Producent karty zintegrowanej	Intel®
Model karty zintegrowanej	UHD Graphics 770
Model karty dedykowanej	Brak

Komunikacja

Karta sieciowa przewodowa	10/100/1000 Mbps
Typ bezprzewodowej karty sieciowej	WiFi 6 (802.11 ax)
Bluetooth	Tak

Interfejsy WE/WY

HDMI	1 szt - HDMI 1.4b, 1 szt - HDMI 2.1
Display Port	1 szt - DP 1.4a
USB 3.2 Gen 1 (5 Gbps)	2 szt
USB 3.2 Gen 2 (10 Gbps)	3 szt
USB 3.2 Gen 2x2 typ C (20 Gbps)	1 szt
RJ-45 [LAN]	1 szt
Wyjście słuchawkowe	Combo
Wejście mikrofonu	Combo
Wyjście liniowe audio	1 szt

Multimedia

Karta dźwiękowa	HD Audio
Ilość głośników	2
Moc głośników	5 W
Kamera	5,0 Mpix + IR przód
Wbudowany mikrofon	Tak
Czytnik kart pamięci	Tak
Formaty kart obsługiwane przez czytnik	SD, SDHC, SDXC

System operacyjny

Wersja systemu operacyjnego	Windows 11 Pro
Architektura systemu	64 bit
Wersja językowa systemu operacyjnego	polska

Zabezpieczenia

Gniazdo linki zabezpieczającej	Tak
Szyfrowanie TPM	Tak

Gwarancja

Typ gwarancji	Producenta
Rodzaj gwarancji	Pro Support (Naprawa u klienta) z zachowaniem dysku twardego
Czas trwania gwarancji	36 miesięcy

Oprogramowanie dodatkowe do komputera

Typ oprogramowania	Biurowe
Typ licencji	Nowa licencja
Rodzaj licencji oprogramowania	Do zastosowań komercyjnych
Czas trwania licencji	Nieograniczony
Liczba użytkowników przewidziana w licencji	1
Liczba urządzeń przewidziana w licencji	1
Wersja produktu	PKC
Obsługiwane platformy systemowe	Mac OS, Windows 10, Windows 11
Rodzina oprogramowania	Office 2021
Aplikacje	Excel, OneNote, Outlook, PowerPoint, Word
Typ nośnika oprogramowania	Download
Wersja językowa	Polska

2. UPS – 1 szt.

Moc pozorna / Moc czynna : 3000VA (2700W),

Rodzaj UPS: Line-Interactive 1-Fazowy 1/1,

Czas podtrzymania: ok. 9 min (przy 50% obciążenia),

Power Factor wyjściowy: 0.9,

Rodzaj obudowy: RACK 19 / Tower,

Kształt fali: Pure Sine Wave (Czysta fala sinusoidalna),

Wyjście: 8x IEC C13 (programowalne),

Ilość oraz rodzaj baterii na wyposażeniu: 6x 12V / 9Ah,

Porty komunikacyjne: USB oraz RS-232,

Funkcja USB-HID - nie wymaga instalacji dodatkowych sterowników!,

Wyłącznik EPO (Emergency Power Off),

Funkcja Cold Start - możliwość uruchomienia z baterii (zimny start),

Obrotowy wyświetlacz: LCD,

Moc ładowarki: 1A~6A,

Inteligentny Slot na moduł rozszerzeń (np. SNMP do kontroli zdalnej),

Złącze dla dodatkowych baterii (wydłużanie czasu podtrzymania),

Wymiary: 2U / 88 x 438 x 610mm (wys. x szer. x gł.),

3. Macierz dyskowa – 1 szt.

Procesor	Architektura 64 bit
Procesor liczba rdzeni	Nie mniej niż 4
Pamięć RAM	Nie mniej niż 4GB DDR4
Pamięć RAM liczba slotów	Minimum 1 slot
Pamięć RAM - możliwość rozszerzenia	nie mniej niż do 16GB

Pamięć Flash	Nie mniej niż 512MB
Liczba zatok na dyski twarde	Minimum 8
Obsługiwane dyski twarde	3.5" oraz 2.5" SATA
Pojemność możliwych do stosowania dysków twardych	do 18TB
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej dwóch
Porty LAN	Minimum 2 x 2,5 Gb/s
Porty LAN 10 Gb/s	Minimum 2 na złączu SFP+
Diody LED	Minimum Status, LAN, HDD,
Porty USB 3.2	Minimum 4
Port PCiE umożliwiające rozbudowę urządzenia o dodatkowe karty rozszerzeń	Tak, minimum 1
Przyciski	Reset, Zasilanie
Typ obudowy	RACK, 2U
Dopuszczalna temperatura pracy	od 0 do 40˚C
Wilgotność względna podczas pracy	5-95% R.H.
Zasilanie	Zasilacz redundantny max. 2x250 W, 100-240 V

Specyfikacja oprogramowania

Agregacja łączy	Tak
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Możliwość podłączenia karty WLAN na USB	Tak
Szyfrowanie wolumenów	Tak, min AES 256
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, 50, 60, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek woluminów i LUN blokowych Obsługa replikacji migawek
Wbudowana obsługa iSCSI	Multi-LUN na Target Obsługa LUN Mapping & Masking Obsługa MPIO Migawka LUN Kopia zapasowa iSCSI LUN

Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box
Darmowe aplikacje na urządzenia mobilne	Monitoring i zarządzanie urządzeniem Synchronizacja plików Obsługa kamer Dostępne na systemy iOS oraz Android
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu
VPN	VPN client / VPN server Obsługa PPTP OpenVPN
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Ustawienia: Back up, przywracania, resetowania systemu

Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem oraz blokowanie na podstawie Geolokalizacji Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja	3 lata

4. Dysk do macierzy – 4 szt.

Pojemność: 8000 GB
Format: 3.5"
Interfejs: SATA III (6.0 Gb/s) - 1 szt.
Pamięć podręczna cache: 256 MB
Prędkość obrotowa: 5400 obr./min
Prędkość odczytu (maksymalna): 210 MB/s
Niezawodność MTBF: 1 000 000 godz.
Minimalna głośność pracy: 27 dB
Dodatkowe informacje:
Technologia RAID
Zgodność z systemami NAS
Gwarancja: 36 miesięcy (gwarancja producenta)

5. Urządzenie wielofunkcyjne I – 15 szt.

Druk w kolorze:	Nie
Automatyczny druk dwustronny:	Tak
Rozdzielczość druku w czerni [dpi]:	2400 x 1200
Szybkość druku w czerni [str/min]:	30
Szybkość wydruku pierwszej strony (czerń) [s]:	8.5
Druk na płytach CD/DVD:	Nie
	Skaner
Typ skanera:	CIS
Rozdzielczość optyczna [dpi]:	1200 x 1200
Inne:	Nie
Maksymalny format skanowania:	210 x 297 mm

	Kopiarka
Rozdzielczość kopiowania [dpi]:	600 x 600
Zmniejszanie / powiększanie:	25 - 400
Prędkość kopiowania - czerń [str/min]:	30
Funkcje kopiowania:	Kopiowanie wielokrotne
	Faks
Wbudowany faks:	Nie
Automatyczna sekretarka:	Nie
	Techniczne
Maksymalny format druku:	A4
Podajnik papieru:	250 arkuszy
Taca odbiorcza:	120 arkuszy
Pamięć:	64 MB
Wyświetlacz:	Tak
Wi-Fi:	Nie
Bluetooth:	Nie
NFC:	Nie
Praca w sieci:	Nie
Obsługiwane formaty nośników:	A4, A5, A6, Executive, Letter
Poziom hałasu [dB]:	48
Pobór mocy drukowanie [W]:	440
Pobór mocy wyczekiwanie [W]:	6.2
Wydajność druku czarnego [strony]:	1200
	Złącza
Złącze Ethernet (LAN):	Nie
Złącze USB:	Tak
Złącze LPT:	Nie
	Fizyczne
Wysokość [mm]:	272
Szerokość [mm]:	410
Głębokość [mm]:	398
Waga [kg]:	10.3
	Parametry
Rodzaj drukarki (Technologia druku):	Laserowa
Obsługiwane systemy:	Linux, Mac OS X 10.8, Windows 10, Windows 11, Windows 7, Windows 8
Kolor obudowy:	Szaro-czarny
Wyposażenie:	Kabel zasilający, Płyta CD z oprogramowaniem, Toner startowy
Załączona dokumentacja:	Instrukcja obsługi w języku polskim, Karta gwarancyjna
Gwarancja:	24 miesiące, Door To Door

6. Urządzenie wielofunkcyjne II – 1 szt.

Dane ogólne

Technologia	Elektrofotograficzna drukarka laserowa
Klasyfikacja lasera	Produkt zawierający laser klasy 1 (IEC60825-1:2007)
Procesor	Cortex-A9 800MHz
Pamięć	1 GB
Interfejs lokalny	Hi-Speed USB 2.0
Interfejs sieci przewodowej	10Base-T/100Base-TX/1000Base-T
Wyświetlacz	Kolorowy ekran dotykowy o przekątnej 12.3cm
Skróty	48

Drukarka

Prędkość druku – Standard (A4)	Do 50 stron na minutę
Prędkość druku – Dupleks (A4)	Do 24 stron na minutę (12 arkuszy na minutę)
Rozdzielczość	Do 1 200 x 1 200 dpi
Tryb cichej pracy	Możliwość obniżenia poziomu hałasu podczas drukowania poprzez zmniejszenie szybkości druku do 25 stron na minutę
Czas wydruku pierwszej strony	Mniej niż 7,5 sekundy z trybu gotowości
Czas rozgrzewania	Mniej niż 4,7 sekundy z trybu uśpienia
Automatyczny druk dwustronny	Drukowanie na obu stronach arkusza papieru
Języki druku	PCL6, BR-Script3 (Emulacja języka PostScript®3™), IBM Proprinter XL, Epson FX-850 PDF wersja 1.7, XPS wersja 1.0
Czcionki rezydentne (PCL)	73 czcionek skalowalnych, 12 czcionek bitmapowych, 13 kodów kreskowych
Czcionki rezydentne (Postscript)	66 skalowalnych
Wbudowane kody kreskowe (PCL)	Code39, Interleaved 2 of 5, FIM (US-PostNet), Post Net (US-PostNet), EAN-8, EAN-13, UPC-A, UPC-E, Codabar, ISBN (EAN), ISBN (UPC-E), Code128 (set A, set B, set C), EAN128 (set A, set B, set C)

Funkcje sterownika drukarki

Drukowanie N stron	Można zmniejszyć 2, 4, 9, 16 lub 25 stron A4 i wydrukować je na 1 stronie A4 (Mac: 2, 4, 6, 9 lub 16 stron)
Drukowanie plakatów	Powiększanie 1 strony A4 do rozmiaru plakatu przy użyciu 4, 9, 16 lub 25 stron A4
Drukowanie znaków wodnych	Na dokumentach można drukować wstępnie zdefiniowany tekst lub tekst zdefiniowany przez użytkownika w formie znaku wodnego
Drukowanie ID	Na dokumentach mogą być drukowane dane identyfikacyjne (data i godzina, krótki tekst zdefiniowany przez użytkownika lub nazwa użytkownika komputera)
Ręczny dupleks	Ręczny druk dwustronny (zalecany w przypadku nośników nieobsługiwanych przez dupleks automatyczny)
Drukowanie broszur	Drukowanie dokumentów w formie broszury formatu A5 przy użyciu funkcji automatycznego lub ręcznego druku dwustronnego
Pomijanie pustych stron	Urządzenie ignoruje wszystkie puste strony w dokumentach
Profile drukowania	Często używane konfiguracje drukowania można zapisać, by zapewnić sobie do nich szybki dostęp
Drukowanie tekstu na czarno	Podczas drukowania urządzenie konwertuje cały tekst w dokumencie do koloru czarnego
Archiwum wydruków	Funkcja umożliwia zapisywanie kopii wszystkich drukowanych dokumentów w postaci plików PDF

Drukowanie kopii	Drukowanie dodatkowych kopii tego samego dokumentu na papierze z podajników dodatkowych
Bezpośrednie drukowanie	Drukowanie bezpośrednio z pamięci Flash USB. Obsługiwane formaty plików: PDF wersja 1.7, JPEG, Exif+JPEG, PRN (utworzone przez sterownik drukarki), TIFF (zeskanowane za pomocą urządzenia Brother), XPS wersja 1.0
Bezpośrednie skanowanie	Bezpośrednie skanowanie do pamięci Flash USB. Obsługiwane formaty plików: PDF, PDF/A, zabezpieczony PDF, podpisany PDF, JPEG, XPS, TIFF

Skaner

Typ skanera	Podwójny CIS (Contact Image Sensor)
Automatyczne skanowanie dwustronne	Tak
Skanowanie w trybie kolorowym i czarno-białym	Tak
Prędkość skanowania w trybie czarno-białym	50 obrazów na minutę
Prędkość skanowania dwustronnego w trybie czarno białym	100 obrazów na minutę
Szybkość skanowania w trybie kolorowym	20 obrazów na minutę
Szybkość skanowania dwustronnego w trybie kolorowym	34 obrazy na minutę
Rozdzielczość skanowania przy użyciu ADF	Do 600 x 600 dpi
Rozdzielczość skanowania przy użyciu szyby skanera	Do 1 200 x 1 200dpi
Rozdzielczość skanowania interpolowana	Do 19 200 x 19 200dpi
Głębia kolorów	16 777 216 kolorów (24 bity)
Skala szarości	256 odcieni szarości (8 bitów)
Standardowe funkcje	Skanowanie do pamięci USB, wiadomości e-mail, OCR, obrazu i pliku
Skanowanie w sieci	Skanowanie do folderu sieciowego (tylko Windows®), FTP, SFTP, serwera Email5, platformy SharePoint Server 2007/2010/2013 i aplikacji Easy Scan to Email
Skanowanie do chmury	Bezpośrednie skanowanie do Evernote™, Box, Dropbox, Google Drive™, OneDrive, Evernote™, OneNote
Funkcje skanowania	Usuwanie koloru tła, Pomijanie pustych stron, Skanowanie dokumentu tożsamości4, Skanowanie 1 na 24, Automatyczne prostowanie stron podczas skanowania z użyciem ADF, Dzielenie PDF
Skanowanie do Microsoft Office	Skanowanie do Microsoft® Word, Microsoft® Excel i Microsoft® PowerPoint
Skanowanie do pliku PDF z możliwością wyszukiwania	Skanowanie dokumentów do plików pdf z możliwością wyszukiwania
Skanowanie do platformy SharePoint	Skanowanie dokumentów bezpośrednio do platformy SharePoint
Zaznacz obszar i Skanuj	Funkcja umożliwia zaznaczenie na oryginalnym dokumencie obszarów, które mają być skanowane lub pominięte podczas skanowania
Skanowanie za pomocą protokołu Usług internetowych systemu Windows®	Możliwość skanowania bezpośrednio do urządzenia z systemem Windows® (Windows® 7 i nowsze)

Sterownik skanera

	TWAIN i WIA
Windows®	Windows® 10 (wersja 32 i 64 bitowa), Windows® 8 (wersja 32 i 64 bitowa),

	Windows® 7 (wersja 32 i 64 bitowa), Windows Vista® (wersja 32 i 64 bitowa), Windows® XP Professional (wersja 32 i 64 bitowa) Windows® XP Home
Macintosh5	TWAIN i ICA OS X 10.8.5, 10.9.x, 10.10.x, 10.11.x
Linux5	SANE (wersja 32 i 64 bitowa)

Kopiarka

Prędkość kopiowania (A4)	Do 50 kopii na minutę
Automatyczne kopiowanie dwustronne	Tak
Czas uzyskania pierwszej kopii	Mniej niż 9,5 sekundy z trybu gotowości
Rozdzielczość	Do 1 200 x 600 dpi
Wielokrotne kopie/Układanie/ Sortowanie	Urządzenie wykonuje do 999 kopii każdej strony / Układanie lub Sortowanie
Powiększanie Zmniejszanie	Urządzenie zmniejsza lub powiększa rozmiar dokumentu od 25% do 400% co 1%
Kopiowanie N na 1	Pozwala użytkownikowi zmieścić 2 lub 4 strony na jednym arkuszu A4
Kopia dowodu tożsamości 2 na 1	Możliwość wydrukowania obu stron dokumentu tożsamości na jednej stronie A4
Skala szarości	256 odcieni szarości (8 bitów)
Kopiowanie paragonów	Wykonywanie wyraźniejszych kopii paragonów
Zaznacz obszar i Kopiuj	Funkcja umożliwia zaznaczenie na oryginalnym dokumencie obszarów, które mają być kopiowane lub pominięte podczas kopiowania

7. Serwer – urządzenie sieciowe – przełącznik (switch) – 1 szt.

Zarządzanie:	Zarządzalny L2
Dostęp:	Przeglądarka WWW (GUI) Wiersz poleceń (CLI) SNMP v1/v2c/v3 RMON Telnet
Architektura sieci	Gigabit Ethernet
Całkowita liczba portów	28
Złącza	RJ-45 10/100/1000 Mbps - 24 szt. SFP+ - 4 szt.
Power over Ethernet (PoE)	Brak PoE
Obsługiwane standardy	IEEE 802.3 IEEE 802.3 u IEEE 802.3 x IEEE 802.3 ab IEEE 802.3 ae
Rozmiar tablicy MAC	16 k
Ramka Jumbo	9,000 B
Liczba grup VLAN	4096
Algorytm przełączania	Store-and-forward
Przepustowość	128 Gb/s
Bufor pamięci	1,5 MB
Maksymalny pobór mocy	22,3 W
MTBF	516 593 h

Dodatkowe informacje
Automatyczne krosowanie portów (Auto MDI-MDIX)
Diagnostyka przewodów
Praca w trybie half i full-duplex
QoS
VLAN

8. Urządzenie wielofunkcyjne - usługa instalacji sprzętu

Rozpakowanie urządzenia i przygotowanie do pracy

Instalacja na stanowisku wskazanym przez zamawiającego

Instalacja sterowników na stacjach roboczych oraz wykonanie próbnych wydruków

Przeszkolenie personelu z obsługi urządzenia

9. Serwer - usługa instalacji oprogramowania

Konfiguracja i instalacja udziałów sieciowych i polityk bezpieczeństwa na macierzy dyskowej

CZĘŚĆ NR 2:

1. Serwer – zapora sieciowa UTM – 1 szt.

Wymagania ogólne
Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje.
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.

Funkcje modułu Firewall
1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej AcQve Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego rouQngu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać MulQcast rouQng.
6. Musi obsługiwać Policy Based rouQng.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (DifferenQated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, staQc, acQve/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.

19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.
22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: AcQveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z AcQve Directory.
27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej AcQve Directory.
28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego agenta na stacjach roboczych użytkowników.
29. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsom oraz Citrix.
30. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
31. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
32. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
33. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
34. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
35. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
36. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji hpp.
37. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
38. Musi zapewniać funkcjonalność Content RouQng w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
39. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
40. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

Dostarczony system bezpieczeństwa musi zapewniać:
1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed niechcianą pocztą.
4. Kontrolę wykorzystywanych aplikacji.
5. Możliwość filtrowania URL.

Parametry fizyczne systemu Firewall:
Element systemu pełniący funkcję Firewall musi dysponować:
- 5 portami 1Gb RJ45.
- Minimum 2 GB pamięci RAM.
- Minimum 2 porty USB 3.0.
- Minimum jeden port typu Console.
- Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza.

Parametry wydajnościowe systemu:
• Przepustowość Firewall minimum: 1.4 Gbps.
• Przepustowość IPSec VPN nie mniejsza niż: 460 Mbps.
• Przepustowość skanowania antywirusowego nie mniejsza niż: 500 Mbps.
• Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 271 Mbps.
• Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 154 Mbps.
• Obsługa nie mniej niż: 10 tuneli IPSec site-to-site.
• Obsługa nie mniej niż: 10 tuneli client-to-site.
• Obsługa nie mniej niż: 100.000 jednoczesnych połączeń.
• Obsługa nie mniej niż: 8.500 nowych połączeń na sekundę.
• W ramach Firewall system musi obsługiwać minimum: 10 sieci VLAN.

W ramach ochrony przed atakami system musi zapewniać:
1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL InjecQon, Cross-Site-ScripQng, Buffer OverFlow, Remote File Inclusions.
6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

W ramach kontroli antywirusowej system musi zapewniać:
1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 10MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

W ramach kontroli antyspamowej system musi zapewniać:
1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.
6. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

W ramach filtrowania zawartości URL system musi zapewniać:
1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.

3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określenia różnego rodzaju akcji dla połączeń do wybranych adresów URL na podstawie reputacji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu hpps.
13. Wyłączenie inspekcji hpps dla wybranych kategorii stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:
1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1800, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji. Wymagane funkcje VPN systemu:
1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer DetecQon (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego rouQngu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 8,10 i 11, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.

Zarządzanie:
1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub plaCormą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub plaCormy centralnego zarządzania, logowania, raportowania.

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
19. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
23. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

Certyfikaty

1. System realizujący funkcję firewall musi być wyprodukowany zgodnie z normą ISO 9001 oraz ISO-14001.
2. ICSA lub EAL4 dla funkcji Firewall.

Licencje i wsparcie techniczne

1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:
• Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Rozpoznawanie urządzeń pracujących w sieci – na okres 3 lat.
2. System musi być objęty serwisem gwarancyjnym producenta przez okres 3 lat, 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 (świadczone telefonicznie lub poprzez portal).

Wymagania dotyczące instalacji i konfiguracji systemu oraz szkoleń użytkowników

1. Wykonawca powinien posiadać minimum 3 certyfikowanych inżynierów na poziomie Professional (lub odpowiednim) w zakresie instalacji i konfiguracji systemu bezpieczeństwa oferowanego producenta. Certyfikaty inżynierów Wykonawca będzie zobowiązany przedstawić na każde żądanie Zamawiającego.
2. Wykonawca w ramach przedmiotu zamówienia zobowiązuje się do zapewnienia dla co najmniej dwóch pracowników Zamawiającego szkolenia (prowadzonego przez autoryzowanego trenera producenta), z zakresu obsługi i konfiguracji systemu bezpieczeństwa dostarczonego w ramach zamówienia.

Wraz z dostarczeniem sprzętu wchodzą następujące czynności:

- Aktywacja Licencji
- Aktualizacja Firmware
- Konfiguracja kont administracyjnych
- Konfiguracja interfejsów sieciowych
- Konfiguracja DNS, NTP
- Konfiguracja DNAT
- Konfiguracja DHCP
- Konfiguracja mVPN (SSL, IKEv2)

Uruchomienie oraz konfiguracja modułów bezpieczeństwa:

- Network Discovery
- Geolokalizacja
- IPS
- App Control
- WebBlocker
- spamBlocker
- Gateway AntiVirus
- Reputation Enabled Defense (RED)
- IntelligentAV
- APT Blocker
- Access Portal

Konfiguracja globalnych polityk bezpieczeństwa dla protokołów:

- DNS
- NTP
- FTP
- HTTP
- HTTPS
- POP3
- IMAP
- SMTP

Uruchomienie inspekcji ruchu szyfrowanego dla protokołów:

- SMTP
- IMAP
- POP3
- HTTPS