

Minimalne wymagania i ilość dostarczonego sprzętu :

1. **Serwer NAS – 1 szt.**
2. **Przełącznik sieciowy 24 portowy zarządzalny – 2 szt.**
3. **Przełącznik sieciowy 24 portowy PoE zarządzalny – 2 szt.**
4. **Przełącznik sieciowy 8 portowy zarządzalny – 3 szt.**
5. **Klaster UTM – 1 szt.**
6. **Kontroler sprzętowy – 1 szt.**
7. **Access Pointy – 3 szt.**
8. **Dostawa i wdrożenie systemu do analizy i agregacji logów oraz monitoringu zasobów systemu informatycznego**
9. **UPS do serwerów i szafy GPD – 1 szt.**
10. **Antywirus .**

1. Dysk sieciowy NAS – 1szt.

Nazwa	Minimalne wymagania dla sprzętu
Typ urządzenia	Serwer NAS
Obudowa	Rack 1U
Procesor	Czterordzeniowy procesor o taktowaniu 2,2 GHz osiągający w teście PassMark na sierpień 2022 co najmniej 4 580 punktów
Sprzętowy mechanizm szyfrowania	Tak (AES-NI)
Pamięć RAM	min. 8 GB pamięci ECC SODIMM z możliwością rozszerzenia do min. 32 GB
Możliwości rozbudowy	Sprzęt powinien być wyposażony w min. 4 kieszenie na dyski twarde typu hot-swap z możliwością rozszerzenia do 8 dysków łącznie przy użyciu dodatkowych jednostek rozszerzających podłączanych do jednostki głównej za pomocą portu eSATA.
Dyski twarde	Sprzęt powinien być wyposażony w 4 dyski o pojemności min. 8 TB 3,5" HDD o prędkości obrotowej 5400 rpm i interfejsem SATA 6 Gb/s
Porty zewnętrzne	Minimum: <ul style="list-style-type: none"> 2 porty USB 3.2.1 1 port eSATA (jako gniazdo rozszerzenia)
Porty sieciowe	Minimum: <ul style="list-style-type: none"> 4 porty 1GbE RJ45 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Funkcja Wake on LAN/WAN	Tak
Gniazdo rozszerzeń PCIe 2.0	Min. 1x 4-liniowe gniazdo x8 gen. 3
Wentylator obudowy	Min. 3 wentylatory (40 × 40 × 20 mm)
Obsługiwane protokoły sieciowe	Min. SMB1 (CIFS), SMB2, SMB3, NFSv3, NFSv4, NFSv4.1, NFS Kerberized sessions, iSCSI, HTTP, HTTPS, FTP, SNMP, LDAP, CalDAV
Obsługiwane systemy plików	Min.: <ul style="list-style-type: none"> Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
Zarządzanie pamięcią masową	<ul style="list-style-type: none"> Maksymalny rozmiar pojedynczego wolumenu: 108 TB Minimalny liczba wewnętrznych wolumenów: 64 Minimalny liczba obiektów iSCSI Target: 128 Minimalny liczba jednostek iSCSI LUN: 256 Obsługa klonowania/migawek jednostek iSCSI LUN
Obsługiwane typy macierzy RAID	Min. SHR, Basic, JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows® (ACL) i aplikacji
Wirtualizacja	Obsługa VMware vSphere with VAAI, Microsoft Hyper-V, Citrix, OpenStack
Usługa katalogowa	Integracja z usługami Windows® AD, logowanie użytkowników domeny przez protokoły SMB/NFS/AFP/FTP lub aplikację File Station, integracja z LDAP
Bezpieczeństwo	Zapora, szyfrowany folder współdzielony, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania, obsługa Let's Encrypt, HTTPS (dostosowywane mechanizmy szyfrowania)
Obsługiwane przeglądarki	Google Chrome®, Firefox®, Microsoft Edge®, Safari® 13 i nowsze oraz Safari (iOS 13.0 i nowsze) na urządzeniach iPad, Chrome (Android™ 11.0 i nowsze) na tabletach
Oprogramowanie	<ul style="list-style-type: none"> Urządzenie musi umożliwiać utworzenie przestrzeni dyskowej w oparciu o nowoczesny system plików, który będzie zapewniał obsługę migawek, generowania sum kontrolnych CRC a także

	<p>lustrzanych kopii metadanych aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów współdzielonych</p> <ul style="list-style-type: none"> Oprogramowanie zarządzające serwerem NAS musi zapewnić darmowe, kompleksowe rozwiązanie do tworzenia kopii zapasowych przeznaczone dla heterogenicznych środowisk IT, umożliwiające zdalne zarządzanie i monitorowanie ochrony komputerów, serwerów i maszyn wirtualnych na jednym, centralnym, przyjaznym dla administratora interfejsie. Ponadto gromadzone dane na urządzeniu mają mieć możliwość replikacji jako lokalne kopie zapasowe, sieciowe kopie zapasowe i kopie zapasowe danych w chmurach publicznych przy użyciu darmowego narzędzia instalowanego z Centrum Pakietów Wymaga się zapewnienia darmowej aplikacji do realizacji chmury prywatnej bez opłat cyklicznych, która będzie posiadała wygodną konsolę administratora zarządzaną z GUI a także agenty na urządzenia PC/MAC oraz aplikację mobilną na Android/iOS. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń a także wspierać algorytm Intelliversioning. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików office w czasie rzeczywistym. Urządzenie musi umożliwiać pracę w trybie klastra wysokiej dostępności (HA) aby zapewnić nieprzerwany, natychmiastowy dostęp do zasobów bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system). Wszystkie dane z powodzeniem zapisane na serwerze aktywnym będą na bieżąco kopiowane do serwera pasywnego zapewniając replikację w czasie rzeczywistym i dostęp do danych oraz usług w przypadku uszkodzenia jednostki aktywnej dając gwarancję ciągłości pracy. Utworzenie klastra HA ma się opierać o 2 identyczne urządzenia.
Montaż	<ul style="list-style-type: none"> Montaż urządzenia należy przeprowadzać przy użyciu dodatkowych, wygodnych w użyciu przesuwanych szyn rack
Gwarancja	<ul style="list-style-type: none"> 3 lata na urządzenia główne 1 rok na dodatkowe akcesoria montażowe w postaci przesuwanych szyn rack

Zakres instalacji i konfiguracji

- w urządzeniu należy zainstalować dyski twarde oraz wykonać ich konfigurację (RAID-5),
- urządzenie należy zainstalować w szafie RACK Zamawiającego.

2. Przełącznik sieciowy 24 portowy zarządzalny – 2 szt.

Nazwa	Minimalne wymagania dla sprzętu
Porty przełącznika	minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+
Port konsolowy	RJ45 (RS-232)
Szybkość przełączania	minimum 128Gb/s
Przepustowość	minimum 95Mp/s (dla pakietów 64Kb)
Bufor pakietów	minimum 1,5MB
Ramki Jumbo	minimum 10k
Tablica adresów MAC	minimum 16k
Tablica ACL	minimum 512
Tablica VLAN	minimum 4094
Taktowanie procesora	minimum 800MHz
Pamięć RAM	minimum 256MB
Zasilanie	zabudowany zasilacz 230V AC
Certyfikaty bezpieczeństwa	CE, RoHS
VLAN	Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
DHCP	IPv4/IPv6 DHCP Client, IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping, IPv4/IPv6 DHCP Server
Spanning tree	IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding
Agregacja łączy	IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance
Bezpieczeństwo	Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing, Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
Multicast	IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
Lista kontroli dostępu	IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
Diagnostyka	sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP
Zarządzanie	TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), Sntp/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
Oprogramowanie oraz wsparcie techniczne	oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
Dodatkowe wymagania	Dostarczenie wkładek światłowodowych oraz patchkord niezbędnych do połączenia przełączników w stack
Gwarancja	lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych.

3. Przełącznik sieciowy 24 portowy PoE zarządzalny – 2 szt.

Nazwa	Minimalne wymagania dla sprzętu
Porty przełącznika	minimum 24x 10/100/1000Base-T RJ45 PoE oraz minimum 4x 1/10GBase-X SFP+
Port konsolowy	RJ45 (RS-232)
Szybkość przełączania	minimum 128Gb/s
Przepustowość	minimum 95Mp/s (dla pakietów 64Kb)
Bufor pakietów	minimum 1,5MB
Ramki Jumbo	minimum 10k
Tablica adresów MAC	minimum 16k
Tablica ACL	minimum 512
Tablica VLAN	minimum 4094
Taktowanie procesora	minimum 800MHz
Pamięć RAM	minimum 256MB
Obsługa technologii PoE	IEEE 802.3 af/at
Budżet mocy PoE	minimum 370W
Zasilanie	zabudowany zasilacz 230V AC
Certyfikaty bezpieczeństwa	CE, RoHS
VLAN	Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ
DHCP	IPv4/IPv6 DHCP Client, IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping, IPv4/IPv6 DHCP Server
Spanning tree	IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding
Agregacja łączy	IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance
Bezpieczeństwo	Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing, Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,
Multicast	IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
Lista kontroli dostępu	IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN
Diagnostyka	sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP
Zarządzanie	TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), Sntp/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking
Funkcje PoE	Support IEEE 802.3at for all ports, PD failure detection, PoE scheduling
Oprogramowanie oraz wsparcie techniczne	oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
Dodatkowe wymagania	Dostarczenie wkładek światłowodowych oraz patchkord niezbędnych do połączenia przełączników w stack
Gwarancja	lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych.

4. Przełącznik sieciowy 8 portowy zarządzalny - 3szt.

Nazwa	Minimalne wymagania dla sprzętu
Porty przełącznika	minimum 8x 10/100/1000Base-T RJ45 oraz minimum 2x 100/1000Base-X SFP
Port konsolowy	RJ45 (RS-232)
Szybkość przełączania	minimum 20Gb/s
Przepustowość	minimum 14Mp/s (dla pakietów 64Kb)
Bufor pakietów	minimum 0,5MB
Ramki Jumbo	minimum 10k
Tablica adresów MAC	minimum 8k
Tablica ACL	minimum 1408
Tablica VLAN	minimum 4094
Taktowanie procesora	minimum 500MHz
Pamięć RAM	minimum 128MB
Zasilanie	zabudowany zasilacz 230V AC
Certyfikaty bezpieczeństwa	CE, RoHS
VLAN	Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Selective QinQ, Flexible QinQ
DHCP	IPv4/IPv6 DHCP Client, IPv4/IPv6 DHCP Relay, Option 82, Option 37/38, IPv4/IPv6 DHCP Snooping, IPv4/IPv6 DHCP Server
Spanning tree	IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding
Agregacja łączy	IEEE 802.3ad (LACP), 8 groups per device / 8 ports per group
Bezpieczeństwo	Storm Control based on packets and bytes, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing, Anti-ARP-Scan, ARP Binding, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting Radius, TACACS+
Multicast	IGMP v1/v2/v3 snooping, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication
Lista kontroli dostępu	IP ACL, MAC ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, VLAN ACL
Diagnostyka	VCT, DDM, Ping, Trace Route, RSPAN
Zarządzanie	TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMPv1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, , SNTN/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, CPU Mirror, IEEE 802.3ah/802.1ag OAM EFM, ULDP (like UDLD), LLDP/LLDP MED., auto provisioning
Oprogramowanie oraz wsparcie techniczne	oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług
Gwarancja	lifetime + min. 1 rok po wycofaniu produktu z linii produkcyjnej. W przypadku gdy produkt zostanie wycofany wcześniej niż 5 lat od daty zakupu, gwarancja powinna obowiązywać min. 6 lat.

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- konfiguracja interfejsu zarządzania, sieci VLAN, RSTP, dhcp snooping, syslog zgodnie z wytycznymi służb informatycznych.

5. Klaster UTM – 1szt.

Nazwa	Minimalne wymagania dla sprzętu
Obsługa sieci	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna (firewall)	<ol style="list-style-type: none"> 1. Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia. 6. Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac. 7. Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall. 8. Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł. 9. Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos. 10. Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego). 11. System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.
Intrusion prevention system (IPS)	<ol style="list-style-type: none"> 1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia. 6. Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS. 7. Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP. 8. Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0. 9. Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.
Kształtowanie pasma (traffic shapping)	<ol style="list-style-type: none"> 1. Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

	<ol style="list-style-type: none"> Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring). Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.
Ochrona antywirusowa	<ol style="list-style-type: none"> Urządzenie ma umożliwić rozbudowę o zaawansowany skaner antywirusowy dostarczany przez firmy trzecie (inne niż producent rozwiązania). Po rozbudowie administrator ma mieć możliwość określenia akcji w przypadku wykrycia zagrożenia bądź gdy analiza skanerem antywirusowym została zakończona błędem. Skaner antywirusowy ma pochodzić od europejskiego producenta. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. Po rozbudowie administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.
Ochrona antyspam	<ol style="list-style-type: none"> Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). Ochrona antyspam ma działać w oparciu o: <ol style="list-style-type: none"> białe/czarne listy, DNS RBL, Skaner heurystyczny. W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
Wirtualne sieci prywatne (VPN)	<ol style="list-style-type: none"> Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). Urządzenie ma wspierać co najmniej następujące typy sieci VPN: <ol style="list-style-type: none"> PPTP VPN, IPSec VPN, SSL VPN. SSL VPN ma działać w trybie tunelu. Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem. Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal) Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub 'n' Spoke oraz modconf. Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.
Filtr dostępu do stron www	<ol style="list-style-type: none"> Urządzenie ma posiadać wbudowany filtr URL. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. Administrator ma mieć możliwość dodawania własnych kategorii URL. Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej: <ol style="list-style-type: none"> blokowanie dostępu do adresu URL, zezwolenie na dostęp do adresu URL, blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych. Filtr URL musi uwzględniać komunikację po protokole HTTPS. Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.

	10. Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch
Uwierzytelnianie	<ol style="list-style-type: none"> Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o: <ol style="list-style-type: none"> lokalną bazę użytkowników (wewnętrzny LDAP), zewnętrzną bazę użytkowników (zewnętrzny LDAP), usługę katalogową Microsoft Active Directory. Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP. Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły: <ol style="list-style-type: none"> SSL, Radius, Kerberos. Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy. Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta. Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny. Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS). Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH. Rozwiązanie musi zapewniać Zero-Trust Network Access (ZTNA), dając dostęp do zasobów na podstawie analizy polityk bezpieczeństwa w oparciu co najmniej o weryfikację wersji systemu operacyjnego, statusu zapory sieciowej czy zainstalowanego programu antywirusowego na stacji
Administracja łączami do internetu (ISP)	<ol style="list-style-type: none"> Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing). Mechanizm równoważenia obciążenia łączy internetowego ma działać w oparciu o następujące dwa mechanizmy: <ol style="list-style-type: none"> równoważenie względem adresu źródłowego, równoważenie względem połączenia. Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. Urządzenie ma umożliwiać przełączenie na łączy zapasowe w przypadku awarii łączy podstawowego (tzw. Failover). Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łączy. W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnień, jitter, wskaźnika utraty pakietów). Monitorowanie dostępności łączy musi być możliwe w oparciu o ICMP oraz TCP.
Routing (trasowanie)	<ol style="list-style-type: none"> Urządzenie ma umożliwiać statyczne trasowanie pakietów. Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łączy zapasowe w przypadku awarii łączy podstawowego. Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing). Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPV2, OSPF oraz BGP. Rozwiązanie musi dawać możliwość wybrania predefiniowanego obiektu typu blackhole.
Administracja urządzeniem	<ol style="list-style-type: none"> Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezasyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.

	<ol style="list-style-type: none"> 3. Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP. 4. Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 5. Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 6. Urządzenie ma umożliwiać zarządzanie z poziomu konsoli (SSH) 7. Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania. 8. Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS. 9. Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup. 10. Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 11. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła. 12. Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording). 13. System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services). 14. Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników. 15. Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS). 16. Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX. 17. Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie: <ol style="list-style-type: none"> a. manualnego eksportu do pliku w dowolnym momencie czasu, b. automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu 18. Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzących bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora. 19. Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika. 20. Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.
Raportowanie	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego. 4. System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu. 6. System raportowania ma umożliwiać eksport wyników raportu do formatu CSV. 7. Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta. 8. Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3. 9. Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).
Pozostałe usługi i funkcje	<ol style="list-style-type: none"> 1. Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.

	<ol style="list-style-type: none"> Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay). Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6. Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny). Urządzenie ma posiadać usługę DNS Proxy. Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP). Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN. Urządzenie musi mieć zaimplementowane Open API Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie. Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
Gwarancja i serwis	<ol style="list-style-type: none"> Urządzenie ma być objęte 24-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa. W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal. Urządzenie ma posiadać do 28.03.2026 w ramach serwisu aktualizacje do FW+IPS, VPN, AS, filtr URL, Obsługa kart SD.
Parametry sprzętowe	<ol style="list-style-type: none"> Rozwiązanie ma być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive. Urządzenie ma być pozbawione dysku twardego, a oprogramowanie wewnętrzne musi działać na wbudowanej pamięci flash. Urządzenie ma być wyposażone w zintegrowany port na kartę microSD. Liczba portów Ethernet 2,5Gbps – min. 8. Liczba portów światłowodowych 1Gbps – min. 1. Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta. Przepustowość Firewall (1518 bajtów UDP) – minimum 8Gbps. Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 4Gbps. Przepustowość filtrowania Antywirusowego – minimum 1Gbps. Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2Gbps. Liczba tuneli VPN IPsec – minimum 100. Liczba tuneli typu SSL VPN (tryb tunelu) – minimum 100. Obsługa interfejsów 802.11q (VLAN) – minimum 128 Liczba równoczesnych sesji – minimum 400 000 i nie mniej niż 25 000 nowych sesji/sekundę. Urządzenie nie ma limitu na liczbę użytkowników. Liczba reguł filtrowania – minimum 8 192. Liczba tras statycznego routingu – minimum 512. Liczba tras dynamicznego routingu – minimum 10 000. Urządzenie ma umożliwiać podłączenie zewnętrznego nadmiarowego zasilacza (zasilanie redundantne). Stan pracy każdego zasilacza musi być sygnalizowany bezpośrednio na obudowie urządzenia. Urządzenie musi być wyposażone w moduł TPM.

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- przeniesienie konfiguracji z dotychczasowego urządzenia brzegowego do dostarczonego urządzenia,
- analiza aktualnej konfiguracji mechanizmów bezpieczeństwa oraz wprowadzenie zmian w konfiguracji urządzenia brzegowego mających na celu zwiększenie poziomu bezpieczeństwa cyfrowego,
- wprowadzenie do konfiguracji urządzenia UTM zmian umożliwiających izolację serwerów od sieci produkcyjnej oraz identyfikacja usług (portów) niezbędnych do zachowania komunikacji ze stacjami roboczymi użytkowników (bez konieczności zmiany adresacji IP),
- analiza ruchu z serwerów aplikacyjnych oraz odseparowanie tych serwerów od sieci Internet; identyfikacja i przepuszczenie połączeń niezbędnych do poprawnej pracy tych serwerów,
- połączenie urządzeń w klaster wysokiej dostępności HA w trybie Active-Passive,

- przeprowadzenie testów funkcjonowania klastra UTM,
- przygotowanie opisu konfiguracji oraz przekazanie go Zamawiającemu w wersji elektronicznej (edytowalnej).

Wykonawca zagwarantuje, że zadania określone powyżej wykonywać będzie osoba posiadająca niezbędne umiejętności w tym aktualny certyfikat kompetencji wystawiony przez producenta urządzenia lub autoryzowane centrum szkoleniowe.

6. Kontroler sprzętowy – 1 szt.

Nazwa	Minimalne wymagania
Porty	2 porty Ethernet 10/100Mb/s 1 port USB 2.0 1 port Micro USB
Zasilanie	PoE 802.3af/at PoE lub Micro USB (5V DC/ minimalnie 1A)
Funkcje transmisji bezprzewodowej	Funkcje zarządzania warstwy L3 Multi-SSID Równoważenie obciążenia pasma Sterowanie pasmem Airtime Fairness Kształtowanie wiązki Ograniczenie prędkości transmisji Harmonogram sieci bezprzewodowej QoS
Zabezpieczenia transmisji bezprzewodowej	Uwierzytelnianie przy pomocy strony powitalnej Kontrola dostępu Filtrowanie adresów MAC Izolacja klientów sieci bezprzewodowej Mapowanie SSID do VLAN Wykrywanie nieautoryzowanych AP
Zarządzanie AP	Automatyczne wykrywanie Jednorodna konfiguracja Harmonogram restartu Wspólna aktualizacja firmware'u Dioda ON/OFF
Uwierzytelnianie	Strona powitalna Filtrowanie MAC
Aplikacja	Dedykowana aplikacja
Zarządzanie centralne	Do 100 urządzeń
Dostęp do chmury	Tak
Gwarancja	2 lata na urządzenie

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- konfiguracja sieci WiFi zdefiniowanych przez Zamawiającego
- konfiguracja automatycznych kopii bezpieczeństwa

7. Access Point– 3 szt.

Nazwa	Minimalne wymagania
Porty	1 Port RJ45 2,5G PoE+
Zasilanie	802.3at PoE 12 V / 2 A DC (zasilacz w zestawie)
Typ anteny	Wewnętrzne, dookólne: 2,4 GHz: 4× 4 dBi 5 GHz: 4× 5 dBi
Montaż	Montaż sufitowy/naścienny (zestawy montażowe muszą znajdować się w zestawie)
Liczba jednoczesnych klientów	510+
Standardy bezprowadowe	Wi-Fi 6 2,4 GHz: IEEE 802.11 b/g/n/ax 5 GHz: IEEE 802.11 a/n/ac/ax
Częstotliwość pracy	2,4 GHz i 5 GHz
Maksymalna teoretyczna przepustowość	5 GHz: do 4804 Mb/s 2,4 GHz: do 1148 Mb/s
Funkcje transmisji bezprowadowej	1024-QAM 4 razy dłuższy symbol OFDM OFDMA Multi-SSID (do 16 SSID, 8 dla każdego pasma) Wł./wył. transmisji bezprowadowej Automatyczny wybór kanału Kontrola mocy transmisji (na podstawie dBm) QoS (WMM) MU-MIMO HE160 (Szerokość kanału 160 MHz) Płynny roaming Omada Mesh Sterowanie pasmem Równoważenie obciążenia pasma Airtime Fairness Beamforming Ograniczanie prędkości Harmonogram restartu Harmonogram sieci bezprowadowej Statystyki sieci bezprowadowej w oparciu o SSID/AP/klienta
Bezpieczeństwo transmisji bezprowadowej	Uwierzytelnianie przy pomocy strony powitalnej Kontrola dostępu Filtrowanie adresów MAC Izolacja klientów połączonych z siecią bezprowadową Mapowanie SSID do VLAN Wykrywanie nieautoryzowanych AP Obsługa 802.1X Szyfrowanie WPA-Personal/Enterprise, WPA2-Personal/Enterprise, WPA3-Personal/Enterprise
Dostęp do chmury	Tak
Gwarancja	2 lata na urządzenie

Zakres instalacji i konfiguracji

- aktualizacja oprogramowania firmware do najnowszej wersji,
- montaż AP w pomieszczeniach wskazanych przez Zamawiającego.
- wykonawca musi dostarczyć wszystkie niezbędne do montażu materiały (np. przewody, koryta, itp.),

8. Dostawa i wdrożenie systemu do analizy i agregacji logów oraz monitoringu zasobów systemu informatycznego

Zamawiający wymaga dostawy, uruchomienia i konfiguracji (zgodnie z wymogami Zamawiającego) systemu do analizy i agregacji logów oraz monitoringu urządzeń sieci LAN. Rozwiązanie może funkcjonować na maszynie wirtualnej pracującej w zasobach Zamawiającego. Zamawiający dopuszcza zastosowanie rozwiązań opartych o systemy licencjonowane jak również open source.

Oczekiwana funkcjonalność systemu do analizy i agregacji logów oraz monitoringu zasobów systemu informatycznego:

Nazwa	Minimalne wymagania
Zastosowanie	Centralne gromadzenie i analizy logów urządzeń sieci komputerowej oraz monitoring zasobów systemu informatycznego z wysyłaniem powiadomień i alarmów.
System agregacji logów - opis funkcjonalności	System scentralizowanej agregacji logów wykonujący ich analizę w czasie rzeczywistym i generujący powiadomienia dla administratora sieci o wykrytych zagrożeniach lub nieprawidłowościach. System powinien być instalowany w sieci lokalnej nabywcy i wyposażony w lokalną bazę danych, nie może wykorzystywać połączenia z internetem w celu utrzymania funkcjonalności oraz nie może wymagać opłaty subskrypcji/licencji do działania i aktualizacji. Oprogramowanie musi być wyposażone w intuicyjny interfejs graficzny pozwalający na zarządzanie logami przez lokalnego administratora sieci, wykorzystywać graficzne metody wizualizacji danych w postaci wykresów/tabel oraz posiadać możliwość filtrowania danych i ich eksportu do pliku pdf. Rozwiązanie powinno posiadać mechanizm odrzucania zbędnych informacji w celu zminimalizowania wielkości bazy danych. Narzędzie musi posiadać możliwość dostosowania retencji danych. Przesyłanie informacji do serwera logów musi być realizowane przez jednostronne połączenia (wysyłka z monitorowanego urządzenia na serwer) w oparciu o SYSLOG UDP
System agregacji logów - zakres wdrożenia	<ol style="list-style-type: none"> 1. przygotowanie systemu do odbierania i analizy logów z urządzeń wskazanych przez Zamawiającego (bramy sieciowe, przełączniki, punkty dostępu bezprzewodowego i ich kontrolery, sieciowe systemy operacyjne, serwery pamięci NAS/SAN, kontrolery serwerów, zarządcy maszyn wirtualnych, zasilacze awaryjne) oraz krytycznego oprogramowania, 2. zapewnienie wsparcia lokalnego administratora sieci w konfiguracji urządzeń oraz oprogramowania do wysyłki logów w przypadku braku wbudowanych mechanizmów za to odpowiedzialnych, 3. konfiguracja mechanizmu powiadamiania o zdarzeniach z wykorzystaniem szyfrowanego protokołu SMTP na wskazaną przez Zamawiającego skrzynkę mailową (wielokrotne wywołania alertów w ciągu wyznaczonego przez Zamawiającego czasu powinny być kondensowane do jednej wiadomości), 4. przygotowanie paneli wizualizacji danych z wykresami statystyk ilości odbieranych logów, statystyk logów z poszczególnych urządzeń, filtrów pozwalających na wyświetlenie logów pojedynczych urządzeń, 5. optymalizacja systemu pod względem ilości danych tak, aby tygodniowy przyrost rozmiaru bazy danych nie przekraczał 30 MB.
System do monitoringu zasobów informatycznych - opis funkcjonalności	<p>System do scentralizowanej agregacji informacji dotyczących parametrów technicznych urządzeń sieciowych oraz monitoringu pracy urządzeń, aplikacji, baz danych i systemów operacyjnych.</p> <p>System powinien być zainstalowany w sieci lokalnej nabywcy i wyposażony w lokalną bazę danych, nie może wykorzystywać połączenia z internetem w celu utrzymania funkcjonalności oraz nie może wymagać opłaty subskrypcji/licencji do działania i aktualizacji.</p> <p>Oprogramowanie musi być wyposażone w intuicyjny interfejs graficzny pozwalający na zarządzanie przez lokalnego administratora sieci, wykorzystywać graficzne metody wizualizacji danych w postaci wykresów, tabel oraz map. Rozwiązanie powinno posiadać mechanizm definiowania rodzaju i częstotliwości przesyłania danych. Narzędzie musi posiadać możliwość dostosowania retencji danych. Komunikacja z serwerem musi być realizowana przez protokół SNMP (v2 i v3) oraz z wykorzystaniem dedykowanego agenta dla systemów Windows i Linux. W przypadku wykorzystania agenta system musi umożliwiać pracę w dwóch trybach:</p> <ol style="list-style-type: none"> 1. wysyłanie informacji do serwera w oparciu o zdefiniowane reguły, 2. wysyłanie informacji na podstawie zapytania serwera.
System do monitoringu zasobów	<ol style="list-style-type: none"> 1. instalacja i konfiguracja systemu, 2. podłączenie wszystkich urządzeń wskazanych przez Zamawiającego,

informatycznych - zakres wdrożenia	<ol style="list-style-type: none"> 1. optymalizacja zakresu pozyskiwanych danych i informacji na podstawie wytycznych Zamawiającego, 2. przygotowanie map graficznych sieci LAN, 3. przygotowanie wykresów i raportów, 4. konfiguracja powiadamiania, 5. zapewnienie wsparcia lokalnego administratora sieci w konfiguracji urządzeń oraz oprogramowania do współpracy z systemem, 6. konfiguracja mechanizmu powiadamiania o alarmach i ostrzeżeniach z wykorzystaniem szyfrowanego protokołu SMTP na wskazaną przez Zamawiającego skrzynkę mailową, 7. optymalizacja systemu pod względem ilości danych tak, aby tygodniowy przyrost rozmiaru bazy danych nie przekraczał 30 MB.
Dodatkowe wymagania	<ol style="list-style-type: none"> 1. Zamawiający dopuszcza możliwość połączenia wymienionych wyżej funkcjonalności w jeden, zintegrowany system. 2. Wykonawca zagwarantuje Zamawiającemu dostęp do bezpłatnej pomocy technicznej w okresie 2 lat od dnia zakończenia wdrożenia. 3. System musi umożliwiać tworzenie własnych funkcji (makr) służących do przeprowadzania obliczeń na podstawie pozyskanych informacji oraz konstruowania własnych punktów kontrolnych z określeniem wartości granicznych. 4. System musi mieć możliwość zbierania informacji i informowania administratora min. o: <ul style="list-style-type: none"> • błędnym i poprawnym logowaniu do serwerów, • kończącej się przestrzeni dyskowej serwerów i pamięci sieciowych, • dostępności aktualizacji oprogramowania serwerów NAS, • nadmiernym obciążeniu procesora i pamięci RAM w określonym przedziale czasowym, • braku komunikacji z dowolnym urządzeniem i o przywróceniu takiej komunikacji, • zmianie przepustowości na wybranych połączeniach lub portach urządzeń sieciowych, • unieruchomieniu wybranych usług i serwisów pracujących na serwerach, • zestawieniu tunelu szyfrowanego do urządzenia brzegowego UTM, • niedostępności tras urządzenia brzegowego.

Zamawiający dopuszcza aby dostarczone oprogramowanie do analizy i agregacji logów oraz monitoringu zasobów systemu informatycznego było rozwiązaniem komercyjnym, w takim przypadku Zamawiający wymaga zagwarantowania wsparcia technicznego oraz ważnej licencji do 28.03.2026r. . Zastosowanie rozwiązania komercyjnego nie może ograniczać Zamawiającego w zakresie liczby urządzeń wysyłających logi i informacje do system oraz liczby przesyłanych logów. W przypadku zastosowania rozwiązania typu open source. Zamawiający wymaga wsparcia serwisowego do 28.03.2026 polegającego na okresowej (nie rzadziej niż co 6 miesięcy) aktualizacji wszystkich modułów, programów i środowiska operacyjnego oraz pomocy w rozwiązywaniu ewentualnych problemów z funkcjonowaniem systemu.

9. UPS do serwerów i szafy GPD – 1 szt.

Nazwa komponentu	Minimalne parametry techniczne
Technologia	online, podwójne przetwarzanie
Moc wyjściowa	6kVA/6kW; PF=1
Obudowa	Rack/Tower (zestaw do montażu w szafie rack w komplecie)
Napięcie wejściowe	110 ÷ 275 V AC ± 3 %
Napięcie znamionowe (wartość skuteczna)	230V AC
Prąd znamionowy (wejście)	27,4A
Częstotliwość napięcia wejściowego (zakres oraz tolerancja)	45 ÷ 55 / 55 ÷ 65 Hz ± 1 Hz
Częstotliwość znamionowa napięcia wejściowego	50Hz / 60Hz
Zniekształcenia prądu wejściowego THDi	< 3%
Zakres napięcia wyjściowego	208/220/230/240V AC konfigurowalne z poziomu oprogramowania oraz z menu zasilacza na wyświetlaczu LCD
Zniekształcenia napięcia wyjściowego THDu	< 1% dla Pmax (liniowe) < 5% (nieliniowe wg PN EN 62040-3)
Gniazda wyjściowe	2x IEC320 C13 (10A) + listwa zaciskowa
Akumulatory wewnętrzne / Moduły bateryjne	- komplet (min. 20 szt.) baterii 12V o minimalnej pojemności 9Ah dedykowane do UPS, - baterie umieszczone wewnątrz urządzenia lub w zewnętrznym module baterijnym - możliwość podpięcia min 4 szt. modułów bateryjnych - każdy wyposażony w minimum 20 szt. akumulatorów 12V9Ah
Czas podtrzymania UPS + 1 MODUŁ dla obciążenia 6kW/4,8kW/3kW	7 / 10 / 19 min
Przebieżalność	105-125% - 10min / 125-150% - 30s / >150% - 500ms
Ilość i typ gniazd wyjściowych w UPS	min 2x IEC 320 C13 (10 A) niesterowalne, listwa zaciskowa oraz opcja zamontowania dodatkowego modułu PDU wyposażonego w minimum 2x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16A) niesterowalne oraz 2x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16A) sterowalne; listwa zaciskowa
Bypass zewnętrzny	Wymagany, umożliwiający bezprzerwowe odłączenie zasilacza ups do celów serwisowych (odpowiedni do oferowanego zasilacza, w obudowie naściennej lub rack)
EPO	Wymagane – standard NC
Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD oraz diody sygnalizujące stan pracy: usterkę, pracę baterijną, pracę w trybie online, obejście bypass
Wymagane certyfikaty	CE, ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisu; (załączyć dokument w języku polskim)
Komunikacja z urządzeniem	RS232, USB HID, styki bezpotencjałowe 1-wejście; 1-wyjście; karta zarządzania SNMP

Oprogramowanie do monitorowania pracy zasilacza UPS	Tego samego producenta co UPS, bezpłatne bez ograniczeń funkcjonalności oraz ilości podłączonych stanowisk komputerowych; pod Windows 10, Windows 11, Windows Server 2019, Windows Server 2022, Linux - możliwość pobierania ze strony producenta i dokonywania aktualizacji przez użytkownika bez dodatkowych kosztów (potwierdzone oświadczeniem producenta oprogramowania)
Serwis producenta	wymagany, zlokalizowany na terenie Polski, autoryzacja serwisowa lub oświadczenie producenta - załączyć do oferty
Gwarancja	Minimum 24 miesiące elektronika, 24 miesiące akumulatory, serwis door to door, czas naprawy 5 dni roboczych
Dokumentacja	Instrukcja w języku polskim oraz oświadczenie producenta o posiadaniu licencji oraz pełnych praw do oprogramowania do monitorowania pracy UPS

1) Zakres instalacji i konfiguracji

- urządzenia należy podłączyć do instalacji Zamawiającego w serwerowni (GPD) za pośrednictwem dedykowanego bypass-u zewnętrznego (dostarczonego razem z urządzeniem),
- w urządzeniu należy zainstalować kartę SNMP oraz wykonać jej wstępną konfigurację,
- konfiguracja serwera syslog w celu wysyłania informacji i powiadomień do serwera GrayLog oraz Zabbix,
- wykonawca musi dostarczyć wszystkie niezbędne do podłączenia materiały (np. przewody, zaciski, gniazda),

10. Antywirus

ESET -przejsięcie na wyższą wersję programu z Firewall

Zmiana terminu obowiązywania licencji na program antywirusowy ESET wraz ze zmianą rodzaju licencji

Dane aktualnej licencji:

Rodzaj: ESET PROTECT Essential ON-PREM

Liczba licencji: 42

Data ważności: 2025-02-20

Dane nowej licencji:

Rodzaj: ESET PROTECT Advanced lub inna zawierająca moduły Firewall oraz Sandboxing w chmurze

Liczba licencji: 53

Data rozpoczęcia abonamentu: 2025-02-20

Data ważności: 2026-03-28

Konsola zarządzająca: w chmurze ESET