Załącznik nr 5 do SWZ

Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest: **"Dostawa sprzętu komputerowego i oprogramowania w ramach Konkursu grantowego „Cyberbezpieczny Samorząd" o numerze FERC.02.02-CS.01-001/23, Fundusze europejskie na rozwój cyfrowy 2021-2027 (FERC) priorytet II: zaawansowane usługi cyfrowe, działanie 2.2. – wzmocnienie krajowego systemu cyberbezpieczeństwa".**

2. Charakterystyka przedmiotu zamówienia:

Zadanie 1: Przełączniki

1) 4szt. urządzenia typu switch, np. *HP Aruba Instant On 1930 Switch 48G 4SFP+* lub równoważne o minimalnych cechach równoważności jak poniżej:

Procesor	0.8 GHz
Pamięć Flash	256 MB
Pamięć RAM	512 MB
Przeznaczenie	Do szaf RACK 19"
Typ	Zarządzalny
Liczba portów LAN 10/100/1000	48 Sztuk
Podtyp:	10 Gigabit Ethernet
Porty:	48 x 10/100/1000 + 4 x 1 Gigabit / 10 Gigabit SFP+
Wykonanie:	Przepustowość: 130.95 Mpps Zdolność przełączania: 176 Gbps Opóźnienie (1 Gbps): 2.2 µs Opóźnienie (10 Gbps): 1.2 µs
Pojemność:	Routing table entries (static): 32
Zgodność z normami:	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.1ab (LLDP), IEEE 802.3az
Protokół routingu:	IGMPv2, IGMP, routing statyczny IPv4, MSTP, RSTP, STP
Protokół zdalnego zarządzania:	SNMP, RMON, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SCP, DHCP, IPv4, IPv6
Algorytm kodowania:	SSL
Metoda identyfikacji:	RADIUS

Cechy:	Sterowanie przepływem, obsługa DHCP, obsługa ARP, trunking, obsługa VLAN, auto-uplink (auto MDI/MDI-X), nasłuchiwanie IGMP, dublowanie portów, zarządzalność, obsługa IPv6, tryb półdupleksu, tryb pełnego dupleksu, obsługa protokołu Spanning Tree (STP), obsługa protokołu Rapid Spanning Tree (RSTP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa list dostępu (ACL), Quality of Service (QoS), obsługa Jumbo Frames, Trusted Platform Module (TPM), obsługa IPv4, obsługuje LACP, obsługuje LLDP, Link Aggregation Control Protocol (LACP), Class of Service (CoS), obsługuje SNMP, bufor pakietów 1,5MB, Bridge protocol data unit (BPDU), LLDP-MED, Green Ethernet (EEE)
Rozmiar tablicy adresów MAC	16000
Obsługiwane ramki Jumbo:	9216 bajtów
Prędkość magistrali wew.	176 Gb/s
Szybkość przekierowań pakietów	130.95 mpps
Obsługa VLANów	Tak
Zarządzalność	Tak
Możliwość instalacji w szafach 19'	Tak
Zasilacz:	Adapter mocy wewnętrznej
MTBF:	114 Lat
Zgodność z normami:	VCCI, CISPR 24, EN 61000-3-2, IEC 61000-3-2, IEC 61000-3-3, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, EN 61000-3-3, UL 60950-1, IEC 60950-1, EN 60950-1, EN 60825-1, CNS 13438, EN 55024:2010, FCC CFR47 Part 15 A, ICES-003 issue 6 Class A, IEC 62368-1, UL 62368-1 Second Edition, CISPR 32 Class A, EN 62368-1:2014, CAN/CSA-C22.2 No. 60950-1, CISPR 35, EN 55035:2017, EN 55032:2015+AC:2016 Class A
Urządzenie musi być przeznaczone na rynek Polski	

2) 20 szt.: urządzeń typu Switch np. *Switch HP Aruba IOn 1830 8G* lub równoważnych o minimalnych cechach równoważności jak poniżej:

Rodzaj urządzenia:	Przełącznik zarządzalny- 8 porty – smart
Porty:	8x10/100/1000
Wykonanie:	Czas oczekiwania (100Mbps): 5.2 Opóźnienie (1 Gbps): 2.8 Przepustowość: 11,9 Mp/s

	Zdolność przełączania: 16 Gb/s
Wielkość tablicy adresów MAC:	8000 wpisów
Obsługiwane ramki Jumbo:	9216 bajtów
Protokół routingu:	IGMPv2, IGMP
Protokół zdalnego zarządzania:	SNMP 1, SNMP 2c, HTTP, HTTPS, TFTP, SCP, ICMP
Algorytm kodowania:	SSL
Procesor:	800MHz
RAM:	512 MB SDRAM
Pamięć fleszowa:	256 MB
Wskaźniki statusu:	Status portu, tryb dupleksu portu, łącze/aktywność, prędkość
Cechy:	Sterowanie przepływem, automatyczne wykrywanie urządzenia, autonegocjacja, obsługa VLAN, automatyczna funkcja uplink (auto MDI/MDI-X), nasłuchiwanie IGMP, obsługa Syslog, dublowanie portów, możliwość aktualizacji firmwaru, obsługa SNTP, możliwość montowania na ścianie, obsługa protokołu Spanning Tree (STP), dziennik zdarzeń, Quality of Service (QoS), Trusted Platform Module (TPM), Cable Diagnostics Function, bez chłodzenia, obsługuje LLDP, klient DHCP, Class of Service (CoS), zarządzane w chmurze, bufor pakietów 1,5MB, Secure Copy (SCP), Link Aggregation, obsługa podwójnego obrazu, Denial of Service (DoS) protection, Green Ethernet (EEE), BPDU Filter, ochrona pętli, Global Storm Control, Port Scheduling
Zgodność z normami:	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.3ac, IEEE 802.1ab (LLDP), IEEE 802.3az
Interfejsy:	7 x 1000Base-T RJ-45 1 x 1000Base-T RJ-45 wejście PoE
Zasilacz:	Adapter mocy zewnętrznej
MTBF:	188.2 lata
Zgodność z normami:	IEC 61000-3-2, IEC 61000-3-3, EN 61000-3-3, ICES-003 Klasa A, CNS 13438 Class A, KN35, IEC/EN 61000-4-3, IEC/EN 61000-4-4, IEC/EN 61000-4-5, IEC/EN 61000-4-6, IEC/EN 61000-4-8, AS/NZS CISPR 32 Class A, KN32 Class A, IEC/EN 61000-4-11, IEC/EN 61000-4-2, EN 55032:2015, UL 62368-1 Second Edition, IEC/EN60950-1:2006 +A11:2009 +A1:2010 +A12:2011 +A2:2013, IEC/EN 60825-1:2014 Class 1, CISPR 32 Class A, EN 55035, CISPR 35, IEC 62368-1 Second Edition, CAN/CSA-C22.2 No. 62368-1 Third Edition, UL 62368-1 Third Edition, IEC 62368-1 Third Edition, CAN/CSA C22.2 No. 62368-1 Second Edition,

	FCC CFR47 Part 15 B Class A 2018
Produkt musi być przeznaczony na rynek Polski	

3) 1 szt. urządzenia tupu Switch np. *Switch LAN D-link DGS 1250 -52X/E* lub równoważnego o minimalnych cechach równoważności jak poniżej:

Typ	Zarządzalny Smart
Obudowa	Przeznaczona do montażu w szafie RACK 19”
Liczba portów	48 1000BASE-T Gigabit Ethernet
Obsługiwane warstwy	Layer 2, Layer 3
Interfejs zarządzania	Wiersz poleceń CLI, web GUI, port konsoli
Dodatkowe	SNMP, VLAN 802.1Q
Warunki gwarancji	Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta

4) 1 szt.: urządzenia typu Switch np. *UBIQUITI USW-LITE-16-POE* lub równoważnego o minimalnych cechach równoważności jak poniżej:

Montaż:	Możliwość instalacji w szafce 10”
Interfejs zarządzania:	Ethernet
Interfejs sieciowy:	16 portów GbE RJ45 w tym 8 portów PoE/PoE+ (Pins 1, 2+; 3, 6-)
Całkowita przepustowość:	16 Gb/s
Zdolność przełączania:	32 Gb/s
Zasilanie:	AC/DC, wewnętrzne
Maks. zużycie energii:	15W (z wyłączeniem wyjścia PoE)
Dostępne POE w sumie:	45 W
Max. POE wat na port według PSE PoE +:	30 W
Przyciski:	Resetowanie fabryczne

Certyfikaty:	CE, FCC, IC
Przełączanie warstwy 2:	• IGMP snooping • STP / RSTP with priorities and port-level disable • Port isolation • Storm control • Voice VLAN • Port mirroring • LACP port aggregation • Multicast / broadcast rate limiting • MAC address blocking • Flow control • 802.1X control • Jumbo frames • Proprietary loop protection • DHCP snooping / guarding • Egress rate limit • LLDP-MED • Port restricted by MAC • Device isolation with ACLs
Diody LED:	• System - status • Ethernet PoE - prędkość / łącza / aktywność • PoE - link / aktywność
Wymagania dotyczące aplikacji:	konsola centralnego zarządzania wspólna dla przełącznika oraz punktu dostępowego wskazanych w podpunkcie 4, 5, 6 niniejszego zadania

5) 3 szt.: urządzenia typu Switch np. *UBIQUITI USW-Lite-8-POE* lub równoważnych o minimalnych cechach równoważności jak poniżej*:*

Interfejs zarządzania:	Ethernet
Interfejs sieciowy:	8 portów GbE RJ45 w tym 4 porty PoE/PoE+ (Pins 1, 2+; 3, 6-)
Całkowita przepustowość bez blokowania:	8 Gb/s
Zdolność przełączania:	16 Gb/s
Metoda zasilania:	54V DC, 1.1A zasilacz
Dostępne POE w sumie:	52 W
Max. POE wat na	30 W

port według PSE PoE +:	
Przyciski:	Resetowanie fabryczne
Certyfikaty:	CE, FCC, IC
Przełączanie warstwy 2:	• IGMP snooping • STP / RSTP with priorities and port-level disable • Port isolation • Storm control • Voice VLAN • Port mirroring • LACP port aggregation • Multicast / broadcast rate limiting • MAC address blocking • Flow control • 802.1X control • Jumbo frames • Proprietary loop protection • DHCP snooping / guarding • Egress rate limit • LLDP-MED • Port restricted by MAC • Device isolation with ACLs
Diody LED:	• System - status • Ethernet PoE - prędkość / łącza / aktywność • PoE - link / aktywność
Wymagania dotyczące aplikacji:	konsola centralnego zarządzania wspólna dla przełącznika oraz punktu dostępowego

6) 1 szt. urządzenia typu Punkt Dostępowy np. *UBIQUITI UAP-AC-PRO UNIFI ACCESS POINT* lub równoważnego o minimalnych cechach równoważności jak poniżej:

Interfejsy sieciowe:	2 Gb porty Ethernet 10/100/1000
Przycisk:	Reset
Anteny:	3 anteny o podwójnej polaryzacji i zysku 3dBi
Standardy WiFi:	802.11 a/b/g/n/ac
Sposób zasilania:	Pasywne PoE (48V), 802.3af/803.2at
Zakres napięcia:	44-57 V DC
Zasilacz:	48V, 0.5A Gb PoE (w zestawie)
Moc nadawcza:	2.4 GHz: 22 dBm, 5 GHz: 22 dBm
BSSID:	4 na radio

Zabezpieczenia:	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)
Certyfikaty:	CE, FCC, iC
Montowanie:	Na suficie / ścianie (uchwyt w zestawie)
Zaawansowane zarządzanie ruchem:	• VLAN 802.1Q • QoS Limit ustawiany na użytkownika • Izolowanie ruchu gości Wspierane • WMM Voice, Video, Best Effort, Background • Jednocześni klienci 200
Wpierane przepustowości (zależnie od modulacji / szerokości kanału)	• 802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mb/s • 802.11n 6,5 - 450 Mb/s (MCS0 - MCS23, HT 20/40) • 802.11ac 6,5 - 1300 Mb/s (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80) • 802.11b 1, 2, 5.5, 11 Mb/s • 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mb/s
Wymagania dotyczące aplikacji:	konsola centralnego zarządzania wspólna dla przełącznika oraz punktu dostępowego wskazanych w podpunkcie 4, 5, 6 niniejszego zadania

7) 1 szt.: Serwer NAS wraz z 4szt. dysków *10 TB HDD* o parametrach nie niższych niż:

Procesor:	Procesor czterordzeniowy, osiągający w teście wydajności PassMark Average CPU Mark co najmniej 4600 punktów (wynik dostępny pod adresem https://www.cpubenchmark.net)
Pamięć systemowa:	Min. 8GB SODIMM DDR4 z możliwością rozbudowy do 64 GB
Pamięć flash:	5 GB (Ochrona systemu operacyjnego przed podwójnym rozruchem)
RAID:	0,1,5,6,10,50,60,JBOD,Single Disk
Zainstalowane dyski	Ilość: 4szt. Dedykowany do: zaproponowanego serwera NAS Rozmiar: 3.5” Typ: magnetyczny Pojemność: 10TB Wytrzymałość w czasie pracy: 65 G Wytrzymałość w czasie spoczynku: 250 G Niezawodność MTBF: 1000000h Prędkość obrotowa: 7200 obr./min. Pamięć cache: 256 MB Maks. Transfer zewnętrzny: 215 MB/s
Rodzaje wyjść / wejść:	USB 3.2 Gen. 2 – 3 szt. USB 3.2 Gen. 1 Type-C – 1 szt. RJ45(LAN) 2.5 Gbps – 2 szt. PCIe 3.0 x 4 – 2 szt.

Protokoły sieciowe:	AFP, Dynamiczny DNS (DDNS), HTTP, HTTPS. iPv4/iPv6, iSCSI, Serwer CIFS/SMB, Serwer DNS, Serwer DHCP, Serwer FTP, Serwer SFTP, Serwer NFS, Serwer VPN, S.M.A.R.T., SNMP, SSH, Telnet, VLAN (802.1Q), FTPS, TFTP, WebDAV, LDAP
System plików dla dysków zewnętrznych:	FAT32, exFAT, NTFS, NFS+, EXT3, EXT4
System plików:	EXT4
Zasilacz:	W zestawie
Dodatkowe informacje:	Funkcja Wake on LAN/WAN, Szyfrowanie woluminów
Dołączone akcesoria:	Zestaw montażowy, Kabel sieciowy – 1 szt., Kabel zasilający – 1 szt., Radiator dysku SSD M.2 – 2 szt.
Ramka zabezpieczająca:	Ramka Jumbo
Kieszenie na dyski:	2,5”/3,5” – 4szt.(Hot swap) M.2 PCIe NVMe 3.0 x 1 – 2szt.

Pozostałe Wymagane Parametry Sprzętowe:

- Obsługa przyspieszenia pamięci podręcznej SSD
- GPU pass-through
- Koprocesor arytmetyczny FPU
- Mechanizm szyfrowania (AES-NI)
- Obudowa: Typu Tower
- Możliwość rozbudowy o opcjonalne karty PCIe: wyjście HDMI, Port 5/10 Gigabit sieci ethernet, procesor graficzny, transkodowanie wspomagane sprzętowo
- Wskaźniki LED: Stan/zasilanie, USB, LAN, dyski 1–4, M.2 SSD 1–2
- Przyciski: zasilanie, reset, automatyczne kopiowanie USB
- Maks. liczba połączeń współbieżnych (CIFS) — z maks. pojemnością pamięci 200
- Zainstalowane dyski: 4 x 10 TB, 6Gb/s (SATA III) , znajdują się na liście kompatybilności producenta NAS-a przeznaczone do pracy ciągłej
- Standardowa gwarancja (NAS/HDD): 3 lata
- NAS obsługuje oprogramowanie instalowane w postaci kontenerów Docker
- Repozytorium dostępne w urządzeniu musi umożliwiać pobranie oraz instalacje wykorzystywanego w urzędzie oprogramowanie "FerroBackup" w formie kontenera Docker.
- W przypadku awarii urządzenia, nośniki danych pozostają u kupującego (gwarancja KYHD).

8) 1 szt.: **Serwer NAS + *2szt. Dysków HDD 4TB*** o minimalnych parametrach jak poniżej:

Typ	Sieciowy serwer plików NAS
Obudowa	Wolnostojąca Miejsce na instalację min. 2szt. dysków twardych w rozmiarze 3,5''
Procesor	Procesor czterordzeniowy, osiągający w teście wydajności PassMark Average CPU Mark co najmniej 3900 punktów (wynik dostępny pod adresem https://www.cpubenchmark.net)
Pamięć RAM	Min. 2GB DDR4 RAM, z możliwością rozbudowy do 6GB.
Kontroler pamięci masowej	Obsługiwane typy dysków: SATA III, Obsługiwane tryby RAID min.: 0, 1.
Dyski twarde	3,5" 7200 RPM SATA III 4TB – 2 szt. - dedykowane do zaoferowanego NAS
Wbudowane porty	Min. 2 szt. min 1 GbE LAN RJ-45; min 1 port USB min 3.0
System operacyjny - funkcje	Wszystkie wymienione poniżej funkcjonalności zawarte są w cenie urządzenia, bez konieczności ponoszenia dodatkowych kosztów przez Zamawiającego. 1. Wbudowany serwer: CIFS/SMB 3.0, FTP, NFS, 2. Integracja z Microsoft Active Directory (AD).
Protokoły sieciowe	HTTPS, SMB, SMNP, FTP, SSH
Warunki gwarancji	- Serwis urządzenia musi być realizowany przez producenta lub autoryzowanego partnera serwisowego producenta. - W przypadku awarii urządzenia, nośniki danych pozostają u kupującego (gwarancja KYHD).

9) **Dysk USB WD Elements Desktop 10TB USB 3.2 Gen. 1** lub równoważny o minimalnych cechach równoważności jak poniżej:

Pojemność	10TB
Interfejs	USB 3.2 Gen. 1

Złącza	USB Micro-B
Dołączone akcesoria	Kabel USB Zasilacz sieciowy
Informacje dodatkowe	W przypadku awarii urządzenia / dysków: nośniki danych pozostają u zamawiającego.

9) <u>Dysk USB WD Elements Desktop 6TB USB 3.2 Gen. 1</u> lub równoważny o minimalnych cechach równoważności jak poniżej:

Pojemność	6TB
Interfejs	USB 3.2 Gen. 1
Złącza	USB Micro-B
Dołączone akcesoria	Kabel USB Zasilacz sieciowy
Informacje dodatkowe	W przypadku awarii urządzenia / dysków: nośniki danych pozostają u zamawiającego.

10) <u>1szt. Zasilacza awaryjnego UPS</u> o minimalnych parametrach jak poniżej:

Typ	Jednofazowy online (VFI)
Fazy (WEJŚCIE-WYJŚCIE)	1-1
Typ obudowy	Tower

Pojemność mocy	10000VA / 10000W
Współczynnik mocy wyjściowej	1.00
Zakres napięcia wejściowego	110-300 VAC @ 0-60% obciążenia 140-300 VAC @ 60-80% obciążenia 176-300 VAC @ 80-100% obciążenia
Maks. THDi	≤4% przy 100% obciążeniu; ≤6% przy 50% obciążeniu
Zakres częstotliwości	50 Hz lub 60 Hz (samoczynna adaptacja)
Kształt fali	Pełna fala sinusoidalna
Nominalne napięcie wyjściowe	208/220/230/240 V
THDv	≤1% przy 100% obciążeniu liniowym, ≤4% przy 100% obciążeniu nieliniowym
Regulacja napięcia (tryb bateryjny)	

	±1%
Częstotliwość (tryb baterii)	±0,1Hz
Złącze wejściowe	Zacisk
Typ wyjścia	Zacisk
Sprawność w trybie LINE [%] (pełne obciążenie)	94.0
Sprawność w trybie bateryjnym [%] (pełne obciążenie)	91.0
Czas transferu (tryb AC / linia lub tryb bateryjny do trybu ECO) [ms]	<10ms
Czas transferu (z trybu AC/liniowego do trybu bateryjnego) [ms]	0ms
Czas transferu (tryb ECO do trybu AC / trybu liniowego lub trybu	<10ms

bateryjnego) [ms]	
Czas transferu (z trybu liniowego lub trybu baterii do trybu obejścia) [ms]	0ms
Współczynnik szczytu	3:1
Dodatkowe cechy	Dostępny system uziemienia, Wyświetlacz LCD, Jednolity współczynnik mocy 1,0, Wyłącznik wejściowy, Dostępny zestaw baterii, Zgodność z generatorem prądotwórczym, EPO – awaryjne wyłączenie zasilania, AVR – Automatyczny regulator napięcia
Klasyfikacja IEC 62040-3	VFI-SS-111
Czas podtrzymania połowy obciążenia [min]	8.4

11) <u>4 szt Zasilacze awaryjne UPS</u> o minimalnych parametrach jak poniżej:

Typ	online
Obudowa	Rack

Kształt fali	Czysta fala sinusoidalna
Moc	3000W
Moc znamionowa	3kVA
Napięcie znamionowe	230VAC
Napięcie wejściowe	110VAC - 300VAC ± 5%
Napięcie wyjściowe	230VAC
Częstotliwość wyjściowa	50/60Hz ± 0.05HZ
Wbudowana bateria	Tak
Współczynnik mocy	1.0
Współczynnik szczytu	3:1
Czas przenoszenia	0ms

Przeciążenie	Przełączanie na bypass po 4ms
Gniazda	2 x SCHUKO 1 x RS 232
System komunikacji	USB, RS-232, EPO
Zabezpieczenia	- Przed przepięciem - Przed przeciążeniem - Przed zwarciem - Przed wysokim i niskim napięciem
Czas podtrzymania	1000W - 18 min 300W - 60min

12) <u>1 szt Zasilacza awaryjnego UPS</u> o minimalnych parametrach jak poniżej:

Typ	Jednofazowy online
Obudowa	Tower
Kształt fali	Czysta fala sinusoidalna

Wydajność energetyczna	3000VA / 2700W
Zakres częstotliwości	40Hz – 70Hz
THDv	≤2% przy 100% obciążeniu liniowym, ≤5% przy 100% obciążeniu nieliniowym
Napięcie wyjściowe	220/230/240 V
Sprawność w trybie LINE [%] (pełne obciążenie)	90.0
Czas transferu (tryb AC / linia do trybu bateryjnego) [ms]	0ms
Współczynnik mocy wyjściowej	0.9
Współczynnik szczytu obciążenia	3:1
Klasyfikacja IEC 62040-3	VFI-SS-111
Komunikacja	USB typu B – do oprogramowania monitorującego, RS-232

Czas podtrzymania pełnego obciążenia [min]	3.9

13) **<u>1 szt Zasilacza awaryjnego UPS</u>** o minimalnych parametrach jak poniżej:

Typ	Jednofazowy online
Obudowa	Tower
Kształt fali	Pełna fala sinusoidalna
Wydajność energetyczna	1000VA / 800W
Zakres częstotliwości	40Hz – 70Hz
THDv	≤2% przy 100% obciążeniu liniowym, ≤5% przy 100% obciążeniu nieliniowym≤3% @ 100% obciążenia liniowego, ≤6% @ 100% obciążenia nieliniowego
Napięcie wyjściowe	200/208/220/230/240 VAC.
Sprawność w trybie LINE [%] (pełne obciążenie)	88.0

Czas transferu (tryb AC / linia do trybu bateryjnego) [ms]	0ms
Czas transferu (tryb ECO do trybu AC / trybu liniowego lub trybu bateryjnego) [ms]	10ms
Współczynnik mocy wyjściowej	0.8
Współczynnik szczytu obciążenia	3:1
Klasyfikacja IEC 62040-3	VFI-SS-111
Komunikacja	USB typu B – do oprogramowania monitorującego, RS-232
Czas podtrzymania pełnego obciążenia [min]	3.9

14) **1 szt. Serwera** o minimalnych parametrach jak poniżej:

Obudowa	- Obudowa Tower, - Obudowa o głębokości poniżej 17”, - Możliwość instalacji do 3 dysków 3.5", - Panel Filtrujący.

Płyta główna	- Płyta główna z możliwością zainstalowania jednego procesora. - Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. - Na płycie głównej powinny znajdować się minimum 4 sloty przeznaczone dla pamięci - Obsługa min. 128GB RAM
Chipset	- Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych
Procesor	- Jeden procesor min. 6-rdzeniowy, min. 2.9GHz (Turbo min. 5.0GHz), osiągający min. 22 000 pkt. w teście PassMark CPU Mark, zgodnie z listą wyników opublikowanych na stronie https://www.cpubenchmark.net/cpu_list.php
Pamięć RAM	- 2x32GB pamięci RAM ECC UDIMM DDR5 o częstotliwości pracy min. 5600MT/s.
Karta graficzna	- Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1280x1024
Wbudowane porty	- min. 8 portów USB w tym min. 5 USB 3.2 Gen 1 - 1 port VGA - 1 port RS232
Gniazda PCI	- Min. 2 sloty PCIe generacji 4
Interfejsy sieciowe/ FC/SAS	- Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT
Kontroler RAID	- Sprzętowy kontroler dyskowy, posiadający

	a. Możliwość konfiguracji poziomów RAID: 0, 1, 10 b. Wsparcie dla dysków samoszyfrujących.
Dyski twarde	- Zainstalowane Min. 2 dyski SSD SATA o pojemności min. 960GB, 6Gb, Hot-Plug ze sprzętowym wsparciem permanentnego wymazywania danych. - Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Wentylatory	- Min. 1 wentylator z możliwą opcją montażu dodatkowego wentylatora wysokowydajnego (zgodnie z dokumentacją producenta serwera)
Zasilacze	- Zasilacz o mocy maks. min. 500W klasy min. Platinum
Bezpieczeństwo	- Możliwość wyłączenia w BIOS funkcji przycisku zasilania. - BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła - Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. - Moduł TPM 2.0 - Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem - Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	- Niezależna od zainstalowanego na serwerze systemu operacyjnego

	posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: a) zdalny dostęp do graficznego interfejsu Web karty zarządzającej; b) zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); c) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; d) możliwość podmontowania zdalnych wirtualnych napędów; e) wirtualną konsolę z dostępem do myszy, klawiatury; f) wsparcie dla IPv6; g) wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; h) możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; i) możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; j) integracja z Active Directory; k) możliwość obsługi przez dwóch administratorów jednocześnie; l) wsparcie dla dynamic DNS; ł)wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. m) możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera n) możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: a) Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej b) Przesyłanie danych telemetrycznych w czasie rzeczywistym c) Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze d) Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	Możliwość (opcja) zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: - Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych - integracja z Active Directory - Możliwość zarządzania dostarczonymi serwerami bez udziału

	dedykowanego agenta - Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish - Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram - Szczegółowy opis wykrytych systemów oraz ich komponentów - Możliwość eksportu raportu do CSV, HTML, XLS, PDF - Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. -Grupowanie urządzeń w oparciu o kryteria użytkownika - Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji - Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach - 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 - Możliwość definiowania ról administratorów - Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów - Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) - Możliwość instalacji 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 seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. - Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej

	podstawie weryfikacji środowiska w celu wykrycia rozbieżności. - Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile - Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. - Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. - Zdalne uruchamianie diagnostyki serwera. - Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. - Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	- Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 - Serwer musi posiadać deklaracja CE. - Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku - **Wykonawca**

	złoży dokument potwierdzający spełnianie wymogu. - Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022 oraz Microsoft Windows Server 2025.
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.
Warunki gwarancji	- Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii minimum 12 miesięcy. - Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. - Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. - Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. - Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. - 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 Producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: a. Możliwości utworzenia zgłaszania serwisowego w wyniku,

	którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. b. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. c. Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. d. Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. e. Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. - Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. - Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.
System operacyjny	- Microsoft Windows Server 2025 Standard 16C PL lub równoważny.

	Za równoważność rozumie się zakup produktu obejmującego licencję systemu operacyjnego, który zapewnia: - licencję obejmującą wszystkie rdzenie procesora(ów), - Obsługę Windows Server Containers. - Możliwość pełnienia funkcji drugiego kontrolera domeny Active Directory w istniejącej infrastrukturze Zamawiającego (zgodność z AD na poziomie Windows Server). - interfejsy użytkownika dostępne w wielu językach do wyboru - w tym polskim i angielskim, - graficzne środowisko instalacji i konfiguracji dostępne w języku polskim, - wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi), - zabezpieczenie hasłem dostępu do systemu, konta i profilu użytkowników, - mechanizmy logowania w oparciu o login i hasło, - Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy wielowątkowości współbieżnej (ang. Simultaneous Multi-Threading, SMT). - Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). - Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz

	narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. - Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. - Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. - Wsparcie dla środowisk Java i .NET Framework 6.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach. - Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe). c) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie minimum 2 aktywnych środowisk wirtualnych systemów operacyjnych. - Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. - Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. Dostarczone oprogramowanie musi być fabrycznie nowe - Nie dopuszcza się systemu typu REFURBISHED. W przypadku zaoferowania oprogramowania równoważnego względem wyspecyfikowanego przez Zamawiającego w opisie przedmiotu zamówienia, Wykonawca musi na swoją odpowiedzialność i swój koszt

	udowodnić, że zaoferowane produkty spełniają wszystkie wymagania i warunki określone w opisie przedmiotu zamówienia, w szczególności w zakresie: a) warunków licencji / sublicencji / subskrypcji zaoferowanych produktów równoważnych w każdym aspekcie, które nie mogą być gorsze niż dla produktów wymienionych w opisie przedmiotu zamówienia, b) funkcjonalności zaoferowanych produktów równoważnych, które nie mogą być ograniczone i gorsze względem funkcjonalności produktów wymienionych w opisie przedmiotu zamówienia, c) zakresu kompatybilności i współdziałania zaoferowanych produktów równoważnych ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego, który nie może być gorszy niż dla produktów wymienionych w opisie przedmiotu zamówienia, d) poziomu zakłóceń pracy środowiska systemowo-programowego Zamawiającego spowodowanego wykorzystaniem zaoferowanych produktów równoważnych, który nie może być większy niż w przypadku produktów wymienionych w opisie przedmiotu zamówienia; e) poziomu współpracy zaoferowanych produktów równoważnych z systemami Zamawiającego, który nie może być gorszy od tego, jaki zapewniają produkty wymienione w opisie przedmiotu zamówienia, f) zapewnienia pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności zaoferowanych produktów równoważnych z produktami wymienionymi w opisie przedmiotu zamówienia, g) warunków i zakresu usług gwarancji, asysty technicznej i konserwacji zaoferowanych produktów równoważnych, które nie mogą być gorsze niż dla produktów wymienionych w opisie przedmiotu zamówienia, h) obsługi przez zaoferowane produkty równoważne języków interfejsu, w ilości i rodzaju nie mniejszych niż oferują produkty wymienione w opisie przedmiotu zamówienia, i) wymagań sprzętowych dla zaoferowanych produktów równoważnych, które nie mogą być wyższe niż dla produktów wymienionych w opisie

	przedmiotu zamówienia, 2) W przypadku zaoferowania przez Wykonawcę produktu równoważnego Wykonawca dokona wspólnie z Zamawiającym instalacji i testowania produktu równoważnego w środowisku sprzętowo-programowym Zamawiającego. 3) W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane produkty. 4) W przypadku, gdy zaoferowany przez Wykonawcę produkt równoważny nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu produktu równoważnego. 5) Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów innego używanego i współpracującego z nim oprogramowania. 6) Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w jego nowszych wersjach.
Licencje CAL	- 30 Licencji CAL na urządzenie do powyższego systemu operacyjnego

Zadanie 2: Urządzenie klasy UTM

1szt. urządzenia klasy UTM (zawierającego zaawansowany Antywirus, audyt podatności i rozszerzony filtr URL) np. *UTM ST0RMSHIELD SN220 + Premium UTM Security Pack (UTM Security Pack + Zaawansowany Antywirus + Audyt Podatności + Rozszerzony filtr URL) wraz z subskrypcją zabezpieczeń i gwarancją + wdrożenie* lub równoważnego o minimalnych cechach równoważności jak poniżej:

Cechy równoważności:

ARCHITEKTURA SYSTEMU
• System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, umożliwiającej rozbudowę do dwóch takich samych urządzeń pracujących w klastrze wysokiej dostępności co najmniej Active-Passive, o specyfikacji opisanej poniżej • Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. • Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
• Metalowa obudowa typu desktop. • Możliwość zastosowania redundantnego zasilania, z wykorzystaniem zewnętrznego zasilacza. • Obsługa nielimitowanej ilości hostów w sieci chronionej. • Minimalna liczba i typ interfejsów fizycznych: •System realizujący funkcję Firewall musi dysponować minimum 8 interfejsami miedzianymi Ethernet 10/100/2500 •System realizujący funkcję Firewall musi dysponować minimum 1 interfejsem optycznym 1 GbE (SFP) •Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. • Minimalna liczba nowych połączeń na sekundę: 20 000 • Minimalna liczba jednoczesnych połączeń: 300 000 • Minimalna przepustowość Firewall: 4 Gbps • Minimalna przepustowość IPS: 2 Gbps • Minimalna przepustowość Threat Protection: 500 Mbps • Minimalna przepustowość IPSec VPN: 1 Gbps • System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB SSD do celów logowania i raportowania lub musi istnieć możliwość wykorzystania karty SD do celów logowania i raportowania.

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	1. Rozwiązanie musi być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. 8. Rozwiązanie musi oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora. 9. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP 10. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 11. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie. 12. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
Zapora sieciowa, konfiguracja sieciowa oraz routing	16. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. 17. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu

	SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 18. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług. 19. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. 20. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
Podstawowe kształtowanie pasma oraz limity ilości danych	1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia. 2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników	1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 100 kont. 2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP 3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory 4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. 6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Samoobsługowy portal dla użytkowników	2. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 3. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android 4. Rozwiązanie musi umożliwiać zmianę hasła.
Podstawowe opcje VPN	System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: 2. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) 3. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).

OCHRONA SIECI	
IPS	1. Urządzenie ma posiadać moduł wykrywania typu i wersji oprogramowania sieciowego, którego ruch jest filtrowany przez urządzenie. Moduł musi działać na urządzeniu. Nie dopuszcza się stosowania rozwiązania z agentem instalowanym na komputerach w sieci. Powyższy moduł ma nie tylko wykrywać oprogramowanie ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu 2. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur. 3. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 4. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. 5. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur 6. System musi generować alerty w przypadku wykrycia ataku.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP. 3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym 4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów. 5. System musi filtrować pliki na podstawie MIME. 6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 7. Rozwiązanie musi zawierać przynajmniej 77 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www. 8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS. 9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.

Ochrona i kontrola aplikacji	1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download. 2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
OCHRONA ANTYWIRUSOWA	
Ochrona i kontrola Email	1. Rozwiązanie ma posiadać silnik antywirusowy dostarczany od europejskiego dostawcy. 2. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy 3. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. 4. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 5. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 6. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 7. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 8. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. 9. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	

On-cloud Sandboxing	Rozwiązaniem musi posiadać dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności: 1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe 2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab 5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows.
LOGOWANIE I RAPORTOWANIE	
	1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 5. Rozwiązanie musi generować raporty w HTML i CSV. 6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 7. System musi zapewniać podgląd wykorzystania łącza internetowego. 8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP 9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
POZOSTAŁE	

Certyfikaty	Urządzenie musi posiadać: - certyfikat Common Criteria; - certyfikat ICSA Labs dla funkcji VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE;

GWARANCJA I SERWIS

Wymagania ogólne dla dostarczanych rozwiązań :

Dostarczone urządzenia musza być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji.

Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki,

Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu,

Całość dostarczonego sprzętu i oprogramowanie musi być ze sobą kompatybilna i pochodzić od jednego producenta,

Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Warunki gwarancji i serwisu :

Urządzenie ma być objęte rozszerzoną gwarancją typu NBD tzn. w przypadku zgłoszenia awarii urządzenia, wysyłka urządzenia zastępczego lub wysyłka sprawnego urządzenia musi nastąpić w dniu potwierdzenia awarii, a dostawa takiego urządzenia na wskazany przez zgłaszającego adres zaplanowana zostanie na kolejny dzień roboczy. Posiadanie rozszerzonej gwarancji NBD musi zostać potwierdzone licencją dystrybutora/producenta. Podmiot realizujący rozszerzoną gwarancję NBD musi posiadać certyfikat bezpieczeństwa informacji ISO27001 lub równoważny

Na dostarczany sprzęt musi być udzielona **min. 12-miesięczna gwarancja**; Zamawiający wymaga, by serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań,

Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę),

Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający:

- bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji
- dostęp do dokumentacji sprzętu i oprogramowania,
- dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej,
- dostęp do pomocy technicznej producenta.

Zamawiający w momencie odbioru otrzyma:

- licencje obejmujące wszystkie wymagane moduły na okres **min. 12 miesięcy**
- możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.

WYMAGANIA DODATKOWE
Posiadanie przez dostawcę wiedzy i doświadczenia:
• udokumentowanie minimum 10 lat doświadczenia w konfigurowaniu i wdrażaniu urządzeń systemu bezpieczeństwa UTM (Next Generation Firewall), • udokumentowane minimum 5 lat doświadczenia w konfigurowaniu i wdrażaniu rozwiązań zaoferowanego producenta, • posiadanie przynajmniej jednego certyfikatu inżynierskiego wydanego przez producenta na najwyższym poziomie umożliwiającym rozwiązywanie problemów technicznych, • posiadanie przynajmniej jednego certyfikatu producenta na poziomie trenerskim • udokumentowane i potwierdzone referencjami co najmniej trzy sprzedaże rozwiązań klasy UTM o wartości minimum 50 tys zł brutto każda w okresie ostatnich 3 lat.
USŁUGI
Zamawiający wymaga aby Dostawca w ramach dostawy zagwarantował:
• analizę aktualnej struktury sieci pod kątem wdrożenia rozwiązania klasy UTM • wdrożenie zaoferowanego rozwiązania w infrastrukturze Zamawiającego zgodnie z wymaganiami Zamawiającego oraz szkolenie przy-stanowiskowe z konfiguracji wdrożonego rozwiązania (wdrożenie i szkolenie musi się odbyć fizycznie w siedzibie zamawiającego – nie dopuszcza się wykonania prac w trybie zdalnym.) • 3 miesięczną dedykowaną opiekę powdrożeniową realizowaną zdalnie – wymagane jest aby do opieki wyznaczony był dedykowany inżynier z najwyższym certyfikatem producenta dostarczonego rozwiązania. Wsparcie powdrożeniowe musi być świadczone 7 dni w tygodniu w godzinach 8:00 – 20:00 – kontakt z inżynierem poprzez dedykowany bezpośredni numer telefonu.

Zadanie 3: <u>Wsparcie dla UTM Watchguard</u>

Wsparcie dla urządzeń UTM Watchguard – 5h do wykorzystania przez nielimitowany czas Możliwość skorzystania z pakietu wsparcia technicznego. W którego skład wsparcia wchodzi:

- Czas reakcji na pomoc techniczną 72h robocze,
- Konsultacja telefoniczna, mailowa lub za pomocą Chatu z inżynierem technicznym,
- 3 Certyfikowanych inżynierów watchguard (W tym jeden inżynier z certyfikatem trenerskim dla Watchguarda)
- Wymagany certyfikat ISO 9001

Zadanie 4: <u>System do wykonywania backupu danych.</u>

Czas trwania licencji – 12 miesięcy.

1. Produkt i dokumentacja dostępna w polskiej (i angielskiej) wersji językowej
2. Wsparcie dla systemów operacyjnych Windows typu serwer:

Systemy operacyjne Windows:

- Windows Server 2016, 2019, 2022, 2025 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Systemy operacyjne Linux:

System Linux z jądrem w wersjach od 2.6.9 do 6.9 i biblioteką glibc w wersji 2.3.4 lub nowszą, w tym następujące dystrybucje x86 and x86_64:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0-8.8*, 9.0-9.4*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04, 22.10, 23.04, 23.10, 24.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 37, 38
- SUSE Linux Enterprise Server 10, 11, 12, 15
- SUSE Linux Enterprise Server 12 i 15 - obsługa w systemach plików, z wyjątkiem Btrfs
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10.x, 11.x, 12
- CentOS 5.x, 6.x, 7.x, 8.x*
- CentOS Stream 8*,9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*,9.0-9.4* — wersje Unbreakable Enterprise Kernel i Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0-8.8*, 9.4*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.0 − 8.10*, 9.0 − 9.4*
- Rocky Linux 8.0 − 8.4*, 9.0 − 9.3*
- ALT Linux 7.0

3. Licencja dostępna w modelu subskrypcyjnym
4. Możliwość wdrożenia konsoli zarówno w trybie chmurowym jak i on-premis
5. Wsparcie i pełna funkcjonalność oprogramowania dla wielojęzykowych systemów operacyjnych
6. Obsługa środowiska chmurowego
7. Tworzenie kopii zapasowych dysków/partycji
8. Tworzenie kopii zapasowych plików i folderów
9. Replikacja kopii zapasowych do wielu lokalizacji docelowych
10. Tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
11. Kopie zapasowe i granularne przywracanie elementów aplikacji Microsoft Exchange, Microsoft SQL Server, Microsoft SharePoint i Microsoft Active Directory.
12. Możliwość przywrócenia kopii zapasowej dysku/partycji na innym komputerze o innej konfiguracji sprzętowej
13. Obsługa dysków twardych z sektorami o rozmiarze 4KB oraz dysków SSD

* Począwszy od wersji 8.4 obsługiwane tylko z jądrem w wersji od 4.18 i nowszej

14. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej

15. Zdalna instalacja i aktualizacja agentów na komputerach klienckich
16. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych oraz serwerach SFTP
17. Możliwość tworzenia niezmiennych magazynów przechowywania kopii zapasowych (tzw. immutable storage)
18. Możliwość generowania planu przywracania kopii zapasowych
19. Możliwość eksportu i importu planów tworzenia kopii zapasowych na różnych maszynach
20. Szablony schematów rotacji kopii zapasowych
21. Polecenia poprzedzające/następujące
22. Automatyczne usuwanie nieaktualnych kopii zapasowych (retencja)
23. Sprawdzanie poprawności i konsolidacja kopii zapasowych (pełnych, przyrostowych i różnicowych)
24. Wykonywanie zadań i tworzenie kopii zapasowych możliwe z poziomu wiersza polecenia.
25. Możliwość utworzenia ukrytej partycji widzianej tylko przez oprogramowanie do backupu na potrzeby zapisu kopii zapasowych, która będzie chroniona za pomocą hasła
26. Współpraca z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
27. Pełne, przyrostowe i różnicowe kopie zapasowe
28. Wysyłanie powiadomień pocztą e-mail
29. Szyfrowane kopii zapasowych algorytmem AES
30. Tworzenie dynamicznych grup urządzeń na podstawie nazwy urządzenia, ilości pamięci operacyjnej, zakresu adresów IP, typu systemu operacyjnego
31. Możliwość wykonywania czynności przenoszenia kopii zapasowych, replikacji, weryfikacji i czyszczenia na innym systemie.
32. Funkcjonalność ciągłej ochrony danych
33. Wbudowany moduł ochrony antywirusowej. Środowisko Windows
34. Możliwość integracji z Windows Defender Antyvirus
35. Filtrowanie adresów URL
36. Analiza podatności urządzenia (poszukiwanie luk w oprogramowaniu objętym ochroną), środowisko Windows
37. Funkcjonalność zdalnego pulpitu, możliwa do wywołania z poziomu serwera zarządzania oprogramowaniem backupowym środowisko Windows
38. Moduł automatycznego łatania wykrytych luk w oprogramowaniu środowisko Windows
39. Automatyczne tworzenie kopii zapasowej urządzenia, na którym ma zostać wdrożona poprawką
40. Możliwość wywołania funkcji zdalnego wymazywania danych w oparciu o mechanizm wbudowany w Windowsa 10
41. Funkcja aktywnej ochrony przed oprogramowaniem ransomware, chroniąca pliki lokalne i pliki kopii zapasowych przed zaszyfrowaniem. (Środowisko Windows)
42. Predefiniowany schemat tworzenia kopii zapasowych: G-F-S
43. Priorytetowe przywracanie systemu operacyjnego - Jeśli system uległ awarii, można go uruchomić w ciągu kilku sekund, a proces przywracania będzie wykonywany w tle.
44. Uruchamianie usług z minimalnymi prawami użytkownika

45. Zaawansowane raportowanie - możliwość tworzenia raportów w oparciu o predefiniowane schematy
46. Pomoc techniczna dostępna w języku polskim
47. Administrowanie kontami użytkowników Acronis i jednostkami organizacyjnymi
48. Tworzenie kryptograficznego odcisku pliku (sumy kontrolnej) wykorzystującego technologię blockchain
49. Wykonywanie kopii zapasowych uruchamiane po wystąpieniu określonych zdarzeń i warunków
50. Migawki wielowoluminowe
51. Kopia zapasowa „sektor po sektorze"
52. Obsługa dysków dynamicznych
53. Automatyczne ponawianie prób w przypadku niekrytycznych błędów (prób utworzenia kopii zapasowej)
54. Możliwość utworzenia nośnika startowego opartego na środowisku Linux lub WinPE