

Opis Przedmiotu Zamówienia
do postępowania na realizację zamówienia pn.:

Dostawa, wdrożenie i uruchomienie sprzętu i oprogramowania
dla potrzeb cyberbezpieczeństwa

Część 1
1. Serwer do wykonywania kopii zapasowych - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none"> Obudowa Rack 19" o wysokości max 2U Minimum 14 wnęk na dyski , w tym minimum 12 na dyski 3.5" Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającej Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS lub równoważnych środowisk mobilnych) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	<ul style="list-style-type: none"> Płyta główna z możliwością zainstalowania do dwóch procesorów. Obsługa procesorów 32 rdzeniowych. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	<ul style="list-style-type: none"> Dedykowany przez producenta procesor do pracy w serwerach dwuprocesorowych
Procesor	<ul style="list-style-type: none"> Zainstalowany jeden procesor min. 12-rdzeniowy, min. 2.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 216 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej
RAM	<ul style="list-style-type: none"> 128GB DDR5 RDIMM 5600MT/s
Kontroler RAID	<ul style="list-style-type: none"> Sprzętowy kontroler dyskowy, posiadający <ul style="list-style-type: none"> Min. 8GB nieulotnej pamięci cache, Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących
Dyski twarde	<ul style="list-style-type: none"> Zainstalowane: <ul style="list-style-type: none"> 2x dysk SSD SATA o pojemności min. 480GB, Hot-Plug 8x dysk SATA o pojemności min. 12TB, Hot-Plug Możliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności min. 960GB Hot-Plug z możliwością konfiguracji RAID 1

Gniazda PCI	<ul style="list-style-type: none"> Dwa sloty PCIe
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Czteroportowa karta 12Gb SAS HBA
Wbudowane porty	<ul style="list-style-type: none"> 4 porty USB w tym min: <ul style="list-style-type: none"> 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy 2 port VGA z czego jeden z przodu obudowy Możliwość rozbudowy o port RS232
Video	<ul style="list-style-type: none"> Zintegrowana karta graficzna umożliwiające wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	<ul style="list-style-type: none"> Redundantne, Hot-Plug
Zasilacze	<ul style="list-style-type: none"> Redundantne, Hot-Plug min. 700W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkové oprogramowanie	<ul style="list-style-type: none"> Windows Server 2025 Standard dla procesora określonego powyżej lub równoważny, z prawem do legalnego użytkowania przez Zamawiającego. Licencja musi obejmować wymaganą liczbę rdzeni procesora zgodnie z zasadami licencjonowania producenta.
Bezpieczeństwo	<ul style="list-style-type: none"> Zatrzaśk górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania. 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 dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera 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 lub równoważnymi. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta Zarządzania	<ul style="list-style-type: none"> Niezależna od zainstalowanego na serwerze systemu operacyjnego

	<p>posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające:</p> <ul style="list-style-type: none"> o zdalny dostęp do graficznego interfejsu Web karty zarządzającej o szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika o możliwość podmontowania zdalnych wirtualnych napędów o wirtualną konsolę z dostępem do myszy, klawiatury o wsparcie dla IPv6 o wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH o możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer o integracja z Active Directory o możliwość obsługi przez ośmiu administratorów jednocześnie o Wsparcie dla automatycznej rejestracji DNS o wsparcie dla LLDP o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej o możliwość podłączenia lokalnego poprzez złącze RS-232. o możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. o Monitorowanie zużycia dysków SSD o możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, o Automatyczne zgłaszanie alertów do centrum serwisowego producenta o Automatyczne update firmware dla wszystkich komponentów serwera o Możliwość przywrócenia poprzednich wersji firmware o Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON o Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych o Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram o Możliwość wykrywania odchyłań konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera o Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS lub równoważnych środowisk mobilnych) przy użyciu jednego z protokołów BLE lub WIFI.
Oprogramowanie do zarządzania	<ul style="list-style-type: none"> • Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: <ul style="list-style-type: none"> o Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych o integracja z Active Directory o Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta o Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish o Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram o Szczegółowy opis wykrytych systemów oraz ich komponentów o Możliwość eksportu raportu do CSV, HTML, XLS, PDF o Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. o 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 modułarnych 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.
- Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:
 - wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów
 - wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji
 - z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
 - inwentaryzacja komponentów w serwerze i ich mikrokodów
 - historia poboru mocy i temperatury serwera
 - zbieranie danych diagnostycznych serwera do paczki serwisowej

Gwarancja	<ul style="list-style-type: none"> • Minimum 36 miesięcy gwarancji producenta • Możliwości zgłaszania zdarzeń serwisowych do serwisu producenta w trybie 24/7/365 telefonicznie i przez Internet • Certyfikowany technik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki • Naprawa ma odbyć się w siedzibie Zamawiającego • W przypadku wystąpienia awarii dysku twardego, uszkodzony dysk twardy pozostaje u Zamawiającego
Prace wdrożeniowe	<p>Instalacja serwera szafie rack</p> <p>Podłączenie serwera do zasilania i podsieci wskazanych przez Zamawiającego</p> <p>Instalacja i konfiguracja dostarczonego serwerowego systemu operacyjnego zgodnego z wymaganiami OPZ oraz środowiskiem Zamawiającego</p>

2. Urządzenie Network Attached Storage (NAS) - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Procesor	Procesor czterordzeniowy 64-bitowy o taktowaniu nie niższym niż 2.2GHz
Obudowa	Rack 19" o wysokości max. 2U wraz z kompletem szyn umożliwiającym zamontowanie w szafie Rack
Pamięć RAM	Minimum 4 GB DDR4 ECC Możliwość rozszerzenia pamięci RAM do 32GB.
Liczba zatok na dyski twarde	Minimum 8
Dyski twarde	Obsługiwane dyski 3.5" SATA HDD oraz 2.5" SATA HDD i SSD Zainstalowane minimum 8 dysków 3.5" SATA HDD o pojemności 16 TB każdy o parametrach nie gorszych niż: prędkość obrotowa: 7200 RPM, MTBF: 2 500 000, pamięć podręczna: 512 MB, obciążenie roczne: 550 TB Możliwość aktualizacji oprogramowania dysku z poziomu systemu operacyjnego oferowanego urządzenia
Możliwość podłączenia modułu rozszerzającego	Tak
Minimalna ilość dysków z opcjonalnymi modułami rozszerzającymi	Nie mniej niż 12
Porty na karty rozszerzeń	Minimum 1 x Gen3 x8 slot (x4 link)
Porty LAN	Wbudowane min. 4 porty RJ-45 1GbE Dwuportowa karta PCIe 10 GbE w standardzie SFP+
Porty USB 3.2	Minimum 2

Port eSATA	Minimum 1
Zasilanie	Redundantny zasilacz o mocy minimalnej 350W
Mechanizm szyfrowania sprzętowego	Tak, min AES-NI
Wewnętrzny system plików	BTRFS, EXT4 lub równoważny
Obsługiwane tryby RAID	JBOD, RAID 0, RAID 1, RAID 5, RAID 6, RAID 10 lub równoważny
Uprawnienia	Uprawnienia listy kontroli dostępu systemu Windows (ACL)
Usługa katalogowa	Urządzenie musi umożliwiać użytkownikom domenowym logowanie oraz dostęp do plików za pośrednictwem protokołów SMB, FTP, WebDAV oraz portalu/przeglądarki plików dostępnej przez interfejs WWW.
Bezpieczeństwo	<p>Obsługa WORM (Write Once Read Many - jeden zapis, wiele odczytów) dla folderów współdzielonych i migawek, zaporę sieciową, szyfrowanie folderu współdzielonego, szyfrowanie całego woluminu, szyfrowanie SMB, FTP przez SSL/TLS, SFTP, rsync przez SSH, automatyczne blokowanie logowania przy nieuprawnionym dostępie dla protokołów HTTP, HTTPS, SMB, SSH, Telnet, rsync, FTP, HTTPS (dostosowywane mechanizmy szyfrowania), dwuetapowa weryfikacja logowania (2FA), adaptacyjna metoda logowania dla konta administratora (AMFA), możliwość logowania za pomocą klucza sprzętowego w standardzie FIDO2, U2F, grupowanie reguł powiadomień (zdarzenia systemowe) dla różnych adresów e-mail.</p> <p>Urządzenie musi obsługiwać certyfikaty publiczne, w tym automatyczne pozyskiwanie i odnawianie certyfikatów z wykorzystaniem protokołu ACME lub rozwiązania równoważnego.</p>
Oprogramowanie do kopii zapasowej	<p>Oferowany NAS powinien być wyposażony oprogramowanie do kopii zapasowej. Minimalne wymagane funkcje oprogramowania do backupu:</p> <ul style="list-style-type: none"> • kopia zapasowa całego systemu Windows (bare-metal), przywracanie w trybie bare-metal • kopia zapasowa maszyn wirtualnych (VMware, Hyper-V lub równoważnych) • kopia zapasowa systemów Windows, Linux oraz macOS lub równoważnych systemów operacyjnych wykorzystywanych przez Zamawiającego • obsługa deduplikacji, kopii przyrostowej, kompresji i szyfrowania • obsługa wielu wersji i retencji • możliwość wyzwalania kopii zapasowej według harmonogramu, • obsługa klastra przełączania awaryjnego Microsoft Hyper-V • automatyczna weryfikacja utworzonych kopii zapasowych maszyn wirtualnych i serwerów fizycznych, za pomocą utworzonego nagrania wideo z odtworzenia w formie maszyny wirtualnej • centralne zarządzanie • konfiguracja nowych i edycja istniejących zadań kopii zapasowej wielu komputerów i serwerów fizycznych z poziomu jednej centralnej konsoli zarządzającej, w tym minimum w zakresie liczby i czasu przechowywanych wersji, harmonogramu i woluminów objętych backupem dla poszczególnych zadań • portal użytkownika do przywracania danych kopii zapasowej (bez uprawnień administratora) • delegowanie uprawnień do zarządzania kopią zapasową i przywracaniem dla

	<p>użytkowników bez uprawnień administratora</p> <ul style="list-style-type: none"> wykonywanie kopii zapasowych usług chmury publicznej typu Microsoft 365, Google Workspace lub usług równoważnych, w zakresie poczty, plików, kont użytkowników i danych współdzielonych.
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, a także lustrzanych kopii metadanych, aby zapewnić całkowitą integralność danych biznesowych. Dodatkowo wspomniany system musi wspierać ustawienie limitu dla folderów współdzielonych oraz szybkie klonowanie całych folderów udostępnionych 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 lub równoważne środowiska mobilne. Usługa powinna umożliwiać udostępnianie zasobów serwera NAS, synchronizację i tworzenie kopii zapasowych podłączonych urządzeń. Ponadto omawiana usługa powinna umożliwiać pracę z dokumentami biurowymi (edytor tekstowy, arkusz kalkulacyjny, pokaz slajdów) i wspierać wersjonowanie oraz edycję tworzonych plików biurowych jednocześnie przez wielu użytkowników Możliwość tworzenia klastra wysokiej dostępności (HA) z dwóch identycznych serwerów NAS, bez widocznych zmian w użytkowaniu (konfiguracja jako jeden spójny system), z funkcją automatycznego przełączania dostępu do usług i danych na serwer pasywny w przypadku awarii serwera aktywnego. Możliwość utworzenia klastra bez konieczności przywracania serwera aktywnego do ustawień fabrycznych Możliwość tworzenia kopii zapasowej danych z serwera na zewnętrzne dyski twarde (USB), do chmur publicznych i serwera rsync Obsługa minimum 256 migawek na folder współdzielony i minimum 4096 migawek na cały system Funkcja serwera VPN (OpenVPN, L2TP/IPSec) dla minimum 8 jednoczesnych połączeń
Gwarancja	Minimum 36 miesięcy producenta (łącznie z dyskami i dodatkowymi akcesoriami takimi, jak dodatkowa karta sieciowa)
Prace wdrożeniowe	<p>Instalacja NAS'a szafie rack</p> <p>Podłączenie NAS'a do zasilania i podsieci wskazanych przez Zamawiającego</p> <p>Konfiguracja RAID</p> <p>Konfiguracja uwierzytelniania 2FA dla potrzeb administratora</p> <p>Podłączenie do systemu backup'u wymienionego w pkt. 4</p>

3. Napęd taśmowy (streamer) - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Napęd	Napęd LTO-9 zewnętrzny z interfejsem min. SAS 6Gb. Prędkość zapisu danych bez kompresji – minimum 300 MB/sek.
Obudowa	Obudowa desktop wyposażona dedykowany wentylator i przycisk włączania/wyłączania.
Pojemność	Pojemność bez kompresji – minimum 18 TB, pojemność ze sprzętową kompresją 2:1– minimum 30TB

Funkcjonalność	<p>Urządzenie powinno być wyposażone w następujące funkcje:</p> <ul style="list-style-type: none"> • LTFS z partycjonowaniem nośników, umożliwiające zapisanie na nośniku systemu plików oraz kopiowanie i odczyt informacji bez konieczności korzystania z aplikacji backupowej. LTFS powinien wspierać minimum systemy Windows, MacOS, Linux • wsparcie dla technologii POST • wsparcie dla aplikacji ITDT • Dynamic Speed Matching – dynamiczne dopasowanie prędkości zapisu do napływających informacji • odczyt i zapis nośników: LTO-8 i LTO-9 RW i WORM • automatyczne szyfrowanie danych metodą AES 256-bit • automatyczna sprzętowa kompresja danych
Wyposażenie	<p>Kabel SAS umożliwiający podłączenie urządzenia do serwera, długość min. 2m.</p> <p>Wraz z urządzeniem należy dostarczyć 10 kompatybilnych taśm danych o pojemności bez kompresji minimum 18 TB każda oraz 1 taśmę czyszczącą.</p>
Gwarancja	Minimum 36 miesięcy gwarancji producenta.
Prace wdrożeniowe	Podłączenie urządzenia do serwera wymienionego w pkt 1

4. Oprogramowanie do wykonywania kopii zapasowych 35 serwerów fizycznych i wirtualnych - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter</p> <p>Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022 i 2025. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux..</p> <p>Oprogramowanie musi współpracować z platformami wirtualizacyjnymi wykorzystywanymi przez Zamawiającego, w szczególności VMware vSphere/vCenter, ESXi, VMware vSAN, lub rozwiązaniami równoważnymi, w zakresie backupu, odtwarzania, replikacji, raportowania i integracji administracyjnej.</p> <p>Oprogramowanie musi umożliwiać odtwarzanie i uruchamianie maszyn wirtualnych w środowiskach VMware, Hyper-V, Nutanix AHV lub równoważnych platformach wirtualizacyjnych.</p>
Całkowite koszty posiadania	<p>Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej</p> <p>Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.</p> <p>Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.</p> <p>Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.</p>

	<p>Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.</p> <p>Oprogramowanie musi wspierać niezmiennosc kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu.</p> <p>Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.</p> <p>Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu.</p> <p>Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API.</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.</p> <p>Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji.</p> <p>Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania.</p> <p>Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</p> <p>Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej.</p>
Wymagania RPO	<p>Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.</p> <p>Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.</p> <p>Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastora.</p> <p>Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware.</p> <p>Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.</p> <p>Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy.</p> <p>Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).</p> <p>Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi klasy enterprise, takimi jak Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi, Infinidat InfiniGuard lub rozwiązaniami równoważnymi, zapewniającymi deduplikację, kompresję, retencję, niezmiennosc kopii oraz udokumentowaną integrację z oferowanym systemem backupu.</p> <p>Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.</p>

	<p>Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.</p> <p>Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.</p> <p>Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punktu w ramach ustalonego parametru RPO.</p> <p>Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik</p> <p>Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)</p> <p>Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).</p>
Wymagania RTO	<p>Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.</p> <p>Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.</p> <p>Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.</p> <p>Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL i Oracle bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne.</p> <p>Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.</p> <p>Oprogramowanie musi umożliwiać odtworzenie maszyn lub danych do głównych platform chmury publicznej, w tym Microsoft Azure, Microsoft Azure Stack, Amazon EC2, Google Cloud Platform lub rozwiązań równoważnych.</p> <p>Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.</p> <p>Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell.</p> <p>Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.</p> <p>Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów</p>

	<p>AD Sites oraz pozwalać na odtworzenie haseł.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.</p> <p>Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux.</p> <p>Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI.</p> <p>Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN</p>
Ograniczenie ryzyka	<p>Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).</p> <p>Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.</p> <p>Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem.</p> <p>Oprogramowanie musi umożliwiać integrację z rozwiązaniami antywirusowymi lub antymalware poprzez udokumentowany mechanizm integracyjny, np. API, CLI, ICAP, skrypt lub konektor, w celu skanowania zawartości kopii przed odtworzeniem danych.</p> <p>Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.</p>
Środowiska fizyczne	<p>Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego.</p> <p>Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych.</p> <p>Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE lub dystrybucje równoważne stosowane w środowiskach serwerowych.</p> <p>Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix.</p> <p>Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą).</p> <p>Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów.</p> <p>Rozwiązanie musi wspierać backup podłączonych dysków USB.</p>

	<p>Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym.</p> <p>Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury).</p> <p>Rozwiązanie musi wspierać deduplikację oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone.</p> <p>Rozwiązanie musi wspierać kontrolę pasma sieciowego.</p> <p>Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych.</p> <p>Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN.</p> <p>Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft.</p> <p>Rozwiązanie musi wspierać technologię BitLocker.</p> <p>Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania.</p> <p>Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych.</p> <p>Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL i Oracle poprzez bezpośrednie uruchomienie ich z pliku backupu.</p> <p>Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform.</p> <p>Rozwiązanie musi wspierać szyfrowanie.</p> <p>Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne.</p> <p>Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego.</p> <p>Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej.</p> <p>Rozwiązanie musi wspierać tworzenie wielu zadań backupowych.</p>
Raportowanie	<p>System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie.</p> <p>System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.</p> <p>System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V.</p> <p>System musi umożliwiać eksport raportów do popularnych formatów edytowalnych i nieedytowalnych, w szczególności DOCX, XLSX, VSDX, PDF lub formatów równoważnych.</p> <p>System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc.</p> <p>System musi mieć możliwość ustawienia harmonogramu generowania raportów</p>

	<p>i dostarczania ich do odbiorców w określonych przez administratora interwałach.</p> <p>System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów.</p> <p>System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych.</p> <p>System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych.</p> <p>System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury.</p> <p>System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta.</p> <p>System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.</p> <p>System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach 'what-if'.</p> <p>System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy Vmware.</p> <p>System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots).</p> <p>System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie.</p>
Gwarancja	Gwarancja wsparcia technicznego i dostępności aktualizacji oprogramowania w celu utrzymania systemu w aktualnym i bezpiecznym stanie musi być zapewniona na okres co najmniej 12 miesięcy.
Prace wdrożeniowe	<p>Instalacja i konfiguracja oprogramowania na serwerze wymienionym w pkt. 1.</p> <p>Stworzenie listy serwerów podlegających backup'owi.</p> <p>Stworzenie harmonogramu wykonywania kopii zapasowych oraz ich retencji.</p> <p>Stworzenie listy repozytoriów.</p> <p>Stworzenie harmonogramu sprawdzania poprawności wykonywanych kopii zapasowych dla wskazanych przez Zamawiającego serwerów.</p>

Część 2

1. Urządzenie UTM (Unified Threat Management) - 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.</p> <p>Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do</p>

	<p>poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP.</p> <p>Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
Interfejsy, Dysk, Zasilanie	<p>System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:</p> <ul style="list-style-type: none"> • 8 portami Gigabit Ethernet RJ-45 • 4 gniazdami SFP 1 Gbps • 8 gniazdami SFP+ 10 Gbps <p>System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.</p> <p>System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System jest wyposażony w zasilanie 2xAC.</p>
Parametry wydajnościowe	<p>W zakresie Firewall'a obsługa nie mniej niż 10 mln jednoczesnych połączeń oraz 380 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps.</p> <p>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 35 Gbps.</p> <p>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 9 Gbps.</p> <p>Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 6 Gbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 6 Gbps.</p>
Funkcje Systemu Bezpieczeństwa	<p>Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</p> <p>Kontrola Aplikacji.</p> <p>Poufność transmisji danych - połączenia szyfrowane IPSec VPN.</p> <p>Ochrona przed malware.</p> <p>Ochrona przed atakami - Intrusion Prevention System.</p> <p>Kontrola stron WWW.</p> <p>Kontrola zawartości poczty – Antyspam dla protokołów SMTP.</p> <p>Zarządzanie pasmem (QoS, Traffic shaping).</p> <p>Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe,</p>

	<p>które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</p> <p>Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.</p> <p>Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</p>
Polityki, Firewall	<p>Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.</p> <p>Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <ul style="list-style-type: none"> • System musi umożliwiać integrację z platformami SDN, wirtualizacyjnymi i chmurowymi, takimi jak Cisco ACI, OpenStack, VMware NSX, Kubernetes, AWS, Azure, GCP lub rozwiązaniami równoważnymi, w celu dynamicznego wykorzystania informacji o zasobach przy budowie polityk bezpieczeństwa.
Połączenia VPN	<p>System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</p>

Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ul style="list-style-type: none"> • Routingu statycznego. • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. • Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. • BFD (Bidirectional Forwarding Detection). • Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<p>System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<p>System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
Ochrona przed malware	<p>Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</p> <p>System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratorium producenta.</p> <p>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
Ochrona przed atakami	<p>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p>

	<p>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie</p>
Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>System musi umożliwiać kontrolę aplikacji chmurowych, usług społecznościowych, usług współdzielenia dokumentów, usług synchronizacji plików oraz popularnych wyszukiwarek, z możliwością kontroli działań użytkowników, takich jak pobieranie i wysyłanie plików.</p> <p>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).</p> <p>System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
Kontrola WWW	<p>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.</p> <p>System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych</p>

	<p>mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
Zarządzanie	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.</p> <p>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>
Logowanie	<p>W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
Kable/wkładki	4x kabel DAC 10GbE SFP+/SFP+ 0.5m
Gwarancja	<p>Minimum 12 miesięcy gwarancji producenta.</p> <p>Dostęp do aktualizacji oprogramowania i wsparcie techniczne producenta w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.</p> <p>Dostęp do aktualnych baz funkcji ochronnych i serwisów producenta w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, na okres min.12 miesięcy</p>
Prace wdrożeniowe	<p>Instalacja urządzeń w szafie rack.</p> <p>Konfiguracja klastra HA.</p> <p>Instalacja i konfiguracja urządzeń w sieci LAN i WAN Zamawiającego.</p> <p>Konfiguracja routingu pomiędzy sieciami VLAN.</p> <p>Przepisanie konfiguracji z obecnie pracujących urządzeń UTM/router celem zachowania ciągłości funkcjonowania systemu IT Zamawiającego.</p>

2. Urządzenie UTM (Unified Threat Management) - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.</p> <p>Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
Interfejsy, Dysk, Zasilanie	<p>System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:</p> <ul style="list-style-type: none"> • 8 portami Gigabit Ethernet RJ-45. • 2 gniazdami SFP+ 10 Gbps. <p>System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.</p> <p>System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System jest wyposażony w zasilanie AC.</p>
Parametry wydajnościowe	<p>W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.</p> <p>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.</p> <p>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 4 Gbps.</p> <p>Wydajność skanowania ruchu o charakterystyce typowej dla środowiska</p>

	<p>przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.</p>
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <ul style="list-style-type: none"> • Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. • Kontrola Aplikacji. • Poufność transmisji danych - połączenia szyfrowane IPSec VPN. • Ochrona przed malware. • Ochrona przed atakami - Intrusion Prevention System. • Kontrola stron WWW. • Kontrola zawartości poczty – Antyspam dla protokołów SMTP. • Zarządzanie pasmem (QoS, Traffic shaping). • Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. • Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. • Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system. • Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	<p>Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.</p> <p>Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <ul style="list-style-type: none"> • System musi umożliwiać integrację z platformami SDN, wirtualizacyjnymi i chmurowymi, takimi jak Cisco ACI, OpenStack, VMware NSX, Kubernetes, AWS, Azure, GCP lub rozwiązaniami równoważnymi, w celu dynamicznego wykorzystania informacji o zasobach przy budowie polityk bezpieczeństwa.
Połączenia VPN	<p>System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20.

	<ul style="list-style-type: none"> • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.</p>
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ul style="list-style-type: none"> • Routingu statycznego. • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. • Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. • BFD (Bidirectional Forwarding Detection). • Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<p>System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<p>System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
Ochrona przed malware	<p>Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</p> <p>System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla</p>

	<p>systemu operacyjnego Android).</p> <p>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
Ochrona przed atakami	<p>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>System musi umożliwiać kontrolę aplikacji chmurowych, usług społecznościowych, usług współdzielenia dokumentów, usług synchronizacji plików oraz popularnych wyszukiwarek, z możliwością kontroli działań użytkowników, takich jak pobieranie i wysyłanie plików.</p> <p>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
Kontrola WWW	<p>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażań regularnych (Regex).</p> <p>Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści</p>

	<p>w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.</p> <p>System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
Zarządzanie	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.</p> <p>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>
Logowanie	<p>W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
Gwarancja	Minimum 12 miesięcy gwarancji producenta.

	<p>Dostęp do aktualizacji oprogramowania i wsparcie techniczne producenta w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.</p> <p>Dostęp do aktualnych baz funkcji ochronnych i serwisów producenta w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, na okres min.12 miesięcy</p>
Prace wdrożeniowe	<p>Instalacja i konfiguracja urządzeń w sieci LAN i WAN Zamawiającego.</p> <p>Przepisanie konfiguracji z obecnie pracujących urządzeń UTM/router celem zachowania ciągłości funkcjonowania systemu IT Zamawiającego.</p>

3. Urządzenie UTM (Unified Threat Management) - 4 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.</p> <p>System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji.</p> <p>Powinna istnieć możliwość dedykowania co najmniej 5 administratorów do poszczególnych instancji systemu.</p> <p>System wspiera protokoły IPv4 oraz IPv6 w zakresie:</p> <ul style="list-style-type: none"> • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego.
Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
Interfejsy, Dysk, Zasilanie	<p>System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 10 portów Gigabit Ethernet RJ-45.</p> <p>System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.</p> <p>System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System jest wyposażony w zasilanie AC.</p>
Parametry wydajnościowe	<p>W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 90 tys. nowych połączeń na sekundę.</p>

	<p>Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.4 Gbps.</p> <p>Wydajność szyfrowania IPsec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.</p> <p>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.3 Gbps.</p> <p>Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.2 Gbps.</p>
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <p>Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.</p> <p>Kontrola Aplikacji.</p> <p>Poufność transmisji danych - połączenia szyfrowane IPsec VPN.</p> <p>Ochrona przed malware.</p> <p>Ochrona przed atakami - Intrusion Prevention System.</p> <p>Kontrola stron WWW.</p> <p>Kontrola zawartości poczty – Antyspam dla protokołów SMTP.</p> <p>Zarządzanie pasmem (QoS, Traffic shaping).</p> <p>Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</p> <p>Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.</p> <p>Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).</p>
Polityki, Firewall	<p>Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.</p> <p>System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.</p> <p>Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <ul style="list-style-type: none"> • System musi umożliwiać integrację z platformami SDN, wirtualizacyjnymi i chmurowymi, takimi jak Cisco ACI, OpenStack, VMware NSX, Kubernetes,

	AWS, Azure, GCP lub rozwiązaniami równoważnymi, w celu dynamicznego wykorzystania informacji o zasobach przy budowie polityk bezpieczeństwa.
Połączenia VPN	<p>System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługa protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie VPN jest dostępne jako opcja i nie jest wymagane w implementacji.</p>
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ul style="list-style-type: none"> • Routingu statycznego. • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. • Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. • BFD (Bidirectional Forwarding Detection). • Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<p>System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<p>System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
Ochrona przed malware	<p>Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP,</p>

	<p>HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</p> <p>System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
Ochrona przed atakami	<p>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p> <p>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>System musi umożliwiać kontrolę aplikacji chmurowych, usług społecznościowych, usług współdzielenia dokumentów, usług synchronizacji plików oraz popularnych wyszukiwarek, z możliwością kontroli działań użytkowników, takich jak pobieranie i wysyłanie plików.</p> <p>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
Kontrola WWW	<p>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p>

	<p>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.</p> <p>System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
Zarządzanie	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.</p> <p>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>
Logowanie	<p>W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p>

	<p>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
Gwarancja	<p>Minimum 12 miesięcy gwarancji producenta.</p> <p>Dostęp do aktualizacji oprogramowania i wsparcie techniczne producenta w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.</p> <p>Dostęp do aktualnych baz funkcji ochronnych i serwisów producenta w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), antyspam, Web Filtering, bazy reputacyjne adresów IP/ domen, na okres min. 12 miesięcy</p>
Prace wdrożeniowe	<p>Instalacja i konfiguracja urządzeń w sieci LAN i WAN Zamawiającego</p> <p>Przepisanie konfiguracji z obecnie pracujących urządzeń UTM/router celem zachowania ciągłości funkcjonowania systemu IT Zamawiającego</p>

4. Zarządzalne urządzenie sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch) - 2 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa, zasilanie	<p>Obudowa Rack o wysokości max 1U.</p> <p>Dwa redundantne zasilacze AC 230V, z możliwością wymiany czasie pracy.</p>
Interfejsy sieciowe	<p>24 porty 1GbE/10GbE SFP/SFP+</p> <p>2 porty 100GbE/40GbE QSFP28/QSFP+</p>
Zarządzanie	<p>Dedykowany interfejs 1Gb Ethernet RJ-45 do zarządzania.</p> <p>Wbudowany port konsoli szeregowej do pełnego zarządzania.</p> <p>Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).</p> <p>Wsparcie dla SNMP w wersjach 1-3.</p> <p>Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.</p> <p>Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.</p> <p>Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline</p> <p>Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).</p> <p>Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.</p> <p>Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.</p> <p>Automatycznie wykonywane rewizje konfiguracji.</p>
Parametry wydajnościowe	<p>Przepustowość urządzenia - min. 880 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 1300 Mpps</p> <p>Tablica adresów MAC o pojemności - co najmniej 64 tys. wpisów</p> <p>Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund</p>
Wymagane funkcje	<p>Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń</p> <p>Obsługa Jumbo Frames</p>

[Handwritten signatures and initials]

	<p>Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree)</p> <p>Agregacja portów zgodna ze standardem 802.3ad</p> <p>Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q</p> <p>Obsługa routingu statycznego</p> <p>Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP</p> <p>Port-mirroring</p> <p>Uwierzytelnianie 802.1x na poziomie portu</p> <p>Uwierzytelnianie 802.1x w oparciu o adres MAC</p> <p>W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).</p> <p>W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia</p> <p>W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN</p> <p>Obsługa protokołu sFlow</p> <p>Obsługa MACsec PSK mode i MACsec Dynamic-CAK mode</p>
<p>Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania</p>	<p>Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ul style="list-style-type: none"> • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego • Automatyczna detekcja i rekomendacje konfiguracji • Przesyłanie logów na zewnętrzny serwer syslog • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników • Obsługa białych i czarnych list adresów MAC • Wykrywanie aplikacji komunikujących się w sieci • Realizowanie funkcji Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym • Zapewnienie routingu statycznego i dynamicznego (co najmniej OSPF) oraz Policy Based Routing'u
Kable/wkładki	12x kabel DAC 10GbE SFP+/SFP+ min. 5m
Gwarancja	<p>Minimum 12 miesięcy gwarancji producenta</p> <p>Dostęp do aktualizacji oprogramowania i wsparcie techniczne producenta w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.</p>
Prace wdrożeniowe	<p>Instalacja urządzeń w szafie rack</p> <p>Konfiguracja klastra HA</p> <p>Stworzenie podsieci VLAN</p>

5. Zarządzalne urządzenie sieciowe z obsługą VLAN, MACsec, standardu 802.1X (switch) - 3 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa, zasilanie	Obudowa Rack o wysokości max 1U Dwa redundantne zasilacze AC 230V, z możliwością wymiany czasie pracy
Interfejsy sieciowe	24 porty 1GbE/2.5GbE/5GbE RJ-45 4 porty 10GbE/25GbE SFP+/SFP28
Zarządzanie	<p>Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ul style="list-style-type: none"> • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej • Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego • Automatyczna detekcja i rekomendacje konfiguracji • Przesyłanie logów na zewnętrzny serwer syslog • Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników • Obsługa białych i czarnych list adresów MAC • Wykrywanie aplikacji komunikujących się w sieci • Realizowanie funkcji Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym <p>Zapewnienie routingu statycznego i dynamicznego (co najmniej OSPF) oraz Policy Based Routing'u.</p>
Parametry wydajnościowe	<p>Przepustowość urządzenia - min. 440 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 650 Mpps</p> <p>Tablica adresów MAC o pojemności - co najmniej 64 tys. wpisów</p> <p>Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund</p>
Wymagane funkcje	<p>Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ul style="list-style-type: none"> • Centralne zarządzanie konfiguracją urządzenia • Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania • Centralne zarządzanie sieciami VLAN • Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u • Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp. • Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów,

	<p>urządzenie powinno przenieść go do strefy odizolowanej</p> <ul style="list-style-type: none"> Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego Automatyczna detekcja i rekomendacje konfiguracji Przesyłanie logów na zewnętrzny serwer syslog Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników Obsługa białych i czarnych list adresów MAC Wykrywanie aplikacji komunikujących się w sieci Realizowanie funkcji Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym <p>Zapewnienie routingu statycznego i dynamicznego (co najmniej OSPF) oraz Policy Based Routing'u</p>
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania	<p>Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:</p> <ul style="list-style-type: none"> Centralne zarządzanie konfiguracją urządzenia Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania Centralne zarządzanie sieciami VLAN Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp. Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego Automatyczna detekcja i rekomendacje konfiguracji Przesyłanie logów na zewnętrzny serwer syslog Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników Obsługa białych i czarnych list adresów MAC Wykrywanie aplikacji komunikujących się w sieci Realizowanie funkcji Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym Zapewnienie routingu statycznego i dynamicznego (co najmniej OSPF) oraz Policy Based Routing'u
Gwarancja	<p>Minimum 12 miesięcy gwarancji producenta</p> <p>Dostęp do aktualizacji oprogramowania i wsparcie techniczne producenta w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię</p>
Prace wdrożeniowe	<p>Instalacja urządzeń w szafie rack</p> <p>Stworzenie podsieci VLAN</p>

6. Oprogramowanie do zarządzania uprzywilejowanym dostępem (PAM) - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania	Zapewnienie wysokiego poziomu bezpieczeństwa danych i poufności informacji.

funkcjonalne	<p>Wsparcie dla szyfrowania danych w transmisji i przechowywaniu haseł i kluczy.</p> <p>Elastyczność w zakresie skalowania infrastruktury w celu obsługi zwiększonego obciążenia.</p> <p>System musi posiadać mechanizmy failover i redundancji, aby zapewnić ciągłość działania w przypadku awarii serwera lub innego komponentu.</p> <p>System musi posiadać interfejs graficzny (GUI) umożliwiający łatwe zarządzanie kontami uprzywilejowanymi i monitorowanie działań użytkowników.</p> <p>Musi istnieć możliwość sprawdzania silnikiem antywirusowym przesyłanych podczas sesji plików. Kontrola musi być realizowana co najmniej dla transferu plików poprzez web (Web SFTP, Web SAMBA) oraz SCP.</p> <p>Automatyczne blokowanie niebezpiecznych poleceń za pomocą profilu filtrowania SSH. System musi monitorować komendy wydawane przez operatora sesji.</p> <p>System PAM powinien być dostarczony jako urządzenie na utwardzonym przez jednego producenta systemie operacyjnym w formie gotowego i pełnego rozwiązania.</p> <p>Rozwiązanie musi być dostępne w formie urządzeń wirtualnych (virtual appliance) dla VMWare, Hyper-V oraz KVM.</p> <p>Działanie PAM musi pozwalać na obsługę połączeń bezpośrednich jak i proxy.</p> <p>Możliwość obsługi niestandardowych protokołów chociażby poprzez dedykowane wyzwalacze (custom application launcher).</p> <p>Możliwość ostrzegania użytkowników o nagrywaniu w celu zapewnienia zgodności z wymaganiami RODO.</p> <p>System musi obsługiwać moduł vTPM (Virtual Trusted Platform Module) dla przechowywania kluczy prywatnych użytkowników.</p> <p>System musi obsługiwać mechanizm awaryjnego dostępu do zaszyfrowanych haseł przechowywanych w systemie na zasadzie procedury „glass breaking”. Wszystkie działania w tym trybie muszą być logowane celem możliwości przeprowadzenia audytu.</p> <p>System musi automatycznie nagrywać obraz podczas uruchomienia procedury awaryjnej (glass breaking).</p> <p>Automatyczna zmiana hasła konta po poprawnym zalogowaniu.</p> <p>Wsparcie dla zaplanowanej zmiany haseł według harmonogramu.</p> <p>Możliwość tworzenia procedury żądania dostępu do haseł i zatwierdzania takich żądań poprzez konfigurowalną ilość administratorów.</p> <p>Ustawienie dedykowanego dostępu do skonfigurowanego hasła dla jednego administratora. W tym stanie dostęp jest ograniczony tylko dla jednego użytkownika uprzywilejowanego.</p> <p>Wymagane jest wsparcie dla algorytmów szyfrowania SSH o wysokiej sile.</p> <p>Zaawansowany protokół uwierzytelniania RDP, w tym CredSSP i TLS.</p> <p>Kontrola dostępu oparta na rolach (RBAC).</p> <p>Kontrola uprawnień oparta na użytkownikach oraz grupach użytkowników.</p> <p>Kontrola profili dostępowych w formie polityk.</p> <p>Wsparcie dla Disaster Recovery.</p> <p>Użytkownik uprzywilejowany musi mieć możliwość pracy co najmniej w następujących trybach:</p> <ul style="list-style-type: none"> • Agentowa – dostępne wszystkie funkcjonalności. Agent musi być dostępny bezpłatnie • Bezagentowo - za pomocą przeglądarki internetowej wraz z dedykowanym rozszerzeniem. Metoda ta musi umożliwiać uzupełnianie haseł przez PAM oraz nagrywanie sesji • Bezagentowo - za pomocą przeglądarki internetowej bez dodatkowych rozszerzeń.
--------------	---

Uwierzytelnianie	<p>Obsługa uwierzytelniania użytkowników za pomocą certyfikatów</p> <p>Możliwość korzystania z lokalnej bazy danych użytkowników</p> <p>Obsługa uwierzytelniania wieloskładnikowego opartego na SAML</p> <p>Obsługa OIDC (openID Connect), SAML</p> <p>Obsługa wielu połączeń SAML SP</p> <p>Możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.</p> <p>Możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji</p> <p>Dostęp do zasobów użytkowników uprzywilejowanych musi również obejmować możliwości blokady w oparciu o dodatkowe parametry:</p> <ul style="list-style-type: none"> • Kontrola dostępu oparta na adresie źródłowym IP użytkownika • Ograniczanie dostępu oparte na harmonogramie użytkownika
Monitorowanie i raportowanie	<p>Możliwość monitorowania aktywności użytkowników z kontami uprzywilejowanymi.</p> <p>Generowanie szczegółowych raportów audytowych w celu analizy i śledzenia działań użytkowników.</p>
Licencjonowanie	<p>Oprogramowanie musi być objęte kompletną licencją producenta na całe rozwiązanie. Nie dopuszcza się dodatkowych wymagań licencyjnych dla systemu operacyjnego, bazy danych, oprogramowania serwera WWW lub podobnych.</p> <p>Licencja systemu musi pozwalać na jednoczesne podłączenie się co najmniej 10 aktywnych użytkowników do monitorowanych zasobów.</p>
Gwarancja	<p>Gwarancja wsparcia technicznego i dostępności aktualizacji oprogramowania w celu utrzymania systemu w aktualnym i bezpiecznym stanie musi być zapewniona na okres co najmniej 12 miesięcy.</p>
Prace wdrożeniowe	<p>Instalacja i konfiguracja oprogramowania na serwerze HA wymienionym w Części 3.</p> <p>Założenie użytkowników.</p> <p>Podłączenie Active Directory, systemu backup'u i UTM'ów do systemu PAM.</p> <p>Przypisanie trzem wybranym użytkownikom (administratorom Zamawiającego) praw dostępu do trzech przykładowych systemów.</p>

7. Urządzenie UTM (Unified Threat Management) - 5 szt.

Parametr	Charakterystyka (wymagania minimalne)
Wymagania ogólne	<p>Obsługa uwierzytelniania użytkowników za pomocą certyfikatów</p> <p>Możliwość korzystania z lokalnej bazy danych użytkowników</p> <p>Obsługa uwierzytelniania wieloskładnikowego opartego na SAML</p> <p>Obsługa OIDC (openID Connect), SAML</p> <p>Obsługa wielu połączeń SAML SP</p> <p>Możliwość integracji z istniejącymi usługami uwierzytelniania, w nie mniejszym zakresie niż Active Directory, LDAP, radius.</p> <p>Możliwość obsługi większej liczby kont uprzywilejowanych w miarę rozwoju organizacji</p> <p>Dostęp do zasobów użytkowników uprzywilejowanych musi również obejmować możliwości blokady w oparciu o dodatkowe parametry:</p> <ul style="list-style-type: none"> • Kontrola dostępu oparta na adresie źródłowym IP użytkownika • Ograniczanie dostępu oparte na harmonogramie użytkownika

Redundancja, monitoring i wykrywanie awarii	<p>W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klastery Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.</p> <p>Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.</p> <p>Monitoring stanu realizowanych połączeń VPN.</p> <p>System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.</p>
Interfejsy, Dysk, Zasilanie	<p>System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: 10 portów Gigabit Ethernet RJ-45.</p> <p>System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające instalację oprogramowania z klucza USB.</p> <p>System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.</p> <p>System jest wyposażony w zasilanie AC.</p>
Parametry wydajnościowe	<p>W zakresie Firewall'a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 90 tys. nowych połączeń na sekundę.</p> <p>Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512B.</p> <p>Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3.4 Gbps.</p> <p>Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 7 Gbps.</p> <p>Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 2.3 Gbps.</p> <p>Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1.2 Gbps.</p> <p>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1.2 Gbps.</p>
Funkcje Systemu Bezpieczeństwa	<p>W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:</p> <p>Kontrola dostępu - zaporę ogniową klasy Stateful Inspection.</p> <p>Kontrola Aplikacji.</p> <p>Poufność transmisji danych - połączenia szyfrowane IPSec VPN.</p> <p>Ochrona przed malware.</p> <p>Ochrona przed atakami - Intrusion Prevention System.</p> <p>Kontrola stron WWW.</p> <p>Kontrola zawartości poczty – Antyspam dla protokołów SMTP.</p> <p>Zarządzanie pasmem (QoS, Traffic shaping).</p> <p>Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <p>Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.</p> <p>Możliwość filtrowania zapytań DNS w ruchu przechodzącym przez system.</p> <p>Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wystanie</p>

	powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	<p>Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń; rejestrowanie zdarzeń.</p> <p>System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:</p> <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. <p>W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.</p> <p>Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: adresy URL, adresy IP.</p> <p>Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.</p> <p>Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.</p> <ul style="list-style-type: none"> • System musi umożliwiać integrację z platformami SDN, wirtualizacyjnymi i chmurowymi, takimi jak Cisco ACI, OpenStack, VMware NSX, Kubernetes, AWS, Azure, GCP lub rozwiązaniami równoważnymi, w celu dynamicznego wykorzystania informacji o zasobach przy budowie polityk bezpieczeństwa.
Połączenia VPN	<p>System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Wsparcie dla IKE v1 oraz v2. • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). • Obsługę protokołu Diffie-Hellman grup 19, 20. • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. • Mechanizm „Split tunneling” dla połączeń Client-to-Site. <p>Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN. Oprogramowanie klienckie VPN jest dostępne jako opcja i nie jest wymagane w implementacji.</p>
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ul style="list-style-type: none"> • Routingu statycznego. • Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego). • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. • Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. • ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy

	<p>routingu.</p> <ul style="list-style-type: none"> • BFD (Bidirectional Forwarding Detection). • Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<p>System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łącz WAN.</p> <p>SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).</p>
Zarządzanie pasmem	<p>System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.</p> <p>System daje możliwość określania pasma dla poszczególnych aplikacji.</p> <p>System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.</p> <p>System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.</p>
Ochrona przed malware	<p>Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).</p> <p>Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.</p> <p>W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości lub umożliwia konfigurację maksymalnego czasu, który system bezpieczeństwa może poświęcić na dekompresję archiwum.</p> <p>System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.</p> <p>System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).</p> <p>Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.</p> <p>Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.</p>
Ochrona przed atakami	<p>Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.</p> <p>System chroni przed atakami na aplikacje pracujące na niestandardowych portach.</p> <p>Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.</p> <p>System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.</p> <p>System dysponuje sygnaturami do ochrony przed atakami na systemy przemysłowe SCADA.</p> <p>Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).</p> <p>Wykrywanie i blokowanie komunikacji C&C do sieci botnet.</p> <p>Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.</p>
Kontrola aplikacji	<p>Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.</p>

	<p>Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.</p> <p>System musi umożliwiać kontrolę aplikacji chmurowych, usług społecznościowych, usług współdzielenia dokumentów, usług synchronizacji plików oraz popularnych wyszukiwarek, z możliwością kontroli działań użytkowników, takich jak pobieranie i wysyłanie plików.</p> <p>Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.</p> <p>Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.</p> <p>Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21).</p> <p>System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).</p>
Kontrola WWW	<p>Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.</p> <p>W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.</p> <p>Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.</p> <p>Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.</p> <p>Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).</p> <p>Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.</p> <p>Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.</p> <p>Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.</p> <p>System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.</p>
Uwierzytelnianie użytkowników w ramach sesji	<p>System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:</p> <ul style="list-style-type: none"> • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych. <p>System daje możliwość zastosowania w tym procesie uwierzytelniania wieloskładnikowego.</p> <p>System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.</p> <p>Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.</p>
Zarządzanie	<p>Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.</p> <p>Komunikacja elementów systemu zabezpieczeń z platformami centralnego</p>

	<p>zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.</p> <p>Istnieje możliwość włączenia mechanizmów uwierzytelniania wieloskładnikowego dla dostępu administracyjnego.</p> <p>System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.</p> <p>System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.</p> <p>Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.</p> <p>Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.</p> <p>Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).</p> <p>Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.</p>
Logowanie	<p>W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.</p> <p>Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
Gwarancja	<p>Minimum 12 miesięcy gwarancji producenta.</p> <p>Dostęp do aktualizacji oprogramowania i wsparcie techniczne producenta w trybie 24x7 przez dedykowany moduł internetowy oraz infolinię.</p> <p>Dostęp do aktualnych baz funkcji ochronnych i serwisów producenta w zakresie: kontrola aplikacji, IPS, antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, ochrona systemów przemysłowych SCADA, na okres min. 12 miesięcy.</p>
Prace wdrożeniowe	<p>Instalacja i konfiguracja urządzeń w sieci LAN i WAN Zamawiającego.</p> <p>Przepisanie konfiguracji z obecnie pracujących urządzeń UTM/router celem zachowania ciągłości funkcjonowania systemu IT Zamawiającego.</p>

8. Zasilacz awaryjny UPS - 5 szt.

Parametr	Charakterystyka (wymagania minimalne)
Moc pozorna	min. 3000VA
Moc rzeczywista	min. 3000VA
Technologia	on-line (VFI), podwójna konwersja
Sprawność max (dla VFI)	min. 93%

Typ obudowy	Rack 19" o wysokości max. 2U wraz z kompletem szyn umożliwiającym zamontowanie w szafie Rack / Tower
Ilość wydzielanego ciepła dla nominalnych warunków pracy	< 520 BTU / h
Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
Zabezpieczenie wyjściowe	Praca falownikowa – elektroniczne zwarciove i przeciążeniowe
Zabezpieczenie wejściowe	Przeciwpzepięciowe
Akumulatory wewnętrzne w UPS	minimum 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania dla obciążenia 100%	minimum 3,5 min
Czas ładowania baterii wew. w UPS - po 80% wyładowaniu baterii	≤ 3 h
Przeciążalność	100 ÷ 105 - ostrzeżenie (praca normalna); 105 ÷ 125 - 5 min; 125 ÷ 150 - 30 s; > 150 - 500 ms
Ilość i typ gniazd wyjściowych	Min. 8x IEC 320 C13 (10 A) + 1x IEC 320 C19 (16 A), z czego minimum 4 gniazda sterowalne
Sygnalizacja	Wyświetlacz LCD
Test baterii	Wymagana możliwość uruchomienia testu baterii z poziomu menu zasilacza
Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych	Wymagana możliwość podłączenia do 4 zewnętrznych modułów bateryjnych
Możliwość pracy w trybie konwertera częstotliwości	Wymagane
Złącze EPO	wymagane ustawienie NC
Interfejsy komunikacyjne	RS232, USB 2.0, styki bezpotencjałowe: wejściowe (1), wyjściowe (1), sieciowa karta zarządzająca SNMP/HTTP
Gwarancja	Minimum 24 miesiące gwarancji producenta na elektronikę i akumulatory. Serwis realizowany w systemie door to door.

Część 3

1. Serwer wysokiej dostępności (HA) niezbędny do wdrożenia rozwiązań z zakresu bezpieczeństwa – 1 szt.

Serwer wysokiej dostępności zbudowany z dwóch węzłów (node).

Minimalne parametry węzła (node):

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	<ul style="list-style-type: none">Obudowa Rack 19" o wysokości max 1UMinimum 10 slotów na dyski 2.5"Możliwość instalacji dysków SAS/SATA/NVMeObudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, pozwalający jednoznacznie stwierdzić, czy system działa poprawnie i pokazujący podstawowe stany działania serwera w tym adres IP karty zarządzającejObudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI
Płyta główna	<ul style="list-style-type: none">Płyta główna z możliwością zainstalowania minimum jednego procesoraMożliwość obsługi procesorów 128 rdzeniowychPłyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowymNa płycie głównej powinno znajdować się 12 slotów przeznaczonych do instalacji pamięciPłyta główna powinna obsługiwać do 3TB pamięci RAM
Chipset	<ul style="list-style-type: none">Dedykowany przez producenta procesora do pracy w serwerach jednoprocessorowych
Procesor	<ul style="list-style-type: none">Zainstalowany jeden procesor 16-rdzeniowy, 3.0GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku 177 w teście SPECrate2017_int_base w konfiguracji jednoprocessorowej, dostępnym na stronie www.spec.org dla oferowanego serwera
RAM	<ul style="list-style-type: none">384GB DDR5 RDIMM 5600MT/s
Kontroler RAID	<ul style="list-style-type: none">Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 10
Dyski twarde	<ul style="list-style-type: none">Zainstalowane dwa dyski SSD SATA o pojemności 480GB, Hot-PlugMożliwość zainstalowania dwóch dysków M.2 NVMe SSD o pojemności 960GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCIe	<ul style="list-style-type: none">Trzy sloty PCIe
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none">Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)Dwuportowa karta PCIe 10/25Gb Ethernet w standardzie SFP28
Wbudowane porty	<ul style="list-style-type: none">4 porty USB w tym min:<ul style="list-style-type: none">1 port USB 3.0 z tyłu obudowy,1 port micro USB z przodu obudowy

	<ul style="list-style-type: none"> • 2 port VGA z czego jeden z przodu obudowy • Możliwość rozbudowy o port RS232
Video	<ul style="list-style-type: none"> • Zintegrowana karta graficzna z 16MB pamięci osiągająca rozdzielczość 1920x1200
Zasilacze	<ul style="list-style-type: none"> • Redundantne, Hot-Plug 700W klasy Titanium
Elementy montażowe	<ul style="list-style-type: none"> • Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych • Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych
System operacyjny/dodatkové oprogramowanie	<ul style="list-style-type: none"> • Windows Server 2025 Standard dla procesora określonego powyżej lub równoważny, z prawem do legalnego użytkowania przez Zamawiającego. Licencja musi obejmować wymaganą liczbę rdzeni procesora zgodnie z zasadami licencjonowania producenta.
Bezpieczeństwo	<ul style="list-style-type: none"> • Zatrask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardej. • Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania • 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 V3 • Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera • 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 lub równoważnymi. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzającego spełnienie powyższych zaleceń
Karta Zarządzania	<ul style="list-style-type: none"> • Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiające: <ul style="list-style-type: none"> ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej ○ szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika ○ możliwość podmontowania zdalnych wirtualnych napędów ○ wirtualną konsolę z dostępem do myszy, klawiatury ○ wsparcie dla IPv6 ○ wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni

	<p>wstecz.</p> <ul style="list-style-type: none"> o możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer o integracja z Active Directory o możliwość obsługi przez ośmiu administratorów jednocześnie o Wsparcie dla automatycznej rejestracji DNS o wsparcie dla LLDP o wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej o możliwość podłączenia lokalnego poprzez złącze RS-232. o możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. o Monitorowanie zużycia dysków SSD o możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi o Automatyczne zgłaszanie alertów do centrum serwisowego producenta o Automatyczne update firmware dla wszystkich komponentów serwera o Możliwość przywrócenia poprzednich wersji firmware o Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON o Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych o Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram o Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera o Serwer musi posiadać możliwość uruchomienia funkcjonalności umożliwiającej dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE lub WIFI. <p>Możliwość rozszerzenia funkcjonalności karty o:</p> <ul style="list-style-type: none"> o Rozwiązanie musi umożliwiać przekazywanie danych telemetrycznych do zewnętrznych narzędzi analitycznych i monitorujących, takich jak Splunk, Grafana, Elasticsearch lub rozwiązania równoważne, z wykorzystaniem udokumentowanych mechanizmów integracji. Kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania o Automatyczne odświeżanie certyfikatów SSL o możliwość uwierzytelniania wielokładnikowego z wykorzystaniem tokenów sprzętowych, aplikacji mobilnych lub rozwiązań równoważnych, zgodnych z powszechnie stosowanymi standardami uwierzytelniania o możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień o możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera o możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer o możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe o monitorowanie przepływu powietrza na bieżąco (w CFM)
Oprogramowanie do zarządzania	Możliwość 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 modułarnych 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.

	<ul style="list-style-type: none"> • 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.
Gwarancja	<ul style="list-style-type: none"> • Minimum 36 miesięcy gwarancji producenta • Możliwości zgłaszania zdarzeń serwisowych do serwisu producenta w trybie 24/7/365 telefonicznie i przez Internet • Certyfikowany technik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki • Naprawa ma odbyć się w siedzibie Zamawiającego • W przypadku wystąpienia awarii dysku twardego, uszkodzony dysk twardy pozostaje u Zamawiającego
Prace wdrożeniowe	<p>Instalacja serwerów szafie rack</p> <p>Podłączenie serwerów do zasilania i podsieci wskazanych przez Zamawiającego</p> <p>Instalacja i konfiguracja Windows Server z rolą Hyper-V lub równoważną, zapewniającą utworzenie klastra oraz współpracę z infrastrukturą Zamawiającego.</p> <p>Podłączenie macierzy dyskowej wymienionej w pkt.2 do klastra</p> <p>Integracja z usługą katalogową Microsoft Active Directory wykorzystywaną przez Zamawiającego lub równoważną usługą katalogową zapewniającą centralne zarządzanie użytkownikami, grupami i uprawnieniami.</p>

2. Macierz dyskowa - 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Typ obudowy	Obudowa Rack 19" o wysokości max 2U Minimum 12 slotów na dyski 3.5"
Przestrzeń dyskowa	Zainstalowane: 10x dysk Nearline SAS o pojemności min. 12TB, Hot-Plug 2x dysk SSD SAS Mix Used o pojemności min. 1.6TB, Hot-Plug
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 264 dysków twardych
Obsługa dysków	Macierz musi mieć możliwość obsługi dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5"
Sposób zabezpieczenia danych	<p>Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping).</p> <p>Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID.</p> <p>Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia</p>

	<p>dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku).</p> <p>Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.</p>
Tryb pracy kontrolerów macierzowych	<p>Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.</p>
Pamięć cache	<p>Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM.</p> <p>Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi.</p> <p>Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania baterijnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.</p>
Rozbudowa pamięci cache	<p>Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.</p>
Interfejsy	<p>Macierz musi posiadać, co najmniej 8 portów 25Gb iSCSI (4 porty na kontroler)</p>
Kable/wkładki	<p>4x kabel DAC 25GbE SFP28/SFP28 min. 3m</p>
Zarządzanie	<p>Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.</p>
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	<p>Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej.</p> <p>Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Thin Provisioning	<p>Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning.</p> <p>Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP).</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Tiering	<p>Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS.</p> <p>Tiering musi obejmować wszystkie woluminy w danej puli dyskowej.</p> <p>Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.</p>
Wewnętrzne kopie migawkowe	<p>Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej</p>

	<p>przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii.</p> <p>Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Wewnętrzne kopie pełne	<p>Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.</p> <p>Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.</p>
Migracja danych w obrębie macierzy	<p>Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.</p>
Zdalna replikacja danych	<p>Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy.</p> <p>Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.</p>
Podłączanie zewnętrznych systemów operacyjnych	<p>Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami).</p> <p>Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix.</p> <p>Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.</p>
Redundancja	<p>Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów.</p> <p>Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory.</p> <p>Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.</p> <p>Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla zasilacza minimum 80+ Gold.</p>
Gwarancja	<ul style="list-style-type: none"> • Minimum 36 miesięcy gwarancji producenta • Możliwości zgłaszania zdarzeń serwisowych do serwisu producenta w trybie 24/7/365 telefonicznie i przez Internet • Certyfikowany technik producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć

	<p>naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od zakończenia diagnostyki</p> <ul style="list-style-type: none"> • Naprawa ma odbyć się w siedzibie Zamawiającego • W przypadku wystąpienia awarii dysku twardego, uszkodzony dysk twardy pozostaje u Zamawiającego
Prace wdrożeniowe	<p>Instalacja macierzy szafie rack</p> <p>Podłączenie macierzy do zasilania i podsieci wskazanej przez Zamawiającego</p> <p>Konfiguracja macierzy, w tym: stworzenie RAID, stworzenie LUN'ów</p>

3. Klucze sprzętowe U2F - 200 szt.

Parametr	Charakterystyka (wymagania minimalne)
Interfejsy	<p>Złącze USB typu A (USB-A)</p> <p>Obsługa NFC (Near Field Communication) zgodna z ISO/IEC 14443</p> <p>Brak konieczności stosowania baterii (zasilanie z portu USB lub pola NFC)</p>
Obudowa	<p>Obudowa odporna na uszkodzenia mechaniczne (tworzywo wzmocnione lub kompozyt)</p> <p>Odporność na zachłapanie i pył - minimum IP68</p> <p>Zakres temperatur pracy co najmniej 0°C – 40° lub szerszy</p>
Obsługiwane standardy i protokoły	<p>FIDO2 L2</p> <p>FIDO CTAP2.1</p> <p>FIDO U2F</p> <p>OATH – TOTP</p> <p>Smart Card (PIV)</p> <p>OpenPGP</p> <p>Challenge-Response</p> <p>Obsługa kryptografii asymetrycznej (RSA 2048 bit lub wyższa, ECC P-256/P-384)</p>
Wymagania funkcjonalne	<p>Uwierzytelnianie dwuskładnikowe (2FA) i wieloskładnikowe (MFA).</p> <p>Uwierzytelnianie bezhasłowe (passwordless) w środowiskach zgodnych z FIDO2</p> <p>Integracja systemami operacyjnymi: Windows (min. Windows 10), macOS, Linux.</p> <p>Integracja z przeglądarkami internetowymi: Chrome, Edge, Firefox, Safari.</p> <p>Integracja z usługami chmurowymi (np. Microsoft 365, Google Workspace, systemy IAM wspierające FIDO2).</p> <p>Obsługa logowania przez NFC w urządzeniach mobilnych (Android, iOS – w zakresie wspieranym przez producentów systemów).</p> <p>Pełna zgodność z interfejsem USB HID.</p> <p>Brak konieczności instalowania dedykowanych sterowników w standardowych systemach operacyjnych (plug & play).</p> <p>Możliwość zarządzania i konfiguracji przy użyciu ogólnodostępnych narzędzi administracyjnych.</p>
Gwarancja	<p>Minimum 24 miesiące gwarancji producenta.</p> <p>Urządzenie fabrycznie zapakowane w oryginalne opakowanie producenta.</p> <p>Każde urządzenie musi posiadać unikalny numer seryjny.</p>

4. Wdrożenie oprogramowania z zakresu bezpieczeństwa z wykorzystaniem oprogramowania typu open source i/lub oprogramowania używanego obecnie przez Zamawiającego - 1 szt.

Funkcjonalność	Zakres wdrożenia (wymagania minimalne)
<p>4.1.</p> <p>Wdrożenie rozwiązania open-source do badania i zarządzania podatnościami</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest świadczenie usługi polegającej na wdrożeniu spójnego rozwiązania open-source do badania podatności oraz zarządzania podatnościami, działającego w infrastrukturze Zamawiającego.</p> <p>Rozwiązanie ma zapewniać:</p> <ul style="list-style-type: none"> ▪ identyfikację podatności w systemach i sieci, ▪ centralne zarządzanie podatnościami, ▪ obsługę procesu ich usuwania (remediacji), ▪ możliwość integracji z innymi systemami bezpieczeństwa. <p>2. Zakres usługi</p> <p>2.1 Wdrożenie systemu skanowania podatności</p> <p>W ramach usługi Wykonawca:</p> <ul style="list-style-type: none"> ▪ zainstaluje i skonfiguruje narzędzie do skanowania podatności, skonfiguruje: ▪ skany sieciowe, ▪ skany systemów, ▪ skany usług, ▪ przygotuje polityki skanowania, ▪ skonfiguruje harmonogram skanów, ▪ przeprowadzi pierwsze skany testowe. <p>2.2 Wdrożenie systemu zarządzania podatnościami</p> <p>W ramach usługi Wykonawca:</p> <ul style="list-style-type: none"> ▪ wdroży centralny system zarządzania podatnościami, ▪ zapewni: <ul style="list-style-type: none"> ○ agregację wyników skanów, ○ klasyfikację podatności (np. wg poziomu ryzyka), ○ przypisywanie podatności do zasobów, ○ zarządzanie statusem podatności, <p>2.3 Możliwość integracji z systemami zewnętrznymi</p> <p>Rozwiązanie musi umożliwiać integrację z:</p> <ul style="list-style-type: none"> ▪ systemem monitorowania bezpieczeństwa (SIEM), ▪ systemami zarządzania incydentami, ▪ innymi narzędziami bezpieczeństwa. <p>2.4 Testy i uruchomienie</p> <p>Wykonawca:</p> <ul style="list-style-type: none"> ▪ przeprowadzi testy funkcjonalne, ▪ wykona testowe skany, ▪ zweryfikuje poprawność działania systemu, ▪ uruchomi rozwiązanie produkcyjnie. <p>2.5 Dokumentacja</p> <p>Wykonawca dostarczy:</p> <ul style="list-style-type: none"> ▪ dokumentację techniczną wdrożenia,

- instrukcję obsługi systemu,
- procedurę zarządzania podatnościami,
- opis architektury rozwiązania.

2.6 Szkolenie

- szkolenie administratorów (min. 1 dzień),
- szkolenie użytkowników (min. 4 godziny),
- materiały szkoleniowe.

3. Wymagania funkcjonalne

Rozwiązanie musi:

- umożliwiać automatyczne skanowanie podatności,
- identyfikować podatności w:
- systemach operacyjnych,
- usługach sieciowych,

umożliwiać:

- centralne zarządzanie podatnościami,
- przypisywanie podatności do zasobów,
- generować raporty,
- obsługiwać wielu użytkowników i role.

4. Wymagania niefunkcjonalne

- rozwiązanie musi działać w środowisku Zamawiającego (on-premise).
- rozwiązanie musi być open-source,
- licencja musi dopuszczać wykorzystanie komercyjne.
- uwierzytelnianie użytkowników,
- kontrola dostępu,
- szyfrowanie komunikacji,
- rejestrowanie zdarzeń.
- możliwość rozbudowy systemu,
- możliwość zwiększenia liczby skanowanych zasobów.

5. Wymagania dotyczące rozwiązania

Rozwiązanie musi:

- umożliwiać integrację poprzez:
- API,
- nie może wymagać zakupu licencji dla podstawowej funkcjonalności.

6. Okres realizacji

- Maksymalnie do 30.09.2026

7. Gwarancja i wsparcie

- Minimum 12 miesięcy wsparcia wdrożeniowego.

8. Wymagania w zakresie odbioru

Warunkiem odbioru jest:

- działający system,
- wykonane skany testowe,
- wygenerowany raport podatności,
- przekazana dokumentacja,
- przeprowadzone szkolenie.

9. Informacja o ilości stanowisk:

	<p>a) Serwer: 54</p> <p>b) Host: 180</p> <p>c) Urządzeń sieciowych: 325</p>
<p>4.2.</p> <p>Wdrożenie rozwiązania open-source do badania podatności stron WWW</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest wdrożenie rozwiązania open-source służącego do skanowania i analizy podatności aplikacji oraz stron WWW, obejmujące instalację, konfigurację, uruchomienie oraz przygotowanie do eksploatacji w środowisku Zamawiającego.</p> <p>2. Cel zamówienia</p> <p>Celem zamówienia jest zwiększenie poziomu bezpieczeństwa aplikacji webowych poprzez identyfikację podatności, błędów bezpieczeństwa oraz nieprawidłowych konfiguracji, a także wsparcie procesów zarządzania podatnościami i ryzykiem.</p> <p>3. Zakres zamówienia</p> <p>Zakres zamówienia obejmuje:</p> <ul style="list-style-type: none"> ▪ dostawę i wdrożenie rozwiązania open-source do skanowania podatności WWW, ▪ instalację w infrastrukturze Zamawiającego (środowisko fizyczne lub wirtualne), ▪ konfigurację mechanizmów skanowania (pasywnego i aktywnego), ▪ konfigurację skanowania aplikacji publicznych i wewnętrznych, ▪ konfigurację obsługi uwierzytelniania (sesje, cookies, tokeny), ▪ przygotowanie profili i polityk skanowania, ▪ uruchomienie testów bezpieczeństwa, ▪ przygotowanie mechanizmów raportowania, ▪ przekazanie rozwiązania do eksploatacji. <p>4. Wymagania funkcjonalne</p> <p>Rozwiązanie musi:</p> <ul style="list-style-type: none"> ▪ umożliwiać skanowanie aplikacji WWW (HTTP/HTTPS), ▪ realizować skanowanie pasywne i aktywne, ▪ wykrywać podatności, w szczególności: <ul style="list-style-type: none"> ▪ SQL Injection, ▪ Cross-Site Scripting (XSS), ▪ błędy kontroli dostępu, ▪ błędną konfigurację bezpieczeństwa, ▪ podatności sesji i uwierzytelniania, ▪ analizować parametry wejściowe, nagłówki HTTP oraz cookies, ▪ umożliwiać skanowanie aplikacji wymagających logowania, ▪ umożliwiać definiowanie zakresu skanowania oraz wykluczeń, ▪ umożliwiać generowanie raportów z wyników skanowania, ▪ umożliwiać ręczne wspomaganie testów bezpieczeństwa. <p>5. Wymagania techniczne</p> <p>Rozwiązanie musi:</p> <ul style="list-style-type: none"> ▪ być dostępne jako open-source (z możliwością wykorzystania komercyjnego), ▪ działać w infrastrukturze lokalnej Zamawiającego (on-premise), ▪ być możliwe do uruchomienia w środowisku serwerowym lub wirtualnym,

- umożliwiać aktualizację komponentów i reguł skanowania,
- umożliwiać eksport wyników skanowania (np. PDF, HTML, CSV),
- nie wymagać korzystania z usług chmurowych producenta.

Dopuszcza się zastosowanie rozwiązań open-source, w szczególności narzędzi klasy DAST (Dynamic Application Security Testing), takich jak np.: OWASP ZAP lub innych rozwiązań równoważnych spełniających wymagania określone w OPZ.

Za rozwiązanie równoważne uznaje się rozwiązanie zapewniające co najmniej:

- skanowanie pasywne i aktywne aplikacji WWW,
- identyfikację podatności zgodnych z OWASP Top 10,
- możliwość generowania raportów,
- możliwość konfiguracji zakresu testów,
- możliwość pracy w środowisku lokalnym Zamawiającego.

6. Wymagania bezpieczeństwa

- rozwiązanie nie może powodować niekontrolowanego zakłócenia działania systemów produkcyjnych,
- dostęp do narzędzia musi być ograniczony do uprawnionych użytkowników,
- działania użytkowników muszą być rejestrowane,
- dane z testów muszą być chronione przed nieuprawnionym dostępem,
- rozwiązanie musi umożliwiać bezpieczne przechowywanie wyników analiz.

7. Wdrożenie (instalacja, konfiguracja, uruchomienie)

Wdrożenie obejmuje:

- instalację rozwiązania,
- konfigurację środowiska skanowania,
- konfigurację polityk i profili skanowania,
- uruchomienie testów pilotażowych,
- przekazanie rozwiązania do eksploatacji.

8. Dokumentacja

Wykonawca dostarczy:

- dokumentację instalacyjną,
- dokumentację konfiguracyjną,
- instrukcję użytkownika,
- instrukcję administratora.

9. Szkolenia

- przeprowadzenie szkolenia dla administratorów i użytkowników,
- omówienie obsługi narzędzia,
- omówienie interpretacji wyników skanowania.

10. Warunki odbioru

Odbiór nastąpi po:

- poprawnym wdrożeniu rozwiązania,
- przeprowadzeniu testów skanowania,
- dostarczeniu wymaganej dokumentacji,
- przeprowadzeniu szkolenia,
- potwierdzeniu działania rozwiązania w środowisku Zamawiającego.

11. Gwarancja i wsparcie

- minimum 12 miesięcy wsparcia wdrożeniowego.

	<p>12. Postanowienia końcowe</p> <p>Rozwiązanie musi umożliwiać dalszą rozbudowę oraz integrację z innymi systemami bezpieczeństwa funkcjonującymi u Zamawiającego.</p>
<p>4.3.</p> <p>Wdrożenie rozwiązania typu NAC (Network Access Control)</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest wdrożenie rozwiązania typu NAC (Network Access Control) służącego do kontroli dostępu urządzeń i użytkowników do sieci informatycznej Zamawiającego. Rozwiązanie musi być oparte o oprogramowanie open-source.</p> <p>2. Cel zamówienia</p> <p>Celem zamówienia jest:</p> <ul style="list-style-type: none"> ▪ zwiększenie poziomu bezpieczeństwa sieci, ▪ kontrola dostępu do zasobów sieciowych, ▪ ograniczenie dostępu dla urządzeń nieautoryzowanych, ▪ wprowadzenie podstawowych mechanizmów zarządzania dostępem. <p>3. Zakres zamówienia</p> <p>Zakres obejmuje:</p> <ul style="list-style-type: none"> ▪ instalację i konfigurację systemu NAC, ▪ integrację z infrastrukturą sieciową: <ul style="list-style-type: none"> ○ NAC integruje się z: <ul style="list-style-type: none"> ▪ przełącznikami LAN, ▪ kontrolerami WiFi / AP, ▪ (opcjonalnie) bramami VPN, ○ przy użyciu standardowych protokołów: <ul style="list-style-type: none"> ▪ RADIUS (802.1X, MAB), ▪ SNMP / SSH (do zmian konfiguracji), ▪ VLAN / ACL. ▪ integrację z usługami katalogowymi: <ul style="list-style-type: none"> ○ zakres - pobieranie: istniejących użytkowników, grupy użytkowników, atrybuty (np. dział, rola), ▪ konfigurację podstawowych polityk dostępu, ▪ uruchomienie systemu, ▪ przeprowadzenie testów działania, ▪ przygotowanie dokumentacji, ▪ szkolenie administratora, ▪ wsparcie powdrożeniowe. <p>4. Minimalne wymagania funkcjonalne</p> <p>Rozwiązanie musi zapewniać:</p> <ul style="list-style-type: none"> ▪ kontrolę dostępu do sieci przewodowej lub bezprzewodowej, ▪ uwierzytelnianie użytkowników lub urządzeń (np. 802.1X, MAB lub równoważne), ▪ możliwość definiowania zasad dostępu do sieci, ▪ możliwość przypisywania urządzeń do segmentów sieci (np. VLAN lub równoważne), ▪ możliwość ograniczenia lub blokowania dostępu do sieci, ▪ rejestrowanie zdarzeń związanych z dostępem do sieci. <p>5. Minimalne wymagania techniczne</p>

Rozwiązanie musi:

- umożliwiać wdrożenie w środowisku lokalnym (on-premise),
- współpracować z urządzeniami sieciowymi wykorzystującymi standardowe protokoły,
- umożliwiać integrację z usługami katalogowymi (np. LDAP, Active Directory lub równoważne),
- wykorzystywać mechanizmy uwierzytelniania sieciowego (np. RADIUS lub równoważne),
- umożliwiać dostęp administracyjny do konfiguracji systemu,
- umożliwiać wykonywanie kopii zapasowych konfiguracji.

6. Wymagania bezpieczeństwa

Rozwiązanie powinno zapewniać:

- kontrolę dostępu do systemu administracyjnego,
- rejestrowanie działań administracyjnych,
- zabezpieczenie konfiguracji systemu,
- możliwość przekazywania logów do systemów zewnętrznych (np. syslog),
- podstawową kontrolę dostępu zgodną z dobrymi praktykami bezpieczeństwa.

7. Wymagania dotyczące wdrożenia

Wykonawca zobowiązany jest do:

- przeprowadzenia instalacji i konfiguracji systemu,
- integracji rozwiązania z infrastrukturą Zamawiającego,
- konfiguracji podstawowych polityk dostępu,
- uruchomienia systemu w środowisku produkcyjnym,
- przeprowadzenia testów działania.

8. Dokumentacja

Wykonawca dostarczy:

- dokumentację powdrożeniową,
- instrukcję administracyjną,
- opis konfiguracji systemu,
- opis zastosowanych polityk dostępu.

9. Szkolenia

Wykonawca przeprowadzi szkolenie dla administratora obejmujące:

- obsługę systemu,
- zarządzanie użytkownikami i urządzeniami,
- wstępną konfigurację
- podstawowe czynności administracyjne.

10. Warunki odbioru

Odbiór nastąpi po:

- wdrożeniu i uruchomieniu systemu,
- potwierdzeniu działania wymaganych funkcjonalności,
- przekazaniu dokumentacji lub wskazania zasobów materiałów szkoleniowych
- przeprowadzeniu szkolenia.

11. Gwarancja i wsparcie

- minimum 12 miesięcy wsparcia wdrożeniowego.

	<p>12. Wymagania dotyczące rozwiązania</p> <p>Zamawiający wymaga zastosowania rozwiązania typu NAC opartego o oprogramowanie open-source. Dopuszcza się rozwiązania równoważne, spełniające powyższe wymagania open-source klasy PacketFence lub równoważne.</p> <p>13. Integracja z systemami zewnętrznymi</p> <p>Rozwiązanie powinno umożliwiać współpracę z innymi systemami funkcjonującymi w infrastrukturze Zamawiającego, w szczególności w zakresie bezpieczeństwa informacji.</p> <p>W szczególności rozwiązanie powinno:</p> <ul style="list-style-type: none"> ▪ umożliwiać przekazywanie informacji o zdarzeniach i logów do systemów zewnętrznych (np. poprzez syslog lub równoważne mechanizmy), ▪ umożliwiać integrację z systemami monitorowania bezpieczeństwa (SIEM), ▪ umożliwiać współpracę z systemami uwierzytelniania i katalogowymi (np. LDAP, Active Directory lub równoważne), ▪ wykorzystywać standardowe protokoły komunikacyjne i mechanizmy integracyjne, ▪ umożliwiać dalszą rozbudowę i integrację z innymi rozwiązaniami bezpieczeństwa (np. systemy monitorowania sieci, systemy wykrywania zagrożeń lub równoważne). <p>Zamawiający dopuszcza integrację z rozwiązaniami klasy SIEM open-source (np. Wazuh lub równoważne).</p> <p>14. Postanowienia końcowe</p> <p>Rozwiązanie powinno być dostosowane do środowiska Zamawiającego oraz spełniać wymagania określone w niniejszym OPZ.</p>
<p>4.4. Wdrożenie systemu NDR</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest wdrożenie, konfiguracja oraz uruchomienie systemu typu NDR (Network Detection and Response) do monitorowania i analizy ruchu sieciowego w środowisku IT oraz OT/ICS, wraz z integracją z istniejącą infrastrukturą teleinformatyczną.</p> <p>2. Cel zamówienia</p> <p>Celem zamówienia jest:</p> <ul style="list-style-type: none"> ▪ zwiększenie poziomu bezpieczeństwa sieci, ▪ zapewnienie ciągłego monitorowania ruchu, ▪ wykrywanie anomalii i zagrożeń, ▪ zapewnienie niezależności monitoringu od urządzeń UTM, ▪ wsparcie reagowania na incydenty. <p>3. Zakres zamówienia</p> <p>Zakres obejmuje:</p> <ul style="list-style-type: none"> ▪ analizę środowiska Zamawiającego, ▪ opracowanie koncepcji wdrożenia, ▪ wdrożenie i konfigurację rozwiązania, ▪ konfigurację punktów monitorowania (SPAN/mirror/TAP), ▪ integrację z istniejącą infrastrukturą (w tym UTM, SIEM): <ul style="list-style-type: none"> ○ wymiana informacji o zdarzeniach, ○ korelacja: <ul style="list-style-type: none"> ▪ zdarzeń obserwowanych przez NDR, ▪ zdarzeń logowanych przez UTM. ○ integracja z SIEM

○ NDR:

- generuje zdarzenia bezpieczeństwa,
- przekazuje je do SIEM,
- umożliwia ich:
 - korelację,
 - archiwizację,
 - analizę kontekstową.

- uruchomienie i testy,
- przygotowanie dokumentacji,
- przeprowadzenie szkolenia,
- zapewnienie wsparcia powdrożeniowego.

4. Wymagania funkcjonalne

System musi zapewniać:

- analizę ruchu sieciowego w czasie rzeczywistym,
- wykrywanie anomalii i incydentów bezpieczeństwa,
- identyfikację nieautoryzowanych działań w sieci,
- korelację zdarzeń z różnych źródeł,
- wizualizację i analizę danych,
- generowanie alertów,
- możliwość integracji z systemami zewnętrznymi,
- monitoring środowisk IT oraz OT/ICS,
- działanie pasywne (bez ingerencji w ruch sieciowy),
- analizę ruchu wewnętrznego (east-west), w tym identyfikację komunikacji pomiędzy segmentami i strefami bezpieczeństwa.

5. Wymagania techniczne

System musi:

- wykorzystywać mechanizmy SPAN/mirror/TAP,
- działać w architekturze rozproszonej (sensory + system centralny),
- działać niezależnie od urządzeń UTM,
- umożliwiać analizę ruchu wewnętrznego (LAN) oraz OT/ICS,
- wspierać standardowe protokoły sieciowe oraz protokoły przemysłowe,
- zapewniać skalowalność rozwiązania,
- umożliwiać integrację poprzez API, syslog lub równoważne mechanizmy,
- umożliwiać przechowywanie i analizę danych historycznych przez okres nie krótszy niż 90 dni lub zgodnie z polityką bezpieczeństwa Zamawiającego,
- umożliwiać przekazywanie zdarzeń do systemów klasy SIEM oraz współpracę z rozwiązaniami typu XDR/SOAR.

6. Wymagania bezpieczeństwa

System musi:

- zapewniać kontrolę dostępu do systemu,
- rejestrować zdarzenia i operacje użytkowników,
- wspierać analizę i obsługę incydentów,
- nie powodować zakłóceń w środowisku OT/ICS,
- umożliwiać analizę ruchu między segmentami sieci.

7. Wdrożenie (instalacja, konfiguracja, uruchomienie)

	<p>Wykonawca:</p> <ul style="list-style-type: none"> ▪ zainstaluje i skonfiguruje system, ▪ wdroży sensory ruchu sieciowego, ▪ zaprojektuje i wdroży rozmieszczenie sensorów w sposób zapewniający rzeczywistą widoczność ruchu sieciowego, w szczególności w punktach styku sieci IT, OT oraz segmentów wewnętrznych, ▪ zintegruje rozwiązanie z infrastrukturą Zamawiającego, ▪ przeprowadzi testy poprawności działania, ▪ uruchomi środowisko produkcyjne. <p>8. Dokumentacja</p> <p>Wykonawca dostarczy:</p> <ul style="list-style-type: none"> ▪ dokumentację techniczną, ▪ dokumentację powdrożeniową, ▪ opis architektury rozwiązania, ▪ instrukcję użytkowania i administracji, ▪ dokumentację konfiguracji systemu umożliwiającą jego samodzielne utrzymanie i rozwój. <p>9. Szkolenia</p> <p>Wykonawca przeprowadzi szkolenie dla administratorów obejmujące:</p> <ul style="list-style-type: none"> ▪ obsługę systemu, ▪ analizę zdarzeń, ▪ reagowanie na incydenty, ▪ podstawową konfigurację. <p>10. Warunki odbioru</p> <p>Odbiór nastąpi po:</p> <ul style="list-style-type: none"> ▪ poprawnym wdrożeniu systemu, ▪ przeprowadzeniu testów, ▪ dostarczeniu kompletnej dokumentacji, ▪ przekazaniu pełnych uprawnień administracyjnych do systemu, ▪ przeprowadzeniu szkolenia. <p>11. Okres realizacji</p> <ul style="list-style-type: none"> ▪ Maksymalnie do 30.09.2026 <p>12. Gwarancja i wsparcie</p> <ul style="list-style-type: none"> ▪ Minimum 12 miesięcy wsparcia wdrożeniowego. <p>13. Postanowienia końcowe</p> <p>Zamawiający wymaga, aby w ramach realizacji zamówienia zostało wdrożone rozwiązanie oparte o technologie open-source lub równoważne, które po zakończeniu wdrożenia umożliwia korzystanie z jego funkcjonalności bez konieczności ponoszenia obowiązkowych opłat licencyjnych.</p> <p>Niedopuszczalne jest uzależnienie działania wdrożonego rozwiązania od płatnych modułów, subskrypcji lub usług producenta w zakresie funkcjonalności wymaganych w niniejszym OPZ.</p> <p>Dopuszcza się rozwiązania open – source oparte m.in. o: Zeek lub równoważne.</p>
<p>4.5.</p> <p>Wdrożenie, konfigurację i integrację systemu</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest usługa polegająca na wdrożeniu, konfiguracji oraz integracji systemu uwierzytelniania i autoryzacji opartego o rozwiązanie typu RADIUS w technologii open-source, przeznaczonego do obsługi dostępu</p>

<p>open-source typu RADIUS</p>	<p>do zasobów sieciowych w środowisku IT oraz OT/ICS/IIoT.</p> <p>2. Cel zamówienia</p> <p>Celem zamówienia jest:</p> <ul style="list-style-type: none"> ▪ centralizacja procesu uwierzytelniania użytkowników i urządzeń, ▪ zwiększenie kontroli dostępu do sieci (LAN/WLAN/VPN), ▪ zapewnienie spójnego mechanizmu autoryzacji w środowiskach IT i OT, ▪ integracja z istniejącą infrastrukturą bezpieczeństwa (np. NAC, SIEM, UTM), ▪ spełnienie wymagań w zakresie cyberbezpieczeństwa (ISO, KSC, NIS2). <p>3. Zakres zamówienia</p> <p>Usługa obejmuje:</p> <ul style="list-style-type: none"> ▪ instalację i konfigurację systemu RADIUS (np. FreeRADIUS lub równoważnego), ▪ wdrożenie mechanizmów uwierzytelniania: ▪ 802.1X, ▪ MAC Authentication Bypass (MAB), ▪ uwierzytelnianie użytkowników (np. LDAP/AD), <p>integrację z:</p> <ul style="list-style-type: none"> ▪ usługą katalogową (Active Directory / LDAP) Zakres - pobieranie: istniejących użytkowników, grupy użytkowników, atrybuty (np. dział, rola), ▪ urządzeniami sieciowymi (switch, WiFi, VPN, firewall): <ul style="list-style-type: none"> ○ Integracja z przełącznikami (LAN – przewodowa) <ul style="list-style-type: none"> ▪ przełącznik nie uwierzytelnia lokalnie użytkownika/urządzenia. ▪ po podłączeniu do portu: ▪ wyzwalany jest 802.1X (dla użytkowników) lub MAB (dla urządzeń), ▪ przełącznik wysyła zapytanie RADIUS do serwera RADIUS. ○ Rola RADIUS <ul style="list-style-type: none"> ▪ RADIUS: ▪ weryfikuje tożsamość (np. AD/LDAP, baza MAC), ▪ podejmuje decyzję (ACCEPT/REJECT), ▪ zwraca atrybuty autoryzacyjne, np.: <ul style="list-style-type: none"> ▪ VLAN, ▪ rola, ▪ ACL ▪ konfigurację polityk dostępu (role, VLAN, segmentacja), ▪ integrację z systemami bezpieczeństwa: <ul style="list-style-type: none"> ○ RADIUS jest używany przez NAC jako:: <ul style="list-style-type: none"> ▪ silnik AAA (uwierzytelnianie i autoryzacja), ▪ źródło decyzji dostępowych. ○ NAC wykorzystuje wynik RADIUS do: <ul style="list-style-type: none"> ▪ przypisania VLAN, ▪ izolacji, ▪ block/quarantine. ▪ wdrożenie w środowisku IT oraz – w razie potrzeby – OT/ICS, ▪ testy działania i optymalizację.
--------------------------------	---

NT 1 M Nowy

4. Wymagania funkcjonalne
- System musi zapewniać co najmniej:
 - centralne uwierzytelnianie użytkowników i urządzeń,
 - obsługę standardu RADIUS (RFC 2865 i pokrewne),
 - wsparcie dla:
 - 802.1X,
 - EAP (np. PEAP, TLS),
 - integrację z katalogiem użytkowników (LDAP/AD),
 - możliwość definiowania polityk dostępu (np. VLAN, ACL),
 - logowanie zdarzeń uwierzytelniania,
 - możliwość integracji z systemami NAC,
 - możliwość eksportu logów do systemów SIEM (np. Wazuh lub równoważne),
 - obsługę wielu punktów dostępu (switch, AP, VPN).
5. Wymagania techniczne
- Rozwiązanie musi:
- być oparte o technologię open-source (np. FreeRADIUS lub równoważne),
 - działać w środowisku Linux (preferowane),
 - umożliwiać wysoką dostępność (np. konfiguracja HA lub redundancja),
 - wspierać szyfrowanie komunikacji (TLS),
 - umożliwiać skalowanie (wzrost liczby użytkowników/urządzeń),
 - działać zarówno w środowisku IT jak i OT (z uwzględnieniem ograniczeń OT),
6. Wymagania bezpieczeństwa
- System musi zapewniać:
- bezpieczne uwierzytelnianie (np. EAP-TLS),
 - szyfrowanie komunikacji (TLS),
 - kontrolę dostępu opartą o polityki,
 - rejestrowanie zdarzeń (logi audytowe),
 - możliwość integracji z SIEM,
 - odporność na podstawowe ataki (np. brute force, replay),
 - separację dostępu dla środowisk IT i OT,
 - możliwość wymuszenia MFA (jeśli zintegrowany z AD/IdP).
7. Wdrożenie (instalacja, konfiguracja, uruchomienie)
- Wykonawca zobowiązany jest do:
- instalacji systemu RADIUS,
 - konfiguracji uwierzytelniania i autoryzacji,
 - integracji z infrastrukturą sieciową,
 - konfiguracji polityk dostępu,
 - przeprowadzenia testów funkcjonalnych i bezpieczeństwa,
 - konfigurację środowiska zapasowego, w celu zapewnienia ciągłości działania,
 - uruchomienia systemu produkcyjnego.
8. Dokumentacja
- Wykonawca dostarczy:

	<ul style="list-style-type: none"> ▪ dokumentację architektury rozwiązania, ▪ konfigurację systemu (opis), ▪ procedury awaryjne (np. fallback przy niedostępności RADIUS), ▪ opis integracji z systemami zewnętrznymi. <p>9. Szkolenia</p> <p>W ramach zamówienia należy przeprowadzić:</p> <ul style="list-style-type: none"> ▪ szkolenie administratorów (min. 1 dzień), ▪ szkolenie z analizy logów i incydentów. <p>10. Warunki odbioru</p> <p>Odbiór nastąpi po:</p> <ul style="list-style-type: none"> ▪ wdrożeniu systemu, ▪ przeprowadzeniu testów, ▪ potwierdzeniu działania uwierzytelniania, ▪ dostarczeniu dokumentacji, ▪ przeprowadzeniu szkoleń. <p>11. Okres realizacji</p> <ul style="list-style-type: none"> ▪ Maksymalnie do 30.09.2026 <p>12. Gwarancja i wsparcie</p> <ul style="list-style-type: none"> ▪ Minimum 12 miesięcy wsparcia wdrożeniowego. <p>14. Postanowienia końcowe</p> <p>Zamawiający wymaga, aby w ramach realizacji zamówienia zostało wdrożone rozwiązanie oparte o technologie open-source lub równoważne, które po zakończeniu wdrożenia umożliwia korzystanie z jego funkcjonalności bez konieczności ponoszenia obowiązkowych opłat licencyjnych. Niedopuszczalne jest uzależnienie działania wdrożonego rozwiązania od płatnych modułów, subskrypcji lub usług producenta w zakresie funkcjonalności wymaganych w niniejszym OPZ.</p>
<p>4.6.</p> <p>Wdrożenie i integracja systemu monitorowania infrastruktury IT i OT/ICS/IIoT</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest wdrożenie, konfiguracja, integracja oraz uruchomienie systemu monitorowania infrastruktury informatycznej i technicznej Zamawiającego, obejmującej środowiska IT oraz – w zakresie uzasadnionym technicznie – OT/ICS/IIoT.</p> <p>Zamówienie obejmuje usługę wdrożeniową systemu opartego o rozwiązanie typu open-source lub równoważne, umożliwiające monitorowanie dostępności, wydajności oraz stanu infrastruktury, wraz z konfiguracją alertów, wizualizacji, raportowania oraz integracji z istniejącymi systemami Zamawiającego.</p> <p>2. Cel zamówienia</p> <p>Celem zamówienia jest:</p> <ul style="list-style-type: none"> ▪ zapewnienie centralnego systemu monitorowania infrastruktury, ▪ zwiększenie dostępności i ciągłości działania systemów, ▪ szybkie wykrywanie awarii i anomalii, ▪ wsparcie reagowania na incydenty techniczne i bezpieczeństwa, ▪ poprawa widoczności środowisk IT oraz OT/ICS, ▪ wsparcie procesów utrzymania, audytu i zarządzania. <p>3. Zakres zamówienia</p> <p>Zakres obejmuje:</p> <ul style="list-style-type: none"> ▪ analizę przedwdrożeniową, ▪ opracowanie koncepcji wdrożenia,

- instalację i konfigurację systemu,
- konfigurację monitoringu infrastruktury:
- serwerów,
- stacji roboczych,
- urządzeń sieciowych,
- usług i aplikacji,
- wybranych elementów OT/ICS/IIoT,
- konfigurację alertów i progów,
- przygotowanie dashboardów i raportów,
- integrację z systemami Zamawiającego - minimalny zakres:
 - integracja z pocztą wysyłanie powiadomień pocztą e-mail lub wysyłanie SMS
 - integracja z SIEM:
 - wysyła alerty i zdarzenia do SIEM,
 - przekazuje metadane:
 - host,
 - czas,
 - typ zdarzenia,
 - poziom krytyczności.
- SIEM:
 - koreluje zdarzenia z innymi źródłami (NDR, firewall, AD),
 - wspiera analizę bezpieczeństwa i audyt.
- testy i uruchomienie produkcyjne,
- dokumentację powdrożeniową,
- szkolenia.

4. Wymagania funkcjonalne

System musi zapewniać co najmniej:

- centralne zarządzanie monitoringiem z jednego interfejsu,
- monitorowanie dostępności hostów, urządzeń i usług,
- monitorowanie parametrów wydajnościowych (CPU, RAM, dyski, sieć),
- monitorowanie usług sieciowych i aplikacyjnych,
- obsługę monitoringu:
 - agentowego,
 - bezagentowego,
- obsługę standardowych protokołów, co najmniej:
 - SNMP,
 - ICMP,
 - zbieranie logów (np. syslog lub równoważne),
- możliwość monitorowania systemów Windows i Linux,
- możliwość monitorowania środowisk wirtualnych,
- możliwość monitorowania infrastruktury OT/ICS w sposób bezpieczny i nieinwazyjny,
- generowanie alertów i powiadomień,
- tworzenie dashboardów, map i wizualizacji,
- przechowywanie historii i trendów,

- raportowanie,
- zarządzanie użytkownikami i uprawnieniami,
- możliwość eksportu danych,
- możliwość rozbudowy systemu,
- możliwość integracji z systemami zewnętrznymi (np. SIEM, syslog, helpdesk, API).

5. Wymagania techniczne

Rozwiązanie musi:

- być oparte o technologię open-source lub równoważną,
- nie wymagać obowiązkowych opłat licencyjnych za podstawowe funkcjonalności,
- umożliwiać instalację w infrastrukturze Zamawiającego (on-premise),
- zapewniać architekturę centralną z możliwością rozproszenia (np. proxy lub równoważne),
- umożliwiać skalowanie,
- wykorzystywać bazę danych typu open-source lub równoważną,
- posiadać interfejs webowy,
- wspierać integrację przez API lub mechanizmy równoważne,
- umożliwiać backup i odtwarzanie konfiguracji,
- zapewniać odpowiednią wydajność dla środowiska Zamawiającego.

6. Wymagania bezpieczeństwa

Rozwiązanie musi:

- zapewniać uwierzytelnianie użytkowników,
- umożliwiać zarządzanie rolami i uprawnieniami,
- wspierać szyfrowanie komunikacji,
- rejestrować zdarzenia i operacje użytkowników,
- umożliwiać integrację z systemami bezpieczeństwa (np. SIEM),
- nie wprowadzać podatności do środowiska Zamawiającego,
- wspierać bezpieczne monitorowanie środowisk OT/ICS (bez ingerencji w procesy technologiczne).

7. Wdrożenie (instalacja, konfiguracja, uruchomienie)

Wykonawca zobowiązany jest do:

- instalacji systemu,
- konfiguracji komponentów,
- wdrożenia monitoringu dla wskazanych elementów infrastruktury,
- konfiguracji alertów i powiadomień,
- przygotowania dashboardów,
- integracji z co najmniej jednym systemem Zamawiającego,
- przeprowadzenia testów,
- uruchomienia produkcyjnego,
- optymalizacji działania systemu.

8. Dokumentacja

Wykonawca dostarczy dokumentację obejmującą:

- architekturę rozwiązania,
- konfigurację systemu,
- opis monitorowanych elementów,

	<ul style="list-style-type: none"> ▪ opis integracji. <p>9. Szkolenia</p> <p>Wykonawca przeprowadzi szkolenie obejmujące:</p> <ul style="list-style-type: none"> ▪ obsługę systemu, ▪ konfigurację monitoringu, ▪ analizę alertów, ▪ podstawy utrzymania systemu. <p>11. Warunki odbioru</p> <p>Odbiór nastąpi po:</p> <ul style="list-style-type: none"> ▪ wdrożeniu systemu, ▪ konfiguracji monitoringu, ▪ poprawnym działaniu alertów, ▪ dostarczeniu dokumentacji, ▪ przeprowadzeniu szkolenia. <p>10. Gwarancja i wsparcie</p> <p>Wykonawca zapewni:</p> <ul style="list-style-type: none"> ▪ wsparcie techniczne po wdrożeniu, ▪ usuwanie błędów, ▪ pomoc w konfiguracji, ▪ okres wsparcia zgodny z umową. <p>11. Okres realizacji</p> <ul style="list-style-type: none"> ▪ Maksymalnie do 30.09.2026 <p>12. Gwarancja i wsparcie</p> <ul style="list-style-type: none"> ▪ Minimum 12 miesięcy wsparcia wdrożeniowego. <p>13. Postanowienia końcowe</p> <p>Zamawiający dopuszcza rozwiązania równoważne spełniające wszystkie wymagania funkcjonalne i techniczne.</p> <p>W przypadku zastosowania rozwiązania równoważnego Wykonawca zobowiązany jest wykazać jego równoważność.</p> <p>Wszystkie prace muszą być wykonane zgodnie z dobrymi praktykami oraz wymaganiami bezpieczeństwa informacji.</p>
<p>4.7.</p> <p>Wdrożenie i integracja systemu ITSM dla środowisk IT i OT/ICS/IIoT</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest wdrożenie, konfiguracja, integracja oraz uruchomienie systemu klasy ITSM (IT Service Management), opartego o rozwiązanie open-source lub równoważne, umożliwiającego obsługę zgłoszeń, incydentów, problemów oraz zmian, wraz z funkcjonalnością zarządzania zasobami (CMDB), w środowiskach IT oraz – w zakresie uzasadnionym technicznie – OT/ICS/IIoT.</p> <p>2. Cel zamówienia</p> <p>Celem zamówienia jest:</p> <ul style="list-style-type: none"> ▪ wdrożenie systemu obsługi zgłoszeń i incydentów, ▪ uporządkowanie procesów ITSM, ▪ wdrożenie ewidencji zasobów IT (CMDB), ▪ poprawa efektywności obsługi zgłoszeń. <p>3. Zakres zamówienia</p> <p>Zakres zamówienia obejmuje:</p> <ul style="list-style-type: none"> ▪ instalację i konfigurację systemu ITSM, ▪ wdrożenie obsługi zgłoszeń oraz incydentów wraz z CMDB,

- konfigurację użytkowników, ról i powiadomień,
- uruchomienie produkcyjne, dokumentację i szkolenie.

4. Wymagania funkcjonalne

System musi zapewniać co najmniej:

- obsługę zgłoszeń (Service Desk),
- obsługę incydentów, zmian i problemów,
- portal użytkownika (self-service),
- obsługę zgłoszeń przez e-mail,
- historię i rejestr działań,
- ewidencję zasobów (CMDB) wraz z relacjami,
- możliwość definiowania SLA i automatyzacji,
- raportowanie i dashboardy,
- integrację z systemami zewnętrznymi (monitoring, SIEM, poczta, LDAP/AD, API).

5. Wymagania techniczne

Rozwiązanie musi:

- być open-source
- nie wymagać obowiązkowych opłat licencyjnych za podstawowe funkcjonalności,
- umożliwiać instalację on-premise,
- posiadać interfejs webowy,
- wspierać bazę danych open-source lub równoważną,
- umożliwiać skalowanie,
- wspierać integrację przez API,
- umożliwiać backup i odtwarzanie danych.

6. Wymagania bezpieczeństwa

System musi:

- zapewniać uwierzytelnianie użytkowników,
- wspierać integrację z LDAP/AD,
- umożliwiać zarządzanie rolami i uprawnieniami,
- rejestrować działania użytkowników,
- wspierać szyfrowanie komunikacji,
- umożliwiać integrację z systemami bezpieczeństwa,
- nie wpływać negatywnie na środowiska OT/ICS.

7. Wdrożenie (instalacja, konfiguracja, uruchomienie)

Wykonawca zobowiązany jest do:

- instalacji i konfiguracji systemu w środowisku Zamawiającego,
- konfiguracji funkcjonalności zgodnie z OPZ,
- przeprowadzenia testów poprawności działania,
- uruchomienia systemu w środowisku produkcyjnym.

8. Dokumentacja

Wykonawca dostarczy dokumentację obejmującą:

- opis architektury i konfiguracji systemu,

9. Szkolenia

Wykonawca przeprowadzi szkolenie obejmujące:

	<ul style="list-style-type: none"> ▪ obsługę systemu, ▪ zarządzanie zgłoszeniami i incydentami, ▪ podstawową administrację systemem. <p>10. Warunki odbioru</p> <p>Odbiór nastąpi po spełnieniu następujących warunków:</p> <ul style="list-style-type: none"> ▪ system został uruchomiony w środowisku produkcyjnym, ▪ funkcjonalności określone w OPZ działają poprawnie, ▪ integracje zostały wykonane, ▪ dokumentacja została przekazana, ▪ szkolenie zostało przeprowadzone. <p>11. Okres realizacji</p> <ul style="list-style-type: none"> ▪ Maksymalnie do 30.09.2026 <p>12. Gwarancja i wsparcie</p> <ul style="list-style-type: none"> ▪ Minimum 12 miesięcy wsparcia wdrożeniowego. <p>13. Postanowienia końcowe</p> <p>Zamawiający dopuszcza rozwiązania równoważne spełniające wymagania określone w OPZ. Jako rozwiązanie referencyjne Zamawiający wskazuje system GLPI.</p> <p>Za rozwiązanie równoważne uznaje się rozwiązanie, które łącznie:</p> <ul style="list-style-type: none"> ▪ zapewnia pełną funkcjonalność systemu ITSM (zgłoszenia, incydenty, problemy, zmiany), ▪ posiada wbudowaną funkcjonalność CMDB wraz z relacjami, ▪ umożliwia integrację z systemami monitoringu i bezpieczeństwa (np. SIEM), ▪ umożliwia integrację z pocztą, LDAP/AD oraz posiada API, ▪ działa jako open-source lub bez obowiązkowych opłat licencyjnych, ▪ umożliwia instalację on-premise, ▪ spełnia wymagania techniczne i bezpieczeństwa OPZ. <p>Wykonawca oferujący rozwiązanie równoważne zobowiązany jest do wykazania jego zgodności z wymaganiami OPZ.</p>
<p>4.8.</p> <p>Wdrożenie systemu SIEM (open-source)</p>	<p>1. Przedmiot zamówienia</p> <p>Przedmiotem zamówienia jest usługa obejmująca wdrożenie, konfigurację oraz integrację funkcjonalności klasy SIEM w środowisku Zamawiającego, umożliwiających centralne zbieranie, normalizację, korelację oraz analizę zdarzeń bezpieczeństwa. Rozwiązanie powinno być oparte o technologie open-source (np. Wazuh lub rozwiązanie równoważne).</p> <p>Zakres obejmuje środowiska:</p> <ul style="list-style-type: none"> ▪ IT (serwery, systemy operacyjne, aplikacje, urządzenia sieciowe), ▪ OT/ICS/IIoT (w zakresie dostępnych źródeł danych i integracji). <p>2. Cel zamówienia</p> <p>Celem zamówienia jest wdrożenie funkcjonalności umożliwiających:</p> <ul style="list-style-type: none"> ▪ centralne monitorowanie zdarzeń bezpieczeństwa, ▪ wykrywanie incydentów i anomalii, ▪ korelację zdarzeń z wielu źródeł, ▪ wsparcie reagowania na incydenty, ▪ zwiększenie widoczności środowiska IT oraz OT. <p>3. Zakres zamówienia</p>

Zakres obejmuje w szczególności:

- instalację i konfigurację rozwiązania,
- wdrożenie komponentów odpowiedzialnych za:
- zbieranie danych,
- analizę i korelację,
- wizualizację,
- konfigurację mechanizmów zbierania logów (agentowych lub bezagentowych),
- integrację z systemami IT (Windows, Linux, urządzenia sieciowe) - Musi być instalacja agent pasywny lub aktywny, konfiguracja SNMP)
- integrację z systemami OT/ICS (**jeżeli dostępne źródła danych**),
- konfigurację reguł detekcji i korelacji,
- konfigurację dashboardów i raportów,
- konfigurację mechanizmów alertowania,
- przeprowadzenie testów i uruchomienie produkcyjne.

4. Wymagania funkcjonalne

Rozwiązanie musi zapewniać co najmniej:

- centralne zbieranie zdarzeń i logów (np. syslog, API, agenty),
- korelację zdarzeń w czasie zbliżonym do rzeczywistego,
- wykrywanie incydentów bezpieczeństwa,
- generowanie alertów,
- wizualizację danych (dashboardsy),
- możliwość definiowania własnych reguł,
- archiwizację i przeszukiwanie danych,
- integrację z innymi systemami bezpieczeństwa (np. systemy sieciowe, NAC, EDR),
- możliwość monitorowania środowisk IT oraz – w zakresie dostępnych danych – OT/ICS,
- skalowalność rozwiązania.

5. Wymagania techniczne

Rozwiązanie musi:

- być oparte o technologie open-source lub równoważne,
- nie wymagać obowiązkowych opłat licencyjnych za podstawowe funkcjonalności,
- umożliwiać wdrożenie w środowisku lokalnym Zamawiającego (on-premise),
- wspierać systemy Windows i Linux,
- umożliwiać integrację z urządzeniami sieciowymi (np. syslog),
- wspierać standardowe protokoły komunikacyjne (np. syslog, API),
- umożliwiać skalowanie rozwiązania,
- umożliwiać integrację z systemami zewnętrznymi (np. systemy zarządzania incydentami, systemy ticketowe).

6. Wymagania bezpieczeństwa

Rozwiązanie musi zapewniać:

- uwierzytelnianie użytkowników,
- zarządzanie rolami i uprawnieniami,

- szyfrowanie komunikacji,
 - rejestrowanie działań użytkowników,
 - zapewnienie integralności danych,
 - możliwość integracji z usługami katalogowymi (np. LDAP, Active Directory).
- 7. Wdrożenie (instalacja, konfiguracja, uruchomienie)**
- Wykonawca zobowiązany jest do:
- instalacji i konfiguracji rozwiązania,
 - integracji ze wskazanymi systemami,
 - konfiguracji reguł detekcji,
 - przeprowadzenia testów,
 - uruchomienia systemu w środowisku produkcyjnym.
- 8. Dokumentacja**
- Wykonawca dostarczy:
- dokumentację techniczną,
 - dokumentację konfiguracji,
 - instrukcję administracyjną,
 - instrukcję użytkownika,
 - opis integracji.
- 9. Szkolenia**
- Wykonawca przeprowadzi szkolenie obejmujące:
- obsługę systemu,
 - analizę zdarzeń,
 - administrację i konfigurację.
- 10. Warunki odbioru**
- Odbiór nastąpi po:
- uruchomieniu rozwiązania,
 - potwierdzeniu działania integracji,
 - przetestowaniu funkcjonalności,
 - przekazaniu dokumentacji,
 - przeprowadzeniu szkolenia.
- 11. Okres realizacji**
- Maksymalnie do 30.09.2026
- 12. Gwarancja i wsparcie**
- Minimum 12 miesięcy wsparcia wdrożeniowego.
- 13. Postanowienia końcowe**
- Wszystkie wymagania określone w niniejszym OPZ należy traktować jako minimalne. Zamawiający dopuszcza zastosowanie rozwiązania open-source (np. Wazuh) lub rozwiązania równoważnego.
- Za rozwiązanie równoważne uznaje się rozwiązanie, które spełnia łącznie następujące warunki:
- umożliwia wdrożenie funkcjonalności klasy SIEM/XDR,
 - zapewnia centralne zbieranie, korelację i analizę zdarzeń bezpieczeństwa,
 - umożliwia integrację z systemami IT oraz – w zakresie dostępnych danych – OT/ICS,
 - zapewnia mechanizmy wykrywania incydentów i alertowania,
 - umożliwia tworzenie reguł, raportów i dashboardów,

	<ul style="list-style-type: none"> ▪ umożliwiał wdrożenie w środowisku lokalnym Zamawiającego, ▪ jest rozwiązaniem open-source, ▪ nie wymaga obowiązkowych opłat licencyjnych za podstawowe funkcjonalności.
4.9. Wdrożenie systemu SOAR	<ol style="list-style-type: none"> 1. Przedmiot zamówienia Przedmiotem zamówienia jest usługa wdrożenia, konfiguracji i integracji systemu open-source klasy SOAR (Security Orchestration, Automation and Response), przeznaczonego do automatyzacji reakcji na incydenty bezpieczeństwa oraz orkiestracji działań pomiędzy systemami bezpieczeństwa. System będzie współpracował z istniejącym u Zamawiającego systemem klasy SIEM oraz innymi systemami funkcjonującymi w środowisku IT oraz – w zakresie wymaganym – OT/ICS/IIoT. 2. Cel zamówienia Celem zamówienia jest: <ul style="list-style-type: none"> ▪ wdrożenie centralnego systemu zarządzania incydentami bezpieczeństwa, ▪ automatyzacja reakcji na incydenty, ▪ skrócenie czasu reakcji na zdarzenia, ▪ zapewnienie spójnej orkiestracji działań pomiędzy systemami bezpieczeństwa, ▪ zwiększenie poziomu bezpieczeństwa organizacji. 3. Zakres zamówienia Zakres obejmuje: <ul style="list-style-type: none"> ▪ instalację i konfigurację systemu SOAR, ▪ integrację z istniejącym systemem SIEM, ▪ integrację z systemami Zamawiającego, w szczególności: <ul style="list-style-type: none"> ○ NAC <ul style="list-style-type: none"> ▪ Integracja poprzez izolację urządzenia (quarantine), ▪ zmienić VLAN / rolę / politykę dostępu, ▪ przywrócić dostęp po zakończeniu incydentu, ▪ pobierać kontekst: <ul style="list-style-type: none"> ▪ użytkownik, ▪ lokalizacja, ▪ typ urządzenia. ○ NDR / IDS / IPS odbiera alerty (anomalia, C2, lateral movement), <ul style="list-style-type: none"> ▪ pobiera kontekst incydentu: <ul style="list-style-type: none"> ▪ IP, porty, protokół, ▪ czas, wolumen ruchu, ▪ koreluje zdarzenia z innymi źródłami (SIEM, EDR), ▪ uruchamia scenariusze reakcji: ▪ eskalacja, ○ firewall / UTM, <ul style="list-style-type: none"> ▪ dodanie adresu IP do listy blokowanych, ▪ tymczasowe zablokowanie komunikacji, ▪ cofnięcie reguły po incydencie, ▪ sprawdzenie reputacji IP/URL, ▪ pobranie logów i kontekstu.

- konfigurację scenariuszy reagowania (playbooków),
- konfigurację mechanizmów automatyzacji,
- opracowanie procedur operacyjnych i automatyzacji,
- przeprowadzenie testów funkcjonalnych i integracyjnych,
- przygotowanie dokumentacji,
- przeprowadzenie szkolenia.

4. Wymagania funkcjonalne

System musi zapewniać:

- obsługę incydentów bezpieczeństwa (case management),
- rejestrację, klasyfikację i obsługę incydentów,
- możliwość tworzenia, modyfikacji i wykonywania scenariuszy reagowania (playbooków),
- automatyczne i półautomatyczne wykonywanie działań,
- agregację danych z systemu SIEM oraz innych źródeł,
- integrację z systemami zewnętrznymi (API, webhook, konektory),
- przypisywanie incydentów i zadań do użytkowników,
- eskalację incydentów,
- rejestrowanie i rozliczalność działań,
- obsługę powiadomień.

5. Wymagania techniczne

Rozwiązanie musi:

- być oparte o oprogramowanie open-source lub rozwiązanie równoważne,
- umożliwiać korzystanie z podstawowych funkcjonalności systemu bez obowiązkowych opłat licencyjnych,
- posiadać publicznie dostępny kod źródłowy lub być dostępne na zasadach licencji open-source,
- umożliwiać wdrożenie w infrastrukturze Zamawiającego (on-premise lub środowisko wirtualne),
- nie wymagać korzystania z usług chmurowych producenta jako warunku działania,
- umożliwiać integrację z systemem SIEM poprzez API, webhook lub inne mechanizmy,
- umożliwiać komunikację poprzez bezpieczne protokoły (np. HTTPS),
- umożliwiać zarządzanie użytkownikami i uprawnieniami,
- zapewniać rejestrowanie zdarzeń i działań,
- umożliwiać rozbudowę rozwiązania.

System musi obejmować jednocześnie:

- zarządzanie incydentami (case management),
- automatyzację działań (playbooki).
- Za rozwiązania spełniające wymagania uznaje się w szczególności:
 - TheHive wraz z Cortex,
 - Shuffle,
 lub rozwiązania równoważne.

6. Wymagania bezpieczeństwa

System musi zapewniać:

- uwierzytelnianie użytkowników,

17 7 14 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100

	<ul style="list-style-type: none"> ▪ kontrolę dostępu opartą o role, ▪ rejestrowanie aktywności użytkowników, ▪ ochronę danych przetwarzanych w systemie, ▪ bezpieczną komunikację, ▪ rozliczalność działań, ▪ możliwość audytu działań. <p>7. Wdrożenie (instalacja, konfiguracja, uruchomienie) Wykonawca zobowiązany jest do:</p> <ul style="list-style-type: none"> ▪ instalacji i konfiguracji systemu, ▪ konfiguracji integracji z SIEM i innymi systemami, ▪ wdrożenia scenariuszy reagowania, ▪ przeprowadzenia testów funkcjonalnych i integracyjnych, ▪ usunięcia błędów, ▪ przekazania systemu do eksploatacji. <p>8. Dokumentacja Wykonawca dostarczy:</p> <ul style="list-style-type: none"> ▪ dokumentację powdrożeniową, ▪ opis architektury rozwiązania, ▪ opis konfiguracji i integracji. <p>9. Szkolenia Wykonawca przeprowadzi szkolenie obejmujące:</p> <ul style="list-style-type: none"> ▪ obsługę systemu, ▪ zarządzanie incydentami, ▪ tworzenie i modyfikację scenariuszy reagowania, ▪ podstawy administracji systemem. <p>10. Warunki odbioru Odbiór nastąpi po:</p> <ul style="list-style-type: none"> ▪ uruchomieniu systemu, ▪ wykonaniu integracji, ▪ wdrożeniu scenariuszy reagowania, ▪ przeprowadzeniu testów, ▪ przekazaniu dokumentacji, ▪ przeprowadzeniu szkolenia. <p>11. Okres realizacji</p> <ul style="list-style-type: none"> ▪ Maksymalnie do 30.09.2026 <p>12. Gwarancja i wsparcie</p> <ul style="list-style-type: none"> ▪ Minimum 12 miesięcy wsparcia wdrożeniowego. <p>13. Postanowienia końcowe Dopuszcza się rozwiązania open-source równoważne pod warunkiem zapewnienia co najmniej równoważnej funkcjonalności, parametrów technicznych oraz możliwości integracyjnych.</p>
<p>4.10. Wdrożenie systemu do zarządzania logami</p>	<p>1. Przedmiot zamówienia Przedmiotem zamówienia jest usługa obejmująca wdrożenie, konfigurację oraz integrację systemu open-source do zarządzania logami, umożliwiającego centralne zbieranie, przetwarzanie, przechowywanie, przeszukiwanie oraz analizę danych dzienników zdarzeń.</p>

K-7 4 MA Nowe

Rozwiązanie powinno być oparte o technologie open-source (np. Graylog lub rozwiązanie równoważne).

Zakres obejmuje środowiska:

- IT (serwery, systemy operacyjne, aplikacje, urządzenia sieciowe),
- OT/ICS/IIoT (w zakresie dostępnych źródeł danych i integracji).

2. Cel zamówienia

Celem zamówienia jest wdrożenie funkcjonalności umożliwiających:

- centralne gromadzenie logów,
- przeszukiwanie i analizę danych dzienników zdarzeń,
- zwiększenie widoczności zdarzeń w środowisku IT oraz OT,
- wsparcie analiz operacyjnych i audytowych,
- uporządkowanie retencji i archiwizacji logów,
- przygotowanie danych do dalszej analizy w systemach klasy SIEM i SOAR.

3. Zakres zamówienia

Zakres obejmuje w szczególności:

- instalację i konfigurację rozwiązania,
- wdrożenie komponentów odpowiedzialnych za:
 - zbieranie logów,
 - przetwarzanie i normalizację danych,
 - indeksowanie i przechowywanie danych,
 - wyszukiwanie i wizualizację,
 - konfigurację źródeł logów (agentowych i bezagentowych),
 - integrację z systemami monitorowania sieci,
 - integracji z systemem SIEM
 - przesyłanie zdarzeń (syslog, API, message queue),
 - mapowanie pól (normalizacja),
 - oznaczanie poziomu ważności (severity),
 - przekazywanie metadanych (host, źródło, czas).
 - integrację z systemami OT/ICS/IIoT (jeżeli dostępne są źródła danych),
 - konfigurację parserów, pipeline'ów oraz reguł przetwarzania logów,
 - konfigurację zasad retencji, archiwizacji i rotacji danych,
 - konfigurację dashboardów, raportów i widoków analitycznych,
 - przygotowanie raportów lub szablonów raportów audytowych,
 - przeprowadzenie testów i uruchomienie produkcyjne.

4. Wymagania funkcjonalne

Rozwiązanie musi zapewniać co najmniej:

- centralne zbieranie logów z wielu źródeł,
- odbiór logów (np. syslog, API, agenty, inne wspierane mechanizmy),
- przetwarzanie, filtrowanie i normalizację danych,
- indeksowanie i przechowywanie logów,
- konfigurację retencji i rotacji danych,
- przeszukiwanie logów w czasie rzeczywistym i historycznie,
- wizualizację danych (dashboardy),
- możliwość definiowania parserów i reguł przetwarzania (pipeline rules),
- generowanie raportów operacyjnych i audytowych,

- mechanizmy alertowania na podstawie warunków logicznych,
 - integrację z systemami SIEM, SOAR oraz innymi narzędziami bezpieczeństwa,
 - możliwość obsługi środowisk IT oraz – w zakresie dostępnych danych – OT/ICS,
 - skalowalność rozwiązania.
- 5. Wymagania techniczne**
- Rozwiązanie musi:
- być oparte o technologie open-source lub równoważne,
 - nie wymagać obowiązkowych opłat licencyjnych za podstawowe funkcjonalności,
 - umożliwiać wdrożenie w środowisku lokalnym (on-premise),
 - współpracować z backendem indeksującym (np. OpenSearch lub równoważnym),
 - wspierać systemy Windows i Linux,
 - umożliwiać odbiór logów z urządzeń sieciowych (np. syslog),
 - wspierać standardowe protokoły (syslog, API),
 - umożliwiać skalowanie rozwiązania,
 - umożliwiać integrację z systemami zewnętrznymi (SIEM, SOAR, ITSM).
- 6. Wymagania bezpieczeństwa**
- Rozwiązanie musi zapewniać:
- uwierzytelnianie użytkowników,
 - zarządzanie rolami i uprawnieniami,
 - szyfrowanie komunikacji,
 - rejestrowanie działań użytkowników i administratorów,
 - zapewnienie integralności danych logów,
 - możliwość integracji z LDAP / Active Directory.
- 7. Wdrożenie (instalacja, konfiguracja, uruchomienie)**
- Wykonawca zobowiązany jest do:
- instalacji i konfiguracji rozwiązania,
 - integracji ze wskazanymi źródłami logów,
 - konfiguracji parserów, pipeline'ów oraz retencji danych,
 - konfiguracji dashboardów i raportów,
 - przeprowadzenia testów,
 - uruchomienia systemu w środowisku produkcyjnym.
- 8. Dokumentacja**
- Wykonawca dostarczy:
- dokumentację techniczną,
 - dokumentację konfiguracji,
- 9. Szkolenia**
- Wykonawca przeprowadzi szkolenie obejmujące:
- obsługę systemu,
 - analizę i przeszukiwanie logów,
 - administrację i konfigurację,
 - tworzenie dashboardów i raportów.
- 10. Warunki odbioru**

	<p>Odbiór nastąpi po:</p> <ul style="list-style-type: none"> ▪ uruchomieniu rozwiązania, ▪ potwierdzeniu zbierania logów z uzgodnionych źródeł, ▪ przetestowaniu funkcjonalności, ▪ przekazaniu dokumentacji, ▪ przeprowadzeniu szkolenia. <p>11. Okres realizacji</p> <ul style="list-style-type: none"> ▪ Maksymalnie do 30.09.2026 <p>12. Gwarancja i wsparcie</p> <ul style="list-style-type: none"> ▪ Minimum 12 miesięcy wsparcia wdrożeniowego. <p>13. Postanowienia końcowe</p> <p>Wszystkie wymagania określone w niniejszym OPZ należy traktować jako minimalne. Zamawiający dopuszcza zastosowanie rozwiązania open-source (np. Graylog) lub rozwiązania równoważnego.</p>
--	---

Wzrost: 180
Ciężar ciała: 75

11-7 7 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100