Załącznik nr 1 do OPZ – Wymagania na elementy Infrastruktury techniczno-systemowej

Dostosowanie Dziedzinowych Systemów Informatycznych w SP ZOZ MSWiA w Koszalinie do współpracy z Platformą e-Usług w celu realizacji e-usług: e-Rejestracja, e-EDM i e-Analizy.

Projekt e-Zdrowie w SP ZOZ MSWiA: rozwój nowoczesnych e-usług publicznych dla pacjentów

W ramach realizacji zamówienia, po rozstrzygnięciu przetargu na dostawę infrastruktury informatycznej realizowanego przez Lidera w ramach Projektu e-Zdrowie, Zamawiający udostępni Wykonawcy następujący sprzęt komputerowy i oprogramowanie:

Lp.	Typ	Ilość szt.	Specyfikacja
			SERWERY
1	**Serwer aplikacyjny Typ 2**	3	Płyta główna: - Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; - wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa minimum 8TB pamięci RAM DDR4 3200 MT/s; - Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 6TB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) - Minimum 5 złącz PCI Express generacji 4, w tym minimum 2 złącza o prędkości x16 i 3 złącza o prędkości x8; - Wszystkie złącza PCI Express muszą być aktywne; - Możliwość instalacji minimum 2 dysków M.2 na płycie głównej lub dedykowanej karcie PCI Express nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora z M.2 bez zajmowania klatek dyskowych serwera) Procesory: - Zainstalowane minimum dwa procesory szesnastordzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECrate2017_int_base minimum 230 pkt - Wynik dla oferowanego serwera wraz z oferowanymi procesorami dostępny na stronie spec.org; (nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych) Pamięć RAM: -Zainstalowane minimum 512 GB pamięci RAM typu DDR4 Registered, minimum 3200MT/s w kościach o pojemności 32GB; - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Resilient Memory, Memory Self-Healing lub równoważnej; Kontrolery dyskowe: - Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 minimum 2GB pamięci podręcznej cache, - Wyposażony w nieulotną pamięć cache (nie dopuszcza się baterii z uwagi na ograniczoną żywotność); Dyski twarde: - Zainstalowane 2 dyski SSD minimum 480GB SATA o parametrze DWPD minimum 3, dyski hotplug; - Minimum 8 wnęk dla dysków twardych Hotplug 2,5 cala, możliwość rozbudowy do 16 dysków twardych Hotplug 2,5 cala - W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego

			Kontrolery LAN: - Jedna dwuportowa karta 2x1Gbit/s RJ45; - Dodatkowa osobna karta 2x 10Gbit/s SFP+ wspierająca wirtualizacje (z podziałem na wirtualne karty o definiowalnej przepustowości); - Dodatkowa osobna karta 2x 10Gbit/s SFP+ wspierająca wirtualizacje (z podziałem na wirtualne karty o definiowalnej przepustowości; - 4 x moduły 10GBase-SR SFP+ jeśli nie są na wyposażeniu dostarczanych kart - Dopuszcza się kartę z portami 2x1Gbit/s RJ45 i max 2x10Gbit/s SFP+ Kontrolery I/O FC/SAS/Inne: - minimum dwie jednoportowe karty FC x 16Gb, z których każda wyposażona jest w moduł 16Gb; Porty: -zintegrowana karta graficzna ze złączem VGA; -1x USB 2.0 dostępne na froncie obudowy -1x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera - - dodatkowe złącze VGA lub złącze cyfrowe HDMI lub DP dostępne z przodu serwera; Ilość dostępnych złącz VGA lub złącze cyfrowe HDMI lub DP i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; Zasilanie, chłodzenie: - Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) - Redundantne wentylatory hotplug; Zarządzanie: - Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM, status karty zrządzającej serwera, wentylatory, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). • Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; • Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; • Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty

			rozszerzeń); • Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; Funkcjonalność konfiguracji i uruchomienia automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email) jest możliwa z poziomu dostępnego systemu zarządzania serwerami. Wspierane OS: - Windows Server 2016/2019/2022, VMWare 6.7, 7.0, Suse 15, RHEL 7/8
2	**Serwer bazodanowy Typ 2**	2	Płyta główna: - Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; - wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa minimum 8TB pamięci RAM DDR4 3200 MT/s; - Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 6TB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) - Minimum 5 złącz PCI Express generacji 4, w tym minimum 2 złącza o prędkości x16 i 3 złącza o prędkości x8; - Wszystkie złącza PCI Express muszą być aktywne; - Możliwość instalacji minimum 2 dysków M.2 na płycie głównej lub dedykowanej karcie PCI Express nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora z M.2 bez zajmowania klatek dyskowych serwera) Wyposażenie w Procesory: a) jeden procesor 64 bit o parametrach: -liczba rdzeni: 8 - procesor wspiera funkcjonalność dynamicznego i automatycznego zwiększenia wydajności serwera dla aplikacji poprzez zwiększenie częstotliwości rdzenia - Dla oferowanego serwera lub innego serwera tego samego producenta, należącego do tej samej linii produktowej i generacji jak oferowany, dwa zaoferowane procesory osiągają w teście SPEC2017 Int Rate Base publikowanym na stronach spec.org wynik minimum 140 punktów per serwer Pamięć RAM: -Zainstalowane minimum 512 GB pamięci RAM typu DDR4 Registered, minimum 3200MT/s w kościach o pojemności 64GB; - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Resilient Memory, Memory Self-Healing lub równoważnej; Kontrolery dyskowe: - Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 minimum 2GB pamięci podręcznej cache, - Wyposażony w nieulotną pamięć cache (nie dopuszcza się baterii z uwagi na ograniczoną żywotność); Dyski twarde: - Zainstalowane 2 dyski SSD minimum 480GB SATA o parametrze DWPD minimum 3 dyski hotplug; -Minimum 8 wnęk dla dysków twardych Hotplug 2,5 cala, możliwość rozbudowy do 16 dysków twardych Hotplug 2,5 cala

			-W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego Kontrolery LAN: - Jedna dwuportowa karta 2x1Gbit/s RJ45; - Dodatkowa osobna karta 2x 10Gbit/s SFP+ wspierająca wirtualizacje (z podziałem na wirtualne karty o definiowalnej przepustowości); - Dodatkowa osobna karta 2x 10Gbit/s SFP+ wspierająca wirtualizacje (z podziałem na wirtualne karty o definiowalnej przepustowości; - 4 x moduły 10GBase-SR SFP+ jeśli nie sa na wyposażeniu dostarczanych kart - Dopuszcza się kartę z portami 2x1Gbit/s RJ45 i max 2x10Gbit/s SFP+ Kontrolery I/O FC/SAS/Inne: - minimum jedna dwuportowa karta FC x 16Gb, gdzie każdy port jest wyposażony w moduł 16Gb; Porty: - zintegrowana karta graficzna ze złączem VGA; -1x USB 2.0 dostępne na froncie obudowy -1x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera - -dodatkowe złącze VGA lub złącze cyfrowe HDMI lub DP dostępne z przodu serwera; Ilość dostępnych złącz VGA lub złącze cyfrowe HDMI lub DP i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; Zasilanie, chłodzenie: - Redundantne zasilacze hotplug o sprawności 94% (tzw klasa Platinum) - Redundantne wentylatory hotplug; Zarządzanie: - Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM, status karty zrządzającej serwera, wentylatory, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). • Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; • Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; • Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej

			dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); • Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; Funkcjonalność konfiguracji i uruchomienia automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email) jest możliwa z poziomu dostępnego systemu zarządzania serwerami Wspierane OS: - Windows Server 2016/2019/2022, VMWare 6.7, 7.0, Suse 15, RHEL 7/8
3	**Serwer backup Typ 1**	1	Płyta główna: - Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów czterdziestordzeniowych; - wyposażona w minimum 32 gniazda pamięci RAM DDR4, obsługa minimum 8TB pamięci RAM DDR4 3200 MT/s; - Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 6TB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania, nie dopuszcza się podtrzymania bateryjnego stanu pamięci) - Minimum 5 złącz PCI Express generacji 4, w tym minimum 2 złącza o prędkości x16 i 3 złącza o prędkości x8; - Wszystkie złącza PCI Express muszą być aktywne; - Możliwość instalacji minimum 2 dysków M.2 na płycie głównej lub dedykowanej karcie PCI Express nie zajmujące klatek dla dysków hot-plug; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora z M.2 bez zajmowania klatek dyskowych serwera) Procesory: - Zainstalowane minimum dwa procesory ośmiordzeniowe w architekturze x86, gdzie w oferowanym serwerze w testach wydajności dla serwera dwuprocesorowego osiągany jest wynik dla SPECrate2017_int_base minimum 130 pkt. - Wynik dla oferowanego serwera wraz z oferowanym procesorem dostępny na stronie spec.org; (nie dopuszcza się procesora o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych) Pamięć RAM: -Zainstalowane minimum 128 GB pamięci RAM typu DDR4 Registered, minimum 3200MT/s w kościach o pojemności 32GB; - Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Resilient Memory, Memory Self-Healing lub równoważnej; Kontrolery dyskowe: - Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 minimum 2GB pamięci podręcznej cache, - Wyposażony w nieulotną pamięć cache (nie dopuszcza się baterii z uwagi na ograniczoną żywotność); Dyski twarde: - Zainstalowane 2 dyski SSD minimum 480GB SATA o parametrze DWPD minimum 3, dyski hotplug; - Zainstalowane 6 dysków NL-SAS o pojemności 8 TB każdy, dyski Hotplug; - W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego Kontrolery LAN:

			- Jedna dwuportowa karta 2x1Gbit/s RJ45; - Dodatkowa osobna karta 2x 10Gbit/s SFP+ wspierająca wirtualizacje (z podziałem na wirtualne karty o definiowalnej przepustowości); - Dodatkowa osobna karta 2x 10Gbit/s SFP+ wspierająca wirtualizacje (z podziałem na wirtualne karty o definiowalnej przepustowości; - 4 x moduły 10GBase-SR SFP+ jeśli nie są na wyposażeniu dostarczanych kart - Dopuszcza się kartę z portami 2x1Gbit/s RJ45 i max 2x10Gbit/s SFP+ Kontrolery I/O FC/SAS/Inne: - minimum dwie jednoportowe karty FC x 16Gb, z których każda wyposażona jest w moduł 16Gb; Porty: -zintegrowana karta graficzna ze złączem VGA; -1x USB 2.0 dostępne na froncie obudowy -1x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera - -dodatkowe złącze VGA lub złącze cyfrowe HDMI lub DP dostępne z przodu serwera; Ilość dostępnych złącz VGA lub złącze cyfrowe HDMI lub DP i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera; Zasilanie, chłodzenie: - Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) - Redundantne wentylatory hotplug; Zarządzanie: - Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM, status karty zrządzającej serwera, wentylatory, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera. - Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.). • Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; • Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; • Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń);

			• Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą; • karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera; Funkcjonalność konfiguracji i uruchomienia automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email) jest możliwa z poziomu dostępnego systemu zarządzania serwerami Wspierane OS: - Windows Server 2016/2019/2022, VMWare 6.7, 7.0, Suse 15, RHEL 7/8
		MACIERZ DYSKOWA	
4	**Macierz Typ 1**	2	Obudowa: 1) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych, kontrolujących wszystkie zasoby dyskowe macierzy z poziomu pojedynczej konsoli WebGUI/CLI administratora; 2) Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez kontrolery i dyski dla zapisów danych Użytkownika; 3) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19”; 4) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia); 5) Każdy moduł/obudowa macierzy powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii; 6) Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy; 7) Moduły dla dalszej rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać gęstości upakowania co najmniej 24 dysków 2,5” lub co najmniej 12 dysków 3,5” na każde maksymalne 3U przestrzeni instalacyjnej w szafie przemysłowej rack standardu 19”; 8) Dostarczona konfiguracja macierzy musi pozwalać na połączenie kaskadowe lub w układzie pętli pomiędzy modułami rozwiązania (moduł kontrolerów, moduły/półki dyskowe), z zapewnieniem wysokiej dostępności rozumianej tak, że awaria dowolnego elementu macierzy w ramach kontrolera i półki dyskowej nie może powodować braku dostępności pozostałych elementów. Okablowanie to musi być zgodne ze standardem SAS 12Gb/s. W przypadku braku obsługi połączeń w układzie pętli dopuszcza się jako alternatywne rozwiązanie macierz z zainstalowanymi 4 kontrolerami RAID; Pojemność: 1) Oferowana macierz musi obsługiwać min. 142 dyski wykonane w technologii hot-plug – jeżeli dla obsługi tej funkcjonalności konieczny jest zakup dodatkowych licencji to należy ją dostarczyć wraz z macierzą; 2) Model oferowanej macierzy musi obsługiwać przestrzeń dyskową w trybie tzw. surowym (RAW) minimum 1000 TB, bez konieczności wymiany zainstalowanych kontrolerów – wymagana zgodność z zapisami aktualnej na moment składania oferty specyfikacji technicznej macierzy, udostępnionej publicznie na stronie internetowej producenta lub jego przedstawiciela w Polsce; 3) Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych

			jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika; Kontrolery: 1) Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active lub układzie, w którym awaria, restart pojedynczego kontrolera nie spowoduje utraty wydajności macierzy. Macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami; 2) Każdy z kontrolerów macierzy musi posiadać po minimum 12 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu; 3) Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 0,8 TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie pojemności dodatkowo instalowanych dysków SSD, 4) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik; 5) Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia 6) Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach; 7) Każdy z kontrolerów RAID powinien posiadać dedykowany minimum 1 interfejs RJ-45 Ethernet obsługujący połączenia z prędkością minimum 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy; 8) Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej; 9) Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC SAN oraz NAS; 10) Dla obsługi operacji blokowych I/O w sieci IP/FC SAN kontrolery macierzy muszą wspierać protokoły transmisji: FC 16Gb/s, iSCSI 10/1Gb/s 11) Dla obsługi operacji plikowych I/O w sieci NAS kontrolery macierzy muszą wspierać minimum protokoły dostępu: CIFS, NFS. Obecnie nie jest wymagana obsługa protokołów CIFS, NFS, ale musi istnieć możliwość rozbudowy o tą funkcjonalność. 13) Kontrolery macierzy muszą obsługiwać do 30 grup dyskowych RAID w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów; Interfejsy: 1) Oferowana macierz musi posiadać minimum 4 porty FC 16Gb/s (obsadzone wkładkami) przypadające na każdy z kontrolerów, przeznaczone do dołączenia serwerów 2) Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencja na instalację i obsługę każdego z wymienionych protokołów transmisji danych; Poziomy RAID: 1) Macierz musi zapewniać dostęp do danych i dalszą pracę w przypadku awarii jednego, dwóch dowolnych dysków w każdej grupie RAID. Wspierane dyski: 1) Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex; 2) Oferowana macierz musi wspierać dyski hot-plug: - dyski elektroniczne SSD i mechaniczne HDD z interfejsami SAS12Gb/s - dyski mechaniczne HDD o prędkości obrotowej 7,2k RPM, 10k RPM, 3) Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD (SAS i NLSAS) 4) Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5”; 5) Macierz musi obsługiwać min. 72 dyski SAS SSD w całym rozwiązaniu; 6) Wymagane jest dostarczenie macierzy zawierającej min.6 dysków SSD (DWPD 3) o pojemności sumarycznej RAW min.11.52 TB, min. 12 dysków SAS o pojemności sumarycznej RAW min. 27TB o prędkości obrotowej 10 000 obr/min; Podane ilości nie uwzgledniaja dysków zapasowych hot-spare

			7) Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach: - hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID (dyski tego samego typu co dysk hot-spare); albo skonfigurowanie zapasowej przestrzeni w ramach pul dyskowych; 8) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess); 9) W przypadku awarii dysku twardego dysk uszkodzony pozostaje u Zamawiającego Opcje software'owe: 1) Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 512 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy; 2) Macierz musi umożliwiać zdefiniowanie min. 512 woluminów (LUN); 3) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego bez konieczności wyłączania macierzy; 4) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową; 5) Macierz musi posiadać wsparcie dla systemów operacyjnych: MS Windows Server 2012R2/2016/2019/2022, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, VMWare , Citrix XEN Server. 6) Macierz musi wspierać technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem) realizowaną natywnie przez obsługiwane systemy operacyjne. 7) Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym lub ciągłym i asynchronicznym, po protokołach FC lub iSCSI, bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji 8) Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy jako tzw. storage-based data replication; 9) Replikacja danych jak w pkt.7 musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych; 10) Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – Licencja na wymienioną funkcjonalność NIE JEST przedmiotem niniejszego postępowania; 11) W przypadku obsługi protokołów CIFS/SMB i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów; 12) Macierz musi obsługiwać dla interfejsów iSCSI i interfejsów obsługujących protokoły CIFS/SMB i NFS lub poprzez dedykowany kontroler systemu plików adresacje IP v.4 i IP v.6; 13) W przypadku korzystania z protokołów dostępu plikowego obsługa CIFS/SMB i NFS musi odbywać się jednocześnie; 14) Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy; 15) Model oferowanej macierzy musi wspierać rozwiązania klasy Metro Cluster w tym dla VMware vSphere Metro Storage Cluster i Microsoft Hyper-V Stretched Cluster tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji lub ciągłej danych pomiędzy minimum 2 macierzami; 16) Mechanizm Metro Cluster musi być obsługiwany zarówno w zakresie replikacji danych po protokołach FC lub IP jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy po protokołach FC lub iSCSI 17) Pod użytym w pkt. 15 pojęciem 'wysoka dostępność zasobów dyskowych' należy rozumieć zapewnienie bezprzerwowego (ub krótkotrwałej przerwy na czas restartu)

			działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej; 18) Dla uruchomienia funkcjonalności rozwiązania klasy Metro Cluster musi być możliwość wykorzystania istniejącej infrastruktury FC/IP SAN w zakresie przełączników FC/Ethernet i kart HBA FC/Ethernet zainstalowanych w serwerach; 19) Funkcjonalność mechanizmu Metro Cluster musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover); 20) Funkcjonalność mechanizmu Metro Cluster musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover); 21) Funkcjonalność mechanizmu Metro Cluster musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback); 22) Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) lub inna technologia realizująca akcelarację dysków mechanicznych tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków 23) Mechanizm AST musi być obsługiwany przy korzystaniu z minimum dwóch dostarczonych technologii dyskowych: SSD, SAS, NLSAS; 24) Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB; 25) Macierz musi być wyposażona w funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) lub równoważna technologia umożliwiająca priorytetyzację dostępu do danych Konfiguracja, zarządzanie: 1) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI) jak i plikowymi; 2) Oprogramowanie zarządzające musi być dostarczone w wariancie dla maksymalnej obsługiwanej pojemności dyskowej macierzy oraz dla maksymalnej liczby dysków wspieranej przez oferowaną macierz; 3) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 4) Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) 5) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: TLS dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI;
BIBLIOTEKA TAŚMOWA			
5	**Biblioteka taśmowa LTO-7**	1	Biblioteka modułowa obudowie RACK przystosowana do montażu w szafie 19”. Zajętość w szafie RACK dostarczanego rozwiązania – nie więcej niż 3U Biblioteka taśmowa musi być wyposażona w minimum jeden napęd LTO Ultrium-7 FC z możliwością rozbudowy do minimum 21 napędów oferowanego typu. Biblioteka musi posiadać minimum 32 sloty wewnętrzne na taśmy LTO Ultrium-7. Możliwość rozbudowy do 280 slotów. Każdy zainstalowany napęd taśmowy musi posiadać natywny interfejs Fibre Channel 8Gb/s wraz z modułem SFP 8Gb/s SR Napęd taśmowy o wydajności minimum 300MB/s. Biblioteka musi posiadać możliwość konfiguracji, co najmniej trzech tzw. „mail slot” umożliwiających wymianę pojedynczej taśmy bez konieczności wyjmowania z biblioteki całego magazynka z taśmami. Wraz z każdą biblioteką musi być dostarczonych 10 szt. taśm LTO Ultrium-7 RW (o pojemności pojedynczej taśmy, co najmniej 6TB - bez uwzględniania kompresji danych) wraz z etykietami kodów kreskowych oraz 1 szt. taśmy czyszczącej. Biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem

			przeglądarki internetowej. Biblioteka taśmowa musi być wyposażona w czytnik kodów kreskowych. Biblioteka musi być wyposażona w redundantne zasilacze 230V AC hot swap Napędy LTO Ultrium-7 muszą posiadać wsparcie dla taśm typu WORM i sprzętową enkrypcję AES 256-bit. Biblioteka taśmowa musi być kompatybilna z dostarczanym oprogramowaniem kopii zapasowych.
URZĄDZENIA SIECI KOMPUTEROWEJ			
6	**Brama UTM /Firewall Typ1**	2	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. Wysokość nie większa niż 2U. Instalacja w szafie przemysłowej rack standardu 19". System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive w ramach dostarczanych urządzeń. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System realizujący funkcję Firewall musi dysponować minimum: · 8 portami Gigabit Ethernet RJ-45. · 2 gniazdami SFP 1 Gbps. · 2 gniazdami SFP+ 10 Gbps W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. Należy zapewnić 2 wkładki 10 Gigabit Ethernet SFP+ SR System musi być wyposażony w dwa redundantne zasilacze 230V AC. · W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 50 000 nowych połączeń na sekundę. · Przepustowość Stateful Firewall: nie mniej niż 9 Gbps · Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2 Gbps. · Wydajność szyfrowania VPN IPSec - nie mniej niż 2.5 Gbps. · Wydajność IPS - nie mniej niż 2 Gbps. · Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje: · Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. · Kontrola Aplikacji. · Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. · Ochrona przed malware co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. · Ochrona przed atakami - Intrusion Prevention System.

			· Kontrola stron WWW. · Zarządzanie pasmem (QoS, Traffic shaping). · Analiza ruchu szyfrowanego protokołem SSL. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: · Translację jeden do jeden oraz jeden do wielu. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. System musi umożliwiać konfigurację połączeń typu IPSec VPN System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie routingu rozwiązanie powinno zapewniać obsługę: · Routingu statycznego. · Policy Based Routingu. · Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: · Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. · Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach System musi umożliwiać skanowanie archiwów. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

			System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. Musi istnieć możliwość logowania do serwera SYSLOG. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: · ICSA lub EAL4 dla funkcji Firewall. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: · Kontrola Aplikacji, IPS, Antywirus, Web Filtering na okres 36 miesięcy.
7	**Brama UTM /Firewall Typ2**	4	Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. Wysokość nie większa niż 1U. Instalacja w szafie przemysłowej rack standardu 19". System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive w ramach dostarczanych urządzeń. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. Monitoring stanu realizowanych połączeń VPN. System realizujący funkcję Firewall musi dysponować minimum: · 5 portami Gigabit Ethernet RJ-45. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. System musi być wyposażony w zasilacz 230V AC. W zakresie Firewall'a obsługa nie mniej niż 0.19 mln jednoczesnych połączeń oraz 13 000 nowych połączeń na sekundę. · Przepustowość Stateful Firewall: nie mniej niż 2 Gbps · Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 0.9 Gbps. · Wydajność szyfrowania VPN IPSec - nie mniej niż 1.5 Gbps. · Wydajność IPS - nie mniej niż 1 Gbps.

			· Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 0.5 Gbps. W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje: · Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. · Kontrola Aplikacji. · Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. · Ochrona przed malware co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. · Ochrona przed atakami - Intrusion Prevention System. · Kontrola stron WWW. · Zarządzanie pasmem (QoS, Traffic shaping). · Analiza ruchu szyfrowanego protokołem SSL. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz: · Translację jeden do jeden oraz jeden do wielu. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. System musi umożliwiać konfigurację połączeń typu IPSec VPN System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie routingu rozwiązanie powinno zapewniać obsługę: · Routingu statycznego. · Policy Based Routingu. · Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą: · Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. · Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach System musi umożliwiać skanowanie archiwów. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.

			Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. Musi istnieć możliwość logowania do serwera SYSLOG. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: · ICSA lub EAL4 dla funkcji Firewall. W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: · Kontrola Aplikacji, IPS, Antywirus, Web Filtering na okres 36 miesięcy.
8	**Switch agregacyjny 10G Typ 1**	4	Typ i liczba portów: • 24 porty 1/10Gigabit Ethernet SFP+ • 2 porty 40/100Gigabit Ethernet QSFP28 • 1 port 10Gb/40Gb QSFP+ Przepustowość przełącznika (switching capacity) - 880 Gbps Możliwość stworzenia wirtualnego systemu/stosu łączącego dwa urządzenia tego samego typu z zapewnieniem następujących funkcjonalności: • Połączenie urządzeń z wykorzystaniem standardowych portów 40/100GE oraz modułów optycznych/twinax • Zarządzanie poprzez jeden adres IP lub kontroler z pojedynczym adresem IP. Dla innych urządzeń system wirtualny widoczny jako pojedynczy węzeł sieciowy • Możliwość tworzenia połączeń cross-stack Link Aggregation zgodnie z IEEE 802.3ad • Wyposażenie we właściwej ilości kabli DAC 100Gb dla zapewnienia wymaganej funkcjonalności. Parametry fizyczne: • Redundantne i wymienne moduły wentylatorów • Redundantne i wymienne zasilacze prądu zmiennego AC • Możliwość wyposażenia urządzenia w zasilacze prądu stałego DC • Wysokość przełącznika 1RU • Możliwość montażu w szafie 19” • Przepływ powietrza przód-tył Parametry wydajnościowe: • Bufor pakietów – 12MB • Pamięć DRAM – 4GB • Dysk SSD – 16GB • Obsługa o 4092 sieci VLAN o 80.000 adresów MAC

			o 212.000 tras IPv4 o 128.000 tras IPv6 o 32.000 tras multicast o Ilość grup Multicast min. 4k Obsługa protokołu NTP Obsługa IGMPv1/2/3 Snooping Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree Obsługa protokołu LLDP i LLDP-MED. Mechanizmy związane z bezpieczeństwem sieci: • Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji • Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością: o dynamicznego przypisania użytkownika do określonej sieci VLAN o dynamicznego przypisania listy ACL • Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X • Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC • Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika kluczami o długości 128-bitów (gcm-aes-128) • Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X • Możliwość uwierzytelniania wielu użytkowników na jednym porcie • Obsługa funkcji Port Security, Trusted DHCP Server, DHCP Secured ARP/ARP Validation • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+ • Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 o Adres MAC źródłowy i docelowy plus maska o Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6 o Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd. o Numery portów źródłowych i docelowych TCP, UDP o Zakresy portów źródłowych i docelowych TCP, UDP o Identyfikator sieci VLAN - VLAN ID o Flagi TCP o Obsługa fragmentów • Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika • Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania • Sprzętowa obsługa sFlow lub NetFlow Możliwość uruchomienia funkcji serwera DHCP Mechanizmy związane z zapewnieniem jakości usług w sieci: • Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) • Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP • Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi (policing, rate limiting) • Kontrola sztormów dla ruchu broadcast/multicast/unicast • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP Obsługa protokołów routingu: • Routing statyczny dla IPv4 i IPv6

			• Routing dynamiczny IPv4/IPv6 – RIP, OSPF • Obsługa protokołu redundancji bramy – HSRP/VRRP • Routingu mulicastów - PIM-SM, PIM-SSM • Obsługa wirtualnych instancji routingu • Filtrowanie IGMP • Obsługa PIM-SM • Obsługa PIM-SSM • Obsługa PIM snooping • Obsługa IGMP v1 - RFC 1112 • Obsługa IGMP v2 - RFC 2236 • Obsługa IGMP v3 - RFC 3376 • Obsługa IGMP v1/v2/v3 snooping Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN Zarządzanie • Port konsoli • Dedykowany port Ethernet do zarządzania out-of-band • Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6 • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Obsługa ramek jumbo (9216 bajtów) Możliwość enkapsulacji ruchu w pakiety VXLAN Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU
9	**Switch dostępowy IG**	7	Typ i liczba portów: • 48 portów 10/100/1000BaseT RJ-45 • 4 porty 1/10G SFP+ Zasilanie i chłodzenie: • Zasilacz AC 230V. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) • Przełącznik umożliwia podtrzymanie zasilania z portów PoE podczas restartu urządzenia • Redundantne wentylatory Możliwość stackowania przełączników z zapewnieniem następujących funkcjonalności: • 8 urządzeń w stosie, przepustowości stackowania na poziomie min. 80 Gbps. • Zarządzanie poprzez jeden adres IP lub możliwość zarządzania przez kontroler. • Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad Parametry wydajnościowe: • Przepustowość przełącznika zapewniająca pracę z pełną wydajnością wszystkich portów, w tym również dla pakietów 64-bajtowych (przełącznik line-rate) • Nieblokująca architektura o wydajności przełączania min. 176 Gb/s • Szybkość przełączania min. 130 Milionów pakietów na sekundę • Pamięć DRAM – 1GB • Pamięć flash – 4GB Obsługa: • 4094 sieci VLAN IDs • 16.000 adresów MAC Obsługa protokołu NTP Obsługa IGMPv1/2/3 Snooping Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree • Obsługa PVST+ • Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 48 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie. Obsługa protokołu LLDP i LLDP-MED.

			Możliwość uruchomienia funkcji serwera DHCP Mechanizmy związane z bezpieczeństwem sieci: • Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji • Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością: o dynamicznego przypisania użytkownika do określonej sieci VLAN o dynamicznego przypisania listy ACL • Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X • Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC • Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X • Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika kluczami o długości 128-bitów (gcm-aes-128) • Możliwość uwierzytelniania wielu użytkowników na jednym porcie • Obsługa funkcji Port Security, DHCP Snooping, DHCP Secured ARP/ARP Validation • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+ • Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 o Adres MAC źródłowy i docelowy plus maska o Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6 o Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd. o Numery portów źródłowych i docelowych TCP, UDP o Zakresy portów źródłowych i docelowych TCP, UDP o Identyfikator sieci VLAN - VLAN ID o Flagi TCP o Obsługa fragmentów • Wbudowana obrona procesora urządzenia przed atakami DoS. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania • Funkcja Private VLAN •. Bezpieczeństwo MAC adresów o ograniczenie liczby MAC adresów na porcie o zatrzaśnięcie MAC adresu na porcie o możliwość wpisania statycznych MAC adresów na port/vlan • Możliwość wyłączenia MAC learning • Sprzętowa obsługa sFlow lub NetFlow Mechanizmy związane z zapewnieniem jakości usług w sieci: • Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) • Kontrola sztormów dla ruchu broadcast/multicast/unicast • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP Obsługa protokołów i mechanizmów routingu: • Routing statyczny dla IPv4 i IPv6 • Routing dynamiczny – RIP Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN Zarządzanie: • Port konsoli • Dedykowany port Ethernet do zarządzania out-of-band • Obsługa protokołów SNMPv3, SSHv2, SCP, https • Obsługa SYSLOG z możliwością definiowania wielu serwerów • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. • Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie

			Obsługa RMON min. 4 grupy: Statistics, History, Alarms, Events (RFC 1757) • Ping dla IPv4 / IPv6 • Traceroute dla IPv4 / IPv6 • Obsługa funkcji TCL/Tk w skryptach CLI • Możliwość uruchamiania skryptów ręcznie o określonym czasie lub co wskazany okres czasu na podstawie wpisów w logu systemowym • Możliwość uruchamianiai skyptów i ACL bezpośrednio na urządzeniu Możliwość montażu w szafie rack 19". Wysokość urządzenia 1 RU
10	**Moduł SFP+ 10Gb Typ 1**	54	Moduł w standardzie 10GBase-SR Muszą mieć formę SFP umożliwiając podłączenie bez wyłączania urządzenia (hot-plug). Muszą posiadać gniazda do złączy optycznych typu LC. Muszą współpracować ze światłowodami wielomodowymi na dystansie do 300m, o długości fali 850 nm. Muszą obsługiwać przepływność co najmniej 10Gb na sekundę w każdym kierunku. Muszą pracować w standardzie Ethernet.
11	**Switch serwerowy Typ 1**	4	Obsługa IGMPv1/2/3 Snooping Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci: • IEEE 802.1w Rapid Spanning Tree • IEEE 802.1s Multi-Instance Spanning Tree • Obsługa PVST+ • Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 48 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie. Obsługa protokołu LLDP i LLDP-MED. Możliwość uruchomienia funkcji serwera DHCP Mechanizmy związane z bezpieczeństwem sieci: • Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji • Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością: o dynamicznego przypisania użytkownika do określonej sieci VLAN o dynamicznego przypisania listy ACL • Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X • Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC • Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X • Możliwość szyfrowania ruchu zgodnie z IEEE 802.1ae (MACSec) dla wszystkich portów przełącznika kluczami o długości 128-bitów (gcm-aes-128) • Możliwość uwierzytelniania wielu użytkowników na jednym porcie • Obsługa funkcji Port Security, DHCP Snooping, DHCP Secured ARP/ARP Validation • Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+ • Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 o Adres MAC źródłowy i docelowy plus maska o Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6 o Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd. o Numery portów źródłowych i docelowych TCP, UDP o Zakresy portów źródłowych i docelowych TCP, UDP o Identyfikator sieci VLAN - VLAN ID o Flagi TCP o Obsługa fragmentów • Wbudowana obrona procesora urządzenia przed atakami DoS. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania • Funkcja Private VLAN •. Bezpieczeństwo MAC adresów o ograniczenie liczby MAC adresów na porcie o zatrzaśnięcie MAC adresu na porcie o możliwość wpisania statycznych MAC adresów na port/vlan

			• Możliwość wyłączenia MAC learning • Sprzętowa obsługa sFlow lub NetFlow Mechanizmy związane z zapewnieniem jakości usług w sieci: • Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi • Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) • Kontrola sztormów dla ruchu broadcast/multicast/unicast • Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP Obsługa protokołów i mechanizmów routingu: • Routing statyczny dla IPv4 i IPv6 • Routing dynamiczny – RIP Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN Zarządzanie: • Port konsoli • Dedykowany port Ethernet do zarządzania out-of-band • Obsługa protokołów SNMPv3, SSHv2, SCP, https • Obsługa SYSLOG z możliwością definiowania wielu serwerów • Port USB umożliwiający podłączenie zewnętrznego nośnika danych. • Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie Obsługa RMON min. 4 grupy: Statistics, History, Alarms, Events (RFC 1757) • Ping dla IPv4 / IPv6 • Traceroute dla IPv4 / IPv6 • Obsługa funkcji TCL/Tk w skryptach CLI • Możliwość uruchamiania skryptów ręcznie o określonym czasie lub co wskazany okres czasu na podstawie wpisów w logu systemowym • Możliwość uruchamianiai skyptów i ACL bezpośrednio na urządzeniu Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU
12	**Switch SAN Typ1**	4	Przełącznik FC musi być wykonany w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8 Gb/s z funkcją autonegocjacji prędkości. Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”. Przełącznik FC musi posiadać zasilacz umożliwiający podłączenie do jednofazowego źródła zasilania AC ~230V, 50Hz zgodnego z PN-IEC 60038 Przełącznik FC musi posiadać minimum 24 sloty na moduły FC. Wymaga się, aby przełącznik został dostarczony z co najmniej 12 portami aktywnymi. Wszystkie wymagane funkcje muszą być dostępne dla minimum 12 portów FC przełącznika. Wszystkie aktywne porty muszą być obsadzone modułami SFP 16Gb/s SR. Rodzaj obsługiwanych portów: E_Port, F_Port, N_Port, M_Port, D_Port lub E/TE, F, NP, SPAN Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10km. Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów. Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych. Zsumowana przepustowość przełącznika FC musi wynosić minimum 384 Gb/s ("end-to-end" w trybie full duplex) Możliwość agregacji połączeń pomiędzy przełącznikami (trunking) na poziomie poszczególnych ramek. Wymagana możliwość utworzenia pojedynczego połączenia „trunk” zbudowanego z minimum ośmiu portów o prędkości 8Gb/s lub z minimum ośmiu portów o prędkości 16Gb/s. Licencja umożliwiająca wykorzystanie tej funkcjonalności nie jest wymagana.

			Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk" oraz obsługiwać grupy połączeń „trunk" o różnych długościach. Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów. Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID. Możliwość wymiany w trybie „na gorąco": minimum w odniesieniu do modułów portów Fibre Channel (SFP). Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika. Przełącznik FC musi umożliwiać wprowadzenie ograniczenia prędkości dla danych wchodzących dla dowolnego portu lub portów. Musi być możliwość określenia limitów niższych niż wynegocjowana prędkość portu. Licencja umożliwiająca wykorzystanie tej funkcjonalności nie jest obecnie przedmiotem oferty. Przełącznik FC musi umożliwiać kategoryzację ruchu między inicjatorem i targetem oraz przydzieleniem takiej pary urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziały do różnych klas priorytetów musi być konfigurowana za pomocą standardowych narzędzi do konfiguracji zoningu. Licencja umożliwiająca wykorzystanie tej funkcjonalności nie jest obecnie przedmiotem oferty. Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN. Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa: - Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric - Możliwość uwierzytelnienia (ang. authentication) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP - Możliwość uwierzytelnienia (ang. authentication) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP - Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów - Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, - Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric. - Konta użytkowników definiowane w środowisku RADIUS lub LDAP - Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS - Obsługa SNMP v1/v3 Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym lub dedykowaną aplikację z interfejsem graficznym dostępnym przez przeglądarkę internetową. Przełącznik FC musi być wyposażone w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC: - logowanie zdarzeń poprzez mechanizm „syslog", - monitorowanie połączeń, i „trunków" Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP" Do każdego dostarczonego modułu SFP 16Gb/s SR musi być dostarczony kabel światłowodowy LC-LC o długości minimum 5 metrów
OPROGRAMOWANIE			
13	**Backup Typ1**	1	Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu

			prostego odtworzenia systemu po całkowitej reinstalacji Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych, które taką funkcjonalność oferują 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 i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp Oprogramowanie musi posiadać wsparcie dla środowisk HCI przynajmniej dla VMware vSAN. Oprogramowanie musi wspierać kopiowanie backupów na urządzenia taśmowe Oprogramowanie musi posiadać wsparcie dla NDMP Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC. Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC. Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn Oprogramowanie musi mieć możliwość kopiowania backupów z wykorzystaniem wbudowanej akceleracji WAN lub wykorzystania mechanizmów zawartych w rozwiązaniach deduplikacyjnych pozwalających na efektywna duplikację danych przesyłając jedynie unikalne bloki do repliki Oprogramowanie musi oferować możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing) Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio z repozytorium backupowego bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana przynajmniej dla środowisk VMware Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji. Oprogramowanie musi wspierać granularne odtwarzanie obiektów i atrybutów Active Directory Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowsze włączając bazy danych z opcją odtwarzania point-in-time Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i

			nowsze. Opcja odtworzenia elementów, witryn, uprawnień. 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. Oprogramowanie musi pozwalać na zaprezentowanie baz MS SQL bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
14	**Wirtualizator Typ1**	1	Oprogramowanie musi być licencjonowane na minimum trzy fizyczne serwery, z których każdy jest wyposażony maksymalnie do dwóch procesorów. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej. Pojedynczy klaster może się skalować do 96 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w sumie w 768 logicznych wątków oraz do 24TB pamięci fizycznej RAM. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-768 procesorowych. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 24 TB pamięci operacyjnej RAM. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM. Rozwiązanie musi wspierać wirtualizację następujących systemów operacyjnych: Windows 2008/2012/2016/2019, Windows 7/8/10, SLES 11/12/15, RHEL 6/7/8, Oracle Linux 6/7/8, Solaris 10/11, Debian 8/9/10, CentOS 8, Ubuntu 18/19/20, Mac OS 10/11. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy. Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania jako wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance. Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

			Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory w zakresie centralnego uwierzytelnienia. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn. System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów. Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej. Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN). Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
15	**System operacyjny Typ1**	4	Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi być przypisane do każdego rdzenia wszystkich procesorów fizycznych w serwerze lub do każdego procesora fizycznego w serwerze, gdzie sumaryczna liczba fizycznych rdzeni procesora/procesorów nie będzie nie większa niż 16. Licencja musi uprawniać do uruchamiania wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. 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. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. Graficzny interfejs użytkownika. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek,

			urządzeń sieciowych, standardów USB, Plug&Play). Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management). Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: - Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC. - 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. - Zdalna dystrybucja oprogramowania na stacje robocze. - Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej. - PKI (Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: - Dystrybucję certyfikatów poprzez http, - Konsolidację CA dla wielu lasów domeny, - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. - Szyfrowanie plików i folderów. - Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). - Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. - Serwis udostępniania stron WWW. - Wsparcie dla protokołu IP w wersji 6 (IPv6). - Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath). Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. Wymagana najnowsza dostępna wersja na dzień publikacji ogłoszenia o zamówieniu. a) Zamawiający nie dopuszcza dostawy licencji typu OEM. b) Zamawiający wymaga dostawy licencji wieczystych. Licencje muszą być fabrycznie nowe, nieużywane, nigdy wcześniej nieaktywowane. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.
16	**Licencja dostępowa na urządzenie**	200	Licencja dostępowa dla urządzenia umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera Microsoft Windows Server (System operacyjny Typ1) typu Dev Cal z wdrożoną rolą Active Directory. Licencje muszą być fabrycznie nowe, nieużywane, nigdy wcześniej nieaktywowane. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u

			Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.
17	**Licencja dostępowa zdalna**	15	Licencja Windows Server RDS DEVICE na urządzenie, przyznająca dla jednego urządzenia prawo dostępu dla sesji usług pulpitu zdalnego do serwera Microsoft Windows Server (System operacyjny Typ1). Licencje muszą być fabrycznie nowe, nieużywane, nigdy wcześniej nieaktywowane. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.