

**„Podniesienie poziomu cyberbezpieczeństwa w Mieście i Gminie Pleszew”,
zadanie 1 - sprzęt**

Nr postępowania: WR.042.03.2024

Opis przedmiotu zamówienia

1. Biblioteka taśmowa – 1 szt.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Obudowa	Przystosowana do montażu w szafie rack 19", wysokość nie większa niż 2U
Napędy taśmowe	Biblioteka taśmowa musi być wyposażona w min. 1 napędy taśmowy LTO9 o natywnym interfejsie SAS, o prędkości min. 12Gb/s
Liczba slotów – storage	Biblioteka musi mieć min. 16 kieszeni na nośniki taśmowe, wszystkie muszą być możliwe do użycia przez zamawiającego. Biblioteka musi posiadać min. 1 kieszeń „mail slot”.
Zarządzanie	Biblioteka musi być zarządzana z poziomu frontowego panelu urządzenia wyposażonego w wyświetlacz LCD zabezpieczonego hasłem lub/i numerem PIN oraz zdalnego modułu zarządzania przez panel WWW (HTML5). Biblioteka musi udostępniać funkcje monitorowania stanu napędów i robota. Biblioteka taśmowa powinna mieć również możliwość zdalnego monitorowania stanu urządzenia i wychwytywania błędów i przeprowadzania testów diagnostycznych. Obsługa SNMP, Syslog. Biblioteka musi posiadać min. 1 interfejs 1GbE do zarządzania. Interfejs musi być zlokalizowany na module zarządzania biblioteką
Dodatkowe oprogramowanie	Biblioteka musi zostać dostarczona z oprogramowaniem pozwalającym na backup jednego serwera z systemem Windows. Oprogramowanie musi wspierać następujące funkcjonalności: deduplikacja, oraz wspierać metody backupu przynajmniej: Disk-to-disk-to-tape, disk-to-tape, archive-to-tape w formacie natywnym.
Kompatybilność	Microsoft Windows, Red Hat Linux, SUSE Linux, Mac OS
Gwarancja	Biblioteka musi posiadać gwarancję producenta minimum 3 lata
Taśmy	Sprzęt powinien być dostarczony wraz z 24 taśmami LTO-9 oraz 2 taśmami czyszczącymi.
Inne	Jeśli do jakiegokolwiek wyżej opisanej funkcjonalności lub rozbudowy fizycznej wymagane jest dostarczenie licencji, to licencje muszą być dostarczone w ramach tego postępowania.

2. Przełączniki sieciowe zarządzalne typ I – 10 szt

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Założenia	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych
Parametry fizyczne platformy	Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Maksymalny pobór mocy: 60 W. Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe	Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 48 porty GE RJ-45. e) 4 porty 10 GE SFP+.
Zarządzanie	<ul style="list-style-type: none"> ▪ Wbudowany 1 port konsoli szeregowej do pełnego zarządzania ▪ Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). ▪ Wsparcie dla SNMP w wersjach 1-3 ▪ Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. ▪ Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. ▪ Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. ▪ Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). ▪ Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. ▪ Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. ▪ Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	<ul style="list-style-type: none"> ▪ Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. ▪ Tablica adresów MAC o pojemności co najmniej 32k wpisów. ▪ Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	<ul style="list-style-type: none"> ▪ Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. ▪ Obsługa Jumbo Frames. ▪ Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). ▪ Agregacja portów zgodna ze standardem 802.3ad. ▪ Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. ▪ Obsługa routingu statycznego. ▪ Port-mirroring. ▪ Uwierzytelnianie 802.1x na poziomie portu. ▪ Uwierzytelnianie 802.1x w oparciu o adres MAC.

	<ul style="list-style-type: none"> W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. Obsługa protokołu sFlow.
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania	<ol style="list-style-type: none"> 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: <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. Musi być możliwe redundantne połączenie z elementami zarządzającymi. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wymagania ogólne	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju

i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

3. Przełączniki sieciowe zarządzalne typ II - 2 szt.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Założenia	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych
Parametry fizyczne platformy	<ul style="list-style-type: none"> Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Maksymalny pobór mocy: 30 W. Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe	Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: a) 24 porty GE RJ-45. e) 4 porty 10 GE SFP+.
Zarządzanie	<ul style="list-style-type: none"> Wbudowany 1 port konsoli szeregowej do pełnego zarządzania Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). Wsparcie dla SNMP w wersjach 1-3 Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	<ul style="list-style-type: none"> Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. Tablica adresów MAC o pojemności co najmniej 32k wpisów. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.
Wymagane funkcje	<ul style="list-style-type: none"> Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. Obsługa Jumbo Frames. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).

	<ul style="list-style-type: none"> • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania	<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. <p>Musi być możliwe redundantne połączenie z elementami zarządzającymi. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania</p>
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> • System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.
Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego

	wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wymagania ogólne	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

4. Przełączniki sieciowe zarządzalne typ III - 2 szt

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Założenia	W ramach postępowania wymagany jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych
Parametry fizyczne platformy	<ul style="list-style-type: none"> Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. Zasilanie AC 230V. Wymagany - z możliwością wymiany w czasie pracy - redundantny zasilacz. Maksymalny pobór mocy: 180 W. Minimalny zakres temperatury pracy: 0-40°C.
Interfejsy sieciowe	Wymagany jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: <ul style="list-style-type: none"> 24 porty 10 GE SFP+ 2 porty 100 GE QSFP28
Zarządzanie	<ul style="list-style-type: none"> Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania. Wbudowany 1 port konsoli szeregowej do pełnego zarządzania. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). Wsparcie dla SNMP w wersjach 1-3. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. Automatycznie wykonywane rewizje konfiguracji.
Parametry wydajnościowe	<ul style="list-style-type: none"> Przepustowość urządzenia - min. 880 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 1300 Mpps. Tablica adresów MAC o pojemności co najmniej 64 k wpisów. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund

Wymagane funkcje	<ul style="list-style-type: none"> • Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. • Obsługa Jumbo Frames. • Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). • Agregacja portów zgodna ze standardem 802.3ad. • Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. • Obsługa routingu statycznego. • Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP. • Port-mirroring. • Uwierzytelnianie 802.1x na poziomie portu. • Uwierzytelnianie 802.1x w oparciu o adres MAC. • W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN). • W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. • W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. • Obsługa protokołu sFlow.
Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania	<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. <p>Musi być możliwe redundantne połączenie z elementami zarządzającymi. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania</p>
Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa	<ul style="list-style-type: none"> • System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. • System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie	System musi być objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wymagania ogólne	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

5. Dyski do macierzy - 6 szt.

Zamawiający posiada macierz NetApp EF 300 obsadzoną dyskami SSD 1.9TB NVMe SED. Wymagane jest dostarczenie dysków wraz z oprogramowaniem kompatybilnych dla wyżej wskazanej macierzy.

Gwarancja na dyski minimum 24 miesiące, uszkodzone nośniki pozostają własnością zamawiającego.

6. Serwer do obsługi backupu - 1 szt.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Obudowa	<ul style="list-style-type: none"> Obudowa Rack o wysokości max 2U z możliwością instalacji 8 dysków 2.5" Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. <p>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) przy użyciu jednego z protokołów BLE/ WIFI.</p>
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.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych
Procesor	Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.9GHz, klasy x86, dedykowane do pracy z zaofertowanym serwerem, umożliwiające osiągnięcie wyniku min. 177 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	384GB DDR5 RDIMM 5600MT/s,
Funkcjonalność pamięci RAM	<ul style="list-style-type: none"> • Demand Scrubbing, • Patrol Scrubbing, Permanent Fault Detection (PFD)
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"> ○ 1x dysk SSD SATA o pojemności min. 480GB, Hot-Plug Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.
Gniazda PCI	Cztery sloty PCIe
Interfejsy sieciowe/FC/SAS	<ul style="list-style-type: none"> • Wbudowane 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) Dwie karty sieciowe 25Gb Ethernet 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 • 2 porty VGA z czego jeden z przodu obudowy Możliwość rozbudowy o port RS232
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024
Wentylatory	Redundantne, Hot-Plug
Zasilacze	Redundantne, Hot-Plug min. 1100W 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	System operacyjny spełniający nw. wymagania minimalne: <ol style="list-style-type: none"> 1) Możliwość wykorzystania 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2) Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3) Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania 7000 maszyn wirtualnych. 4) Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<ol style="list-style-type: none"> 5) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6) Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7) Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8) Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9) Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10) Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11) Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12) Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET 13) Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. 14) Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. 15) Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych. 16) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, 17) Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji. 18) Mechanizmy logowania w oparciu o: <ol style="list-style-type: none"> a) Login i hasło, b) Karty z certyfikatami (smartcard), c) Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), 19) Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych. 20) Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). 21) Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<p>22) Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.</p> <p>23) Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).</p> <p>24) Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.</p> <p>25) Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:</p> <ul style="list-style-type: none"> a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: <ul style="list-style-type: none"> i) Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, ii) Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, iii) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. iv) Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1 i wyższych. c) Zdalna dystrybucja oprogramowania na stacje robocze. d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: <ul style="list-style-type: none"> i) Dystrybucję certyfikatów poprzez http ii) Konsolidację CA dla wielu lasów domeny, iii) Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, iv) Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wsparcie dla algorytmów Suite B (RFC 4869), l) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<p>m) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:</p> <ul style="list-style-type: none"> i) Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, ii) Obsługi ramek typu jumbo frames dla maszyn wirtualnych. iii) Obsługi 4-KB sektorów dysków iv) Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra v) Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. vi) Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode) <p>26) Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.</p> <p>27) Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).</p> <p>28) Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.</p> <p>29) Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>30) Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p>31) Zorganizowany system szkoleń i dostępne materiały edukacyjne w języku polskim.</p>
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 twardych. • 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 <p>Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo</p>

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Karta Zarządzania	<p>mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).</p> <p>Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiającą:</p> <ul style="list-style-type: none"> • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykację i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera <p>oraz z możliwością rozszerzenia funkcjonalności o:</p> <ul style="list-style-type: none"> • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej • Przesyłanie danych telemetrycznych w czasie rzeczywistym • Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze <p>Automatyczna rejestracja certyfikatów (ACE)</p>
Oprogramowanie do zarządzania	<p>Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania:</p> <ul style="list-style-type: none"> • 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

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<ul style="list-style-type: none"> • Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is” do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) • Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. <p>Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.</p>
Oprogramowanie do monitorowania	<p>Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności:</p> <ul style="list-style-type: none"> ○ Monitoring:

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<ul style="list-style-type: none"> ○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: <ul style="list-style-type: none"> ● Obciążeniu procesora ● Zużyciu pamięci RAM ● Temperaturze procesorów ● Temperaturze powietrza wlotowego ● Zużyciu prądu ● Zmianach w fizycznej konfiguracji serwera ● Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliiach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: <ul style="list-style-type: none"> ● Opóźnieniach ● IOPS ● Przepustowości ● Utylizacji kontrolerów ● Pojemności całkowita i dostępna ● Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ● Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliiach.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<ul style="list-style-type: none"> • Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata • Informacje o poziomie redukcji danych • Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: <ul style="list-style-type: none"> • Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny • Stanie komponentów: zasilacze, wentylatory • Podłączonych hostach • Ilości i statusu portów • Utylizacji procesora • Utylizacji poszczególnych portów • Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Aktualizacja firmware ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiązań HCI, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania ○ możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania ○ Raporty ○ Możliwość generowania raportów dla serwerów zawierających informację o: <ul style="list-style-type: none"> • Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej • Średnim obciążeniu: procesorów, pamięci RAM, IO, ○ Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: <ul style="list-style-type: none"> • Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji ○ Generowanie raportów do plików CSV i PDF ○ Cyberbezpieczeństwo ○ Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. ○ Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<ul style="list-style-type: none"> ○ Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. ○ Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. ○ Wspierane urządzenia ○ Urządzenie Producenta dostarczane w ramach postępowania ○ Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) ○ Wirtualny asystent ○ Wbudowana w platformę funkcjonalność wirtualnego asystenta w oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury; ○ Możliwość rozszerzenia funkcjonalności ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. ○ Inne ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android ○ Certyfikaty ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami: <ul style="list-style-type: none"> • ISO 27001 • NIST Security and Privacy Controls for Federal Information Systems and Organization <p>CSA Cloud Control Matrix</p>
Certyfikaty	<ul style="list-style-type: none"> • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	<ul style="list-style-type: none"> • Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<ul style="list-style-type: none"> Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	<ul style="list-style-type: none"> Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 3 lat. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych) Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. 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 otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wsparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: <ul style="list-style-type: none"> Możliwość utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
	<ul style="list-style-type: none"> ○ Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę serwisową. ○ Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. ○ Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i prześle dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. <ul style="list-style-type: none"> • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. <p>Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.</p>
Inne wymagania	Produkt musi pochodzić z autoryzowanego kanału sprzedaży. Wymagana autoryzacja wykonawcy. Zamawiający zastrzega sobie prawo do sprawdzenia legalności pochodzenia produktu.

7. Dysk sieciowy do kopii zapasowych typ I - 1 szt

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Procesor	4-rdzeniowy o taktowaniu minimum 2.2 GHz, procesor musi osiągać wynik co najmniej 5400 punktów w teście porównawczym znajdującym się na stronie https://www.cpubenchmark.net/
Architektura procesora	64-bitowy x86
Koprocesor arytmetyczny	Tak
Obudowa	Rack 2U o maksymalnych wymiarach, 89(H) x 490(W) x 300(D) mm, wraz z szynami do montażu w szafie rack
Pamięć RAM	4GB UDIMM DDR4, możliwość rozszerzenia pamięci RAM do 64GB
Pamięć flash	5GB
Ilość obsługiwanych dysków	8 dysków 3,5-calowych SATA 6Gb/s
Slot M.2	2 sloty na dyski M.2 PCIe NVMe SSD
Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (RJ45) 2 porty 10GbE SFP+ (możliwość dołożenia karty sieciowej, zgodnej z listą kompatybilną producenta serwera sieciowego) doposażonej w 2 moduły SFP+ SR 300m możliwość zamontowania (jako opcja): <ul style="list-style-type: none"> – dodatkowej karty sieciowej 10GbE, – dodatkowej karty sieciowej 25GbE, – dodatkowej karty sieciowej FC, – obsługa VLAN i Jumbo Frame.
Gniazdo PCIe	Gniazdo 1: PCIe Gen 3 x8
Porty USB	2 x USB Typu-C 3.2 Gen 2 (10Gb/s) 2 x USB Typu-A 3.2 Gen 2 (10Gb/s)
Wskaźniki LED	HDD 1-8, Stan, LAN, USB, zasilanie
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0, 1, 5, 6, 10, 50, 60, Tripple Mirror, Tripple Parity
Funkcja Hot Spare	RAID Hot Spare and Global Hot Spare
Szyfrowanie	Możliwość szyfrowania folderów i wolumenów kluczem AES 256-bit.
Wspierane Systemy Operacyjne	<ol style="list-style-type: none"> 1. Apple Mac OS 10.10 or later 2. Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 or later Linux 3. IBM AIX 7, Solaris 10 or later UNIX 4. Microsoft Windows 7, 8, and 10 5. Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019
Stacja monitoringu	w standardzie 8 licencji na podłączenie kamer (możliwość rozbudowy poprzez zakup dodatkowych licencji)
Protokoły	CIFS, SMB, AFP, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Stacja monitoringu, Windows ACL, Serwer plików, Manager plików przez WWW, Obsługa plików QPKG, Funkcja Virtual Disk umożliwiające zwiększenie pojemności serwera przy pomocy inicjatora iSCSI, Montowanie obrazów ISO, Klient LDAP, Serwer Syslog, Server VPN, Obsługa kontenerów (LXC, Docker), Funkcja migawek, Migawki (min. 1024)
Zarządzanie dyskami	Skanowanie w poszukiwaniu złych sektorów, odczyt S.M.A.R.T
Język GUI	Polski

Waga	Maksymalnie 10 kg (brutto)
System plików	Dyski wewnętrzne ZFS lub EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
Funkcje ZFS	Linioowa deduplikacja, kompresja i kompakcja, Cache odczytu & ZIL
Zasilanie	Minimalnie 250W, 100–240 V
Wentylatory	minimalnie 3 x 60 mm
Gwarancja i serwis serwera NAS	3 lata gwarancji producenta z opcją rozszerzenia do lat 5
Ilość zamontowanych dysków	8 dysków o pojemności minimalnej 16TB każdy, SATA, 7200RPM, 512MB cache, min 2 mln godzin MTBF, przeznaczonych do pracy w serwerach NAS w trybie 24/7, gwarancja producenta 5 lat, dyski muszą znajdować się na liście dysków kompatybilnych producenta serwera NAS
Dyski zapasowe	2 dyski zapasowe identyczne jak w serwerze NAS: Pojemność minimalna 16TB każdy, SATA, 7200RPM, 512MB cache, min 2 mln godzin MTBF, przeznaczonych do pracy w serwerach NAS w trybie 24/7, gwarancja producenta 5 lat, dyski muszą znajdować się na liście dysków kompatybilnych producenta urządzenia
Inne wymagania	Produkt musi pochodzić z autoryzowanego kanału sprzedaży. Wymagana autoryzacja wykonawcy. Zamawiający zastrzega sobie prawo do sprawdzenia legalności pochodzenia produktu

8. Dysk sieciowy do kopii zapasowych typ II – 2 szt

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Procesor	4-rdzeniowy o taktowaniu minimum 1.7 GHz, procesor musi osiągać wynik co najmniej 1150 punktów w teście porównawczym znajdującym się na stronie https://www.cpubenchmark.net/ (przykładowy model 4-core Alpine AL324 64-bitowy ARM® Cortex-A57 1,7 GHz lub równoważny o nie gorszych parametrach)
Obudowa	Rack 1U o maksymalnych wymiarach, 44(H) x 440(W) x 480(D) mm, wraz z szynami do montażu w szafie rack
Pamięć RAM	2GB DDR4, z możliwością rozbudowy do 16GB
Pamięć flash	512MB
Ilość obsługiwanych dysków	4 dyski 3,5" / 2.5" SATA 6 Gb/s, 3 Gb/s
Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) , 2 porty 10GbE SFP+ wyposażonej w 2 moduły SFP+ SR 300m możliwość dołożenia karty sieciowej 10GbE, obsługa VLAN i Jumbo Frame
Gniazdo PCIe	Gniazdo 1: PCIe Gen 2 x2
Porty	4x USB 3.2 Gen 1
Wskaźniki LED	HDD 1–4, stan, LAN
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,6,10. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.

Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
System Operacyjny	Apple Mac OS 10.10 oraz nowsze Ubuntu 14.04, CentOS 7, RHEL 6.6, SUSE 12 i nowsze Linux IBM AIX 7, Solaris 10 or later UNIX Microsoft Windows 7, 8, 10 Microsoft Windows Server 2008 R2, 2012, 2012 R2 and 2016, 2019
Stacja monitoringu	w standardzie 8 licencji na podłączenie kamer (możliwość rozbudowy poprzez zakup dodatkowych licencji)
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Stacja monitoringu, Windows ACL, Integracja w Windows ADS, Serwer wydruku, Serwer WWW, Serwer plików, Manager plików przez WWW, Funkcja Virtual Disk umożliwiające zwiększenie pojemności serwera przy pomocy protokołu iSCSI, Montowanie obrazów ISO, Replikacja w czasie rzeczywistym, Serwer RADIUS, Klient LDAP, Serwer Syslog, Container Station
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów
Język GUI	Polski
Gwarancja i serwis	36 miesięcy producenta z możliwością wydłużenia do lat 5
Waga	Maksymalnie 10kg
Pobór mocy	Maksymalnie 40W w trybie pracy
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Zasilanie	Minimalnie 250W, 100–240 V
Wentylatory	Minimalnie 2 x 40mm, 12V DC
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.
Ilość zamontowanych dysków	4 dyski o pojemności minimalnej 16TB każdy, SATA, 7200RPM, 512MB cache, min 2 mln godzin MTBF, przeznaczonych do pracy w serwerach NAS w trybie 24/7, gwarancja producenta 5 lat, dyski muszą znajdować się na liście dysków kompatybilnych producenta serwera NAS
Dyski zapasowe	1 dysk zapasowy identyczny jak w serwerze NAS: Pojemność minimalna 16TB każdy, SATA, 7200RPM, 512MB cache, min 2 mln godzin MTBF, przeznaczonych do pracy w serwerach NAS w trybie 24/7, gwarancja producenta 5 lat, dyski muszą znajdować się na liście dysków kompatybilnych producenta urządzenia
Inne wymagania	Produkt musi pochodzić z autoryzowanego kanału sprzedaży. Wymagana autoryzacja wykonawcy. Zamawiający zastrzega sobie prawo do sprawdzenia legalności pochodzenia produktu

9. Dysk do kopii zapasowych typ USB – 2 szt.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
Rodzaj urządzenia:	Napęd RDX - zewnętrzny
Kolor:	Czarny
Interfejs:	USB 3.0
Szerokość:	11 cm
Głębokość:	17.8 cm
Wysokość:	5.2 cm
Waga:	615 g
W pakiecie z:	2 kartridże 2 TB
Szybkość transmisji danych:	260 MBps (wewnętrzna)
Dołączone przewody:	1 x kabel danych
MTBF:	550,000 godzina(y)
Wymagany system operacyjny:	Apple MacOS, Linux, Microsoft Windows
Gwarancja	minimum 24 miesiące

10. Firewall dla jednostek - 2 szt.

Nazwa elementu, parametru lub cechy	Wymagane minimalne parametry techniczne
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. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu. 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	<ol style="list-style-type: none"> 1. 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. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3. Monitoring stanu realizowanych połączeń VPN. 4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
Interfejsy, Dysk, Zasilanie:	<ol style="list-style-type: none"> 1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: <ul style="list-style-type: none"> • 10 portami Gigabit Ethernet RJ-45. 2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4. System jest wyposażony w zasilanie AC.
Parametry wydajnościowe:	<ol style="list-style-type: none"> 1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps. 7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
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> <ol style="list-style-type: none"> 1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-

	<p>składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.</p> <ol style="list-style-type: none"> 11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13. 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	<ol style="list-style-type: none"> 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz: <ul style="list-style-type: none"> • Translację jeden do jeden oraz jeden do wielu. • Dedykowany ALG (Application Level Gateway) dla protokołu SIP. 3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. <ul style="list-style-type: none"> • Amazon Web Services (AWS). • Microsoft Azure. • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware NSX. • Kubernetes.
Połączenia VPN	<ol style="list-style-type: none"> 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia: <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.

	<ul style="list-style-type: none"> • 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>2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:</p> <ul style="list-style-type: none"> • Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	<p>W zakresie routingu rozwiązanie zapewnia obsługę:</p> <ol style="list-style-type: none"> 1. Routingu statycznego. 2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPv2), OSPF (w tym OSPFv3), BGP oraz PIM. 4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6. BFD (Bidirectional Forwarding Detection). 7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	<ol style="list-style-type: none"> 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	<ol style="list-style-type: none"> 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. System daje możliwość określania pasma dla poszczególnych aplikacji. 3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji	<ol style="list-style-type: none"> 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 21). 7. 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).
Kontrola WWW	<ol style="list-style-type: none"> 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. 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. 3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	<ol style="list-style-type: none"> 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą: <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. 2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

	<ol style="list-style-type: none"> 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. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	<ol style="list-style-type: none"> 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. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	<ol style="list-style-type: none"> Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze lub musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. W przypadku kiedy usługa logowania, raportowania, korelacji zdarzeń realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanych ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.

	<p>5. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.</p> <p>6. Możliwość włączenia logowania per reguła w polityce firewall.</p> <p>7. System zapewnia możliwość logowania do serwera SYSLOG.</p> <p>8. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.</p>
Testy wydajnościowe oraz funkcjonalne	Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: - Logowanie, korelowanie zdarzeń, raportowanie oraz generowanie powiadomień w oparciu o usługę realizowaną w chmurze, na okres 24 miesięcy.
Gwarancja oraz wsparcie	System jest objęty serwisem gwarancyjnym producenta przez okres minimum 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Wymagania ogólne	W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

INFORMACJE DODATKOWE

Wdrożenie

Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:

- 1) Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w pomieszczeniu wskazanym przez Zamawiającego.
- 2) Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
- 3) Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
- 4) Podłączenie wszystkich elementów do infrastruktury Zamawiającego.
- 5) Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
- 6) Dla urządzeń modułarnych wymagany jest montaż i instalacja wszystkich podzespołów.
- 7) Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchcordsy miedziane min. kat. 5 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym zgodnie z zapisami opz urządzeń).
- 8) Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ między innymi celem:
 - a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
 - b. Podłączenia urządzeń serwerowych do przełączników sieci LAN.
 - c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
 - d. Połączenia muszą wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
- 9) Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów

Instalacja i konfiguracja oprogramowania

- 10) Instalacja i konfiguracja systemów operacyjnych dla serwerów wirtualnych.

Testowanie i modyfikacja parametrów infrastruktury sieciowej

- 11) Testowanie mechanizmów bezpieczeństwa serwera,
- 12) Testowanie wydajności przesyłu i zapisu danych do środowiska LAN.
- 13) Testowanie dostępu publicznego do zasobów.
- 14) Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu.
- 15) Testowanie autoryzowanego dostępu do wewnętrznych zasobów.
- 16) Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach.

Opracowane dokumentacji powykonawczej

- 17) Wykonawca jest zobowiązany do przygotowania i przekazania Zamawiającemu dokumentacji powykonawczej, która musi zawierać:
 - a. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).
 - b. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.
 - c. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.

Prace muszą być wykonywane przez lub pod nadzorem inżyniera posiadającego certyfikaty techniczne producenta oferowanego sprzętu:

- Oferowanych serwerów NAS
- Oferowanego systemu przełączników
- Oferowanego firewalla