1. Serwery:

L.P	Parametr	Charakterystyka (wymagania minimalne)
1.	**Ilość sztuk**	2
2.	**Obudowa**	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych.
3.	**Procesor**	Architektura x86, maksymalny TDP dla procesora – 130W. Minimalna ilość rdzeni dla procesora – 8. Minimalna prędkość 3.2GHz bez trybu turbo. Wynik wydajności procesora instalowanego w oferowanym serwerze nie powinien być niższy niż 111 punków base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów. Dopuszczalne jest przeprowadzenie testu dla ww. procesora na serwerze tego samego producenta ale innego typu.
4.	**Liczba procesorów**	Min. 2
5.	**Płyta główna**	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje AMD64 lub EM64T (np. AMD Opteron albo Intel Xeon).
6.	**Pamięć operacyjna**	Zainstalowane minimum 256 GB pamięci RAM o częstotliwości 2933MHz w kościach 32GB. Minimum 16 slotów na pamięć. Mozliwość rozbudowy do 1TB RAM.
7.	**Zabezpieczenie pamięci**	memory mirroring, demand scrubing, patrol scrubing, memory rank sparing, ECC, SDDC, ADDDC.
8.	**Procesor Graficzny**	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu serwera. Wymagana możliwość instalacji portu VGA na panelu przednim.
9.	**Rozbudowa dysków**	W chwili dostawy każdy serwer musi posiadać zainstalowane minimum 2 dyski SAS 300GB 10k 2.5”
10.	**Kontroler dyskowy**	Sprzętowy z pamięcią 2GB cache pozwalający na udostępnienie wszystkich zainstalowanych dysków w trybie JBOD oraz RAID 0,1,10,5,50. Pamięć zabezpieczona nośnikiem trwałym (flash).
11.	**Zasilacz**	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Platinum.
12.	**Interfejsy sieciowe**	Zintegrowane 2porty 1Gb RJ45. Dodatkowe 2 porty 10Gb SFP+. Interfejsy te nie mogą wpływać na ilość dostępnych slotów PCIe wymienionych w punkcie Dodatkowe porty I/O. Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. Dodatkowe adapter z dwoma portami 10GbE SFP+ pod PCIe Dostarczone min. 8 wkładek SFP+ SR oraz 8 kabli LC-LC OM3 5m – (po 4 na serwer).
13.	**Dodatkowe sloty I/O**	Serwer powinien umożliwiać instalacje min 2 kart PCIe.
14.	**Dodatkowe porty**	• z przodu obudowy: 1x USB 3.0, 1x USB 2.0, opcjonalny port VGA. • z tyłu obudowy: 2x USB 3.0, , 1x VGA .
15.	**Chłodzenie**	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1.
16.	**Zarządzanie**	Zdalne zarządzanie serwerem, udostępniania zdalnej konsoli graficznej i podłączania zdalnych napędów. Możliwość podstawowego monitoringu serwera za pomocą telefonu z dedykowaną aplikacją producenta serwera działającą w systemie Android lub iOS podłączonego do portu USB.
17.	**Funkcje zabezpieczeń**	Hasło włączania, hasło administratora, moduł TPM. Wymagana możliwość zainstalowania przedniego panelu zabezpieczającego zamykanego na klucz.

18.	**Urządzenia hot swap**	Dyski twarde, zasilacze, wentylatory.
19.	**Obsługa**	Możliwość instalacji serwera oraz wymiany procesora, radiatora oraz tzw. Backplane'y dysków twardych do celów serwisowych bez użycia dodatkowych narzędzi mechanicznych.
20.	**Diagnostyka**	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.
21.	**Systemy operacyjne**	Wsparcie dla systemów VMware, Microsoft Windows Server, SUSE Linux, Redhat Linux (minimum w najnowszej i poprzedniej wersji systemu) Dołączona licencja na oprogramowanie Microsoft Windows 2019 Datacenter na wszystkie oferowane serwery i obejmująca wszystkie procesory i ich rdzenie Dołączona licencja na oprogramowanie VMware vSphere 6 Essentials Plus na wszystkie oferowane serwery wraz z 5 letnim suportem.
22.	**Waga**	Maximum: 17kg
23.	**Wymagania środowiskowe**	Serwer musi umożliwiać pracę w zakresie temperatur 5-45 st C. Klasa Ashrae 3 i 4.
24.	**Gwarancja**	60 miesięcy gwarancji producenta (zakres 9x5, czas reakcji onsite na następny dzień roboczy). Serwis świadczony bezpośrednio przez producenta sprzętu. Możliwość rozszerzenia serwisu o wyższe poziomy wsparcia – 24h gwarantowany czas naprawy lub lepszy – również jako serwis producenta.
25.	**Inne**	Oferent musi posiadać autoryzację producenta do sprzedaży oferowanego serwera której potwierdzenie należy dołączyć do oferty. Wymagane jest również dołączenie do oferty oświadczenia producenta lub autoryzowanego dystrybutora o gotowości świadczenia serwisu na rzecz Zamawiającego dla wszystkich zaoferowanych podzespołów przez cały okres gwarancji.

2. Macierz SAN:

L.P.	Parametr	Charakterystyka (wymagania minimalne)
1.	**Obudowa**	Macierz musi mieć możliwość zainstalowania w standardowej szafie rack 19" nie będącej przedmiotem zamówienia. Rozmiar jednostki sterującej macierzą nie może przekraczać 2U . Dodawanie kolejnych półek lub dysków musi odbywać się bezprzerwowo. Wymagana możliwość podłączenia polki mieszczącej minimum 50 dysków LFF.
2.	**Kontrolery**	Wymagane dwa moduły sterujące macierzą pracujące w trybie active-active. W przypadku wystąpienia awarii sprawny moduł musi automatycznie przejąć obsługę wszystkich zasobów prezentowanych przez macierz.
3.	**Dostępne porty**	Oferowana macierz musi posiadać w chwili dostawy minimum 12 portów powalających na podłączenie do infrastruktury 10Gb iSCSI z wykorzystaniem kabli DAC lub z wykorzystaniem wkładek SFP+. Te same porty musza umożliwiać podłączenie do infrastruktury FC 16Gbs. Macierz powinna także umożliwiać bezpośrednie (bez wykorzystania przełączników) podłączenie do 6 hostow w sposób redundantny (każdy host podłączony do dwóch kontrolerów macierzy) z wykorzystaniem protokółu FC. Wraz z macierzą muszą być dostarczone uniwersalne wkładki SFP+ pozwalające na podłączenie 10Gb ISCSi/16Gb FC (minimum 8szt) oraz kable 3m LC-LC OM3 (minimum 8szt).
4.	**Cache**	Każdy z modułów sterujących musi być wyposażony w min 8 GB pamięci cache zabezpieczonej mechanizmem mirroringu. Pamięć podręczna musi być zabezpieczona przed utratą danych w przypadku zaniku zasilania.
5.	**Dyski**	Macierz musi obsługiwać dyski twarde typu NL-SAS, SAS i SSD oraz umożliwiać instalację różnych typów dysków w ramach jednej półki dyskowej.

		Macierz musi być wyposażona w minimum 2 dyski 800GB SAS SSD hot-plug o wartości dwpd minimum 3 oraz 12 dysków SAS 1.8TB 10K Macierz musi umożliwiać obsługę minimum 192 dysków LFF lub SFF.
6.	**Funkcjonalność**	Macierz musi obsługiwać typy protekcji RAID 0,1,5,6,10 oraz powinna posiadać funkcjonalność zarządzania informacjami o parzystości oraz dyskami spare w całej puli dysków. (w przypadki awarii dysku, do jego obudowy musi być używany każdy dysk z puli) Macierz musi posiadać funkcjonalność rozszerzenia cache na potrzeby procesów odczytu danych (read cache) do 4TB pojemności. Macierz musi umożliwiać zwiększanie online pojemności poszczególnych wolumenów logicznych oraz dynamiczne alokowanie przestrzeni dyskowej (tzw. „*thin provisioning*"). Wymagana możliwość wykonania minimum 128 kopii migawkowych wolumenów z możliwością rozszerzenia tej funkcjonalności do 512 kopii. Macierz musi mieć możliwość replikacji synchronicznej poprzez siec FC oraz asynchronicznej z wykorzystaniem iSCSI lub FC. Wymagana możliwość definiowania globalnych dysków hot-spare. Macierz musi umożliwiać szyfrowanie zapisywanych na niej danych. Nie wymaga się tej funkcjonalności w chwili dostawy.
7.	**Wydajność**	Obsługa minimum 512 logicznych wolumenów o rozmiarze do 2PB Możliwość obsługi minimum 192 hostów LFF.
8.	**Zarządzanie macierzą**	Dostępne dwa porty 1Gbe Base-T w trybie primary/redundant. Zarządzanie macierzą powinno być możliwe za pomocą graficznego interfejsu użytkownika dostępnego poprzez protokół https, oraz za pomocą linii komend cli osiągalnej poprzez protokół ssh. Macierz musi posiadać automatyczny monitoring z możliwością informowania o awariach poprzez protokół smtp oraz snmp oraz możliwość wysyłania powiadomień awarii do wskazanych odbiorców. Wymagana możliwość autentykacji poprzez LDAP oraz funkcjonalność role-based access control. Producent powinien udostępniać konsolę umożliwiającą dodawanie do domeny zarządzania wielu macierzy jednocześnie
9.	**Inne**	Wymagana jest bezprzerwowa wymiana następujących elementów macierzy: kontrolery, moduły I/O, dyski, zasilacze oraz moduły SFP+. Obsługa systemów operacyjnych hosta: Microsoft Windows Server 2012 R2; 2016, 2019; Red Hat Enterprise Linux (RHEL) 6, 7; SUSE Linux Enterprise Server (SLES) 11, 12, 15; VMware vSphere 6.0, 6.5, 6.7.
10.	**Gwarancja**	Co najmniej 5 letnia gwarancja producenta (zakres 9x5, czas reakcji onsite na następny dzień roboczy), serwis w miejscu instalacji sprzętu świadczony przez producenta macierzy lub autoryzowanego partnera serwisowego.
11.	**Inne**	Oferent musi posiadać autoryzację producenta do sprzedaży oferowanego serwera której potwierdzenie należy dołączyć do oferty. Wymagane jest również dołączenie do oferty oświadczenia producenta lub autoryzowanego dystrybutora o gotowości świadczenia serwisu na rzecz Zamawiającego dla wszystkich zaoferowanych podzespołów przez cały okres gwarancji.

3. Macierz NAS

L.P.	Parametr	Charakterystyka (wymagania minimalne)
1.	**Procesor**	Minimum AMD Ryzen 5
2.	**Architektura procesora**	64-bit x86
3.	**Procesor liczba rdzeni**	Nie mniej niż 6
4.	**Częstotliwość taktowania**	Minimum 3.4 GHz
5.	**Pamięć RAM**	Nie mniej niż 16GB DDR4
6.	**Pamięć RAM liczba slotów**	Minimum 4 sloty
7.	**Pamięć RAM - możliwość rozszerzenia**	nie mniej niż do 64GB
8.	**Pamięć Flash**	Nie mniej niż 5 GB
9.	**Liczba zatok na dyski twarde**	Minimum 8
10.	**Obsługiwane dyski twarde**	3.5" SATA oraz 2.5" SATA / SSD SATA
11.	**Pojemność dysków twardych jakie można stosować**	do 16 TB
12.	**Możliwość podłączenia modułu rozszerzającego**	Tak, do 8
13.	**Porty LAN**	Minimum 2 x 1 Gb/s Ethernet oraz 2 x 10 Gb/s SFP+
14.	**Diody LED**	HDD 1–8, stan, LAN, stan gniazda rozszerzenia pamięci masowej
15.	**Porty USB 3.2 Gen1**	4
16.	**Porty USB 3.2 Gen 2 (10 Gb/s)**	1 x typ C USB 3.1 Gen2 5V/3A 10 Gb/s 1 x typ A USB 3.1 Gen2 5V/1A 10 Gb/s
17.	**Przyciski**	Reset, Zasilanie
18.	**Typ obudowy, montaż**	RACK, 2U wraz z szynami montażowymi do szafy RACK
19.	**Dopuszczalna temperatura pracy**	od 0 do 40˚C
20.	**Wilgotność względna podczas pracy**	5-95% R.H.
21.	**Zasilanie**	Redundantne 2 x 300 W , 100–240 V
22.	**Wysyłanie / odbieranie w systemie Windows**	min. 1300 (MB/s) / 1600 (MB/s) (przy agregacji 2 łączy 10 Gb/s i transferze pliku 10 GB)
23.	**Wysyłanie / odbieranie w systemie Windows(Robocopy) - z wykorzystaniem szyfrowania AES 256bit**	min. 1300 (MB/s) / 1600 (MB/s) (przy agregacji 2 łączy 10 Gb/s i transferze pliku 10 GB)
24.	**Agregacja łączy**	Tak
25.	**Obsługiwane systemy plików**	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+

26.	**Możliwość podłączenia karty WLAN na USB**	Tak
27.	**Łączenie usług z interfejsem**	Tak
28.	**Szyfrowanie wolumenów**	Tak, min AES 256
29.	**Szyfrowanie dysków zewnętrznych**	Tak
30.	**Zarządzanie dyskami**	Pojedynczy Dysk, RAID 0,1, 5,50, 6, 60, 10, 5+Hot Spare, 6+Hot Spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Globalny Hot Spare, Pula pamięci masowej Mechanizm automatycznego pozycjonowania danych w zależności od częstotliwości wykorzystania SSD over provisioning Funkcjonalność migawek dla woluminów oraz LUN, wraz z możliwością ich replikacji na drugie urządzenie Obsługa SSD cache w trybach read i write
31.	**Wbudowana obsługa iSCSI**	Multi-LUNs na Target Minimum do 256 LUNs Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN
32.	**Zarządzanie prawami dostępu**	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
33.	**Obsługa Windows AD**	Logowanie użytkowników do domeny poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Obsługa uwierzytelniania NTLMv2, Funkcja serwera LDAP
34.	**Funkcje backup**	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, serwer Apple Time Machine, backup na zewnętrzne dyski twarde.
35.	**Współpraca z zewnętrznymi dostawcami usług chmury**	Przynajmniej: Amazon S3, Amazon Glacier, Microsoft Azure, Google Cloud Storage, Dropbox,
36.	**Darmowe aplikacje na urządzenia mobilne**	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android
37.	**Minimum obsługiwane serwery**	Serwer plików Serwer FTP Serwer WEB Serwer baz danych MySQL Serwer kopii zapasowych Serwer iTunes Serwer multimediów UPnP

		Serwer wydruku Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu (opcja podłączenia 8 kamer IP w ramach wbudowanej licencji z możliwością podłączenia dodatkowych po dokupieniu licencji)
38.	**VPN**	VPN client / VPN server. Obsługa PPTP, OpenVPN
39.	**Administracja systemu**	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania ręczna Możliwość aktualizacji oprogramowania z powiadomieniem z serwerów producenta Ustawienia: Back up, przywracania, resetowania systemu
40.	**Wirtualizacja**	Możliwość uruchomienia maszyn wirtualnych z systemem Windows, Linux, Unix i Android; import maszyn wirtualnych z systemów VirtualBox, Vmware Workstation; VM clone, VM snapshot; pass-throug dla USB;
41.	**Zabezpieczenia**	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP (tylko admin) Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS
42.	**Możliwość instalacji dodatkowego oprogramowania**	Tak, sklep z aplikacjami; możliwość instalacji z paczek oraz wbudowane narzędzia wirtualizacji umożliwiające zarówno obsługę kontenerów Docker/LXC jak i pełnych maszyn wirtualnych
43.	**Współpraca z środowiskami wirtualnymi**	VMware vSphere, Citrix XenServer , Hyper-V, PlugIn dla vSphere, Windows Server 2016 , obsługa Vmware VAAI dla iSCSI
44.	**Gwarancja**	Minimum 5 lat
45.	**Dyski**	Wraz z macierzą należy dostarczyć 8 dysków o pojemności 8TB, 3,5 cala SATA 600, 7200RPM, 256MB Cache. Dyski te muszą być dedykowane przez producenta do pracy w macierzach typu NAS.
46.	**Inne**	Wraz z ofertą należy dostarczyć oświadczenie producenta lub autoryzowanego dystrybutora o: 1. autoryzacji do sprzedaży 2. że sprzęt będzie pochodził z oficjalnego Polskiego kanału dystrybucji i nie jest częścią żadnego innego projektu 3. gotowości świadczenia wsparcia i realizacji gwarancji przez wymagany okres. Oświadczenia te nie są wymagane dla dysków twardych.

4. Oprogramowanie do tworzenia kopii zapasowych:

I. Wymagania minimalne:

1. Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji:
   a) AWS EC2
   b) Microsoft Hyper-V min. w wersjach 2019, 2016, 2012R2, 2012
   c) VMware vSphere min. w wersjach v4.1-6.7
   d) Nutanix AHV 5.10 (LTS)
   e) Maszyny fizyczne: Windows Server 2019, 2016, 2012R2, 2012, 2008R2
2. Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V, oraz AWS EC2
3. Oprogramowanie musi pozwalać na wdrożenie w środowiskach:
   a) Na serwerze sprzętowym, obsługiwane systemy operacyjne w ramach: Windows Server 2008 R2 – 2019 (x64), Windows 7 – 10 Professional (x64), Ubuntu 16.04 – 18.04 Server (x64), Red Hat Enterprise Linux 6.3 – 7.5 (x64), SUSE Linux Enterprise Server 11 SP3 – 12 SP3 (x64).
   b) Jako maszyna wirtualna Vmware.
   c) Jako maszyna wirtualna Amazon,
   d) Na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4. Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS.
5. Oprogramowanie nie może wymagać instalacji jakiegokolwiek agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania.
6. Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji (np. Frameworków czy baz danych).

II. Licencjonowanie

1. Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariancie wieczystym, w którym licencja nie ma terminu ważności.
2. Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska.
3. W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 5 lat wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania. Wraz z ofertą należy dostarczyć oświadczenie producenta lub autoryzowanego dystrybutora o gotowości świadczenia takiego wsparcia.
4. W ramach dostawy wymagane jest dostarczenie licencji na ochronę 4 gniazd procesorów w hostach VMware.
5. Licencjonowanie innych środowisk może być realizowane na zasadzie subskrypcji wymagającej zakupu dedykowanej licencji dla środowiska

III. Ochrona danych

1. Oprogramowanie musi posiadać funkcje backupu i replikacji:
   a) Backup maszyn wirtualnych VMware.

b) Replikacja maszyn wirtualnych VMware (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu.
c) Backup maszyn wirtualnych Hyper-V.
d) Replikacja maszyn wirtualnych Hyper-V (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu.
e) Backup instancji AWS EC2.
f) Replikacja instancji AWS EC2 (tworzenie I aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych).
g) Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych.
h) Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie.
i) Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu.
j) Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym.
k) Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych. Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
l) Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania

IV. Optymalizacja wykorzystania miejsca na dane

1. Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
   a) Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane.
   b) Kompresja backupu, w tym konfigurowalny stopień kompresji.
   c) Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne.

V. Spójność danych

1. Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
   a) Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux.
   b) Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu.
   c) Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:
      - Microsoft Exchange 2007 – 2016
      - Microsoft SQL 2008 – 2017
   d) Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki.
   e) Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
   f) Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania.
   g) Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji.

VI. Przywracanie danych

1. Oprogramowanie musi posiadać poniższe funkcje:
   a) Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji.

b) Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej) oraz możliwość jej migracji do serwera produkcyjnego.
c) Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej).
d) Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
   - Microsoft Exchange
   - Active Directory
   - MS SQL
e) Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.

VII. Wydajność

1. Oprogramowanie do backupu musi pozwalać na:
   a) Tworzenie backupu I replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT.
   b) Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych.
   c) Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN.
   d) Akceleracją sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci.
   e) Wsparcie dla urządzeń oferujących dodatkową deduplikację danych.

VIII. Zarządzanie

1. Oprogramowanie musi pozwalać na następujące formy zarządzania:
   a) Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych.
   b) Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
   c) Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania.
   d) Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
   e) Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji.

5. Usługi - Instalacja, konfiguracja i wdrożenie systemu klastra wraz z macierzą dyskową, systemem backupowym i oprogramowaniem.

Zakres wdrożenia obejmuje

- instalacja nowych serwerów i macierzy (SAN oraz NAS) wraz z konfiguracją.
- instalacja vmware vSphere wraz z konfiguracją oraz utworzenie klastra wysokiej dostępności.
- przeniesienie obecnego środowiska zamawiającego na vSphere (srodowiisko oparte o serwery fizyczne, hypervisory hyperv oraz cytrix).
- podniesienie poziomu funkcjonalności domeny do 2019.
- instalacja i konfiguracja zapasowego kontrolera domeny .
- analiza obecnego środowiska domenowego i wprowadzenie poprawek (dodatkowe OU, polityki GPO, dodatkowe role (printserwer, fileserwer, WSUS, CA).

- integracja nowych zasobów z AD.
- wdrożenie systemu backupu dla całego środowiska wraz z automatycznym testowaniem kopii zapasowych.

6. Urządzenia sieciowe

Przedmiotem zamówienia jest dostarczanie sprzętu sieciowego wraz z niezbędnym oprogramowaniem i usługami zgodnie ze specyfikacją.
Przedmiot zamówienia składa się z:

6.1 Usługa wdrożenia i wsparcia technicznego
6.2 Przełącznik szkieletowy – szt. 2
6.3 Przełącznik dostępowy – szt. 4
6.4 Oprogramowanie zarządzające – szt. 1
6.5 Moduły optyczne SFP+ - szt. 14
6.6 Moduły optyczne SFP - szt. 6

6.1 Wymagania w zakresie realizacji dostawy, gwarancji, usług wdrożenia i wsparcia technicznego

Całość przedmiotu zamówienia należy zrealizować w ciągu 60 dni.

W ramach realizacji zamówienia należy wykonać wdrożenie oferowanych urządzeń i systemu zarządzania w siedzibie Zamawiającego. W ramach wdrożenia należy: wykonać instalację sytemu zarządzania, konfigurację połączeń sieciowych na przełącznikach oraz stosy, konfigurację polityk dostępowych i innych zgodnych z SIWZ. Wymagane jest również wykonanie integracji z posiadanymi przez Zamawiającego urządzeniami Fortinet na poziomie automatycznej dystrybucji zautoryzowanych użytkowników przez oferowany system zarządzania do firewalla brzegowego oraz podejmowanie automatycznej reakcji na zaistniałe incydenty. Integrację taką musi wykonać inżynier z ważnym certyfikatem Fortinet Security Expert 8 (należy dołączyć go do oferty).

Po wykonaniu wdrożenia należy świadczyć na rzecz Zamawiającego wsparcie techniczne do oferowanych rozwiązań przez okres jednego roku. W tym celu wykonawca musi posiadać co najmniej dwóch inżynierów posiadających aktualny certyfikat techniczny (lub certyfikaty) wystawione przez producenta oferowanych urządzeń sieciowych i systemu zarządzania potwierdzające wiedzę z ich zakresu. Certyfikaty te należy dołączyć do oferty. Jeżeli producent oferowanych rozwiązań stosuje certyfikację serwisową to wykonawca zobowiązany jest do jej posiadania z możlliwością weryfikacji tego faktu na stronie producenta.

Zaoferowane przełączniki sieciowe muszą posiadać ograniczoną dożywotnią gwarancję uprawniającą do naprawy w razie awarii oraz możliwość aktualizacji oprogramowania przez okres co najmniej 5 lat od ich dostawy. Przez pierwszy rok wymagane jest również wsparcie techniczne w pełnym zakresie funkcjonalnym.

Licencja na zaoferowane oprogramowanie musi być dożywotnia wraz z rocznym wsparciem technicznym i aktualizacjami. Musi być zapewniona możliwość przedłużenia tego wsparcia na kolejne lata.

Zamawiający wymaga, by dostarczone urządzenia były nowe oraz by były nieużywane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym Wykonawca jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego

rozpakowaniem). Całość sprzętu i oprogramowania musi pochodzić o jednego producenta z wyłączeniem modułów optycznych.

6.2 Przełącznik szkieletowy – szt. 2

1. Przełącznik posiadający 10 portów 10Gigabit Ethernet SFP+, mogących pracować z prędkością 100 MB, 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+
2. Wysokość urządzenia 1U
3. Nieblokująca architektura o wydajności przełączania min. 200 Gb/s
4. Szybkość przełączania min. 148 Milionów pakietów na sekundę
5. Możliwość łączenia do 8 przełączników w stos za pomocą portów 10G
6. Tablica MAC adresów min. 16k
7. Pamięć operacyjna: min. 1 GB pamięci DRAM
8. Pamięć flash: min. 4 GB pamięci Flash
9. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
10. Obsługa sieci wirtualnych protokołowych IEEE 802.1v
11. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
12. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
13. Obsługa Q-in-Q IEEE 802.1ad
14. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
15. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
16. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
17. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
18. Wbudowany DHCP Serwer i klient
19. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
20. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
21. Możliwość monitorowania zajętości CPU
22. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
23. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
24. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
25. Obsługa CDPv2

Obsługa Routingu IPv4

26. Sprzętowa obsługa routingu IPv4 – forwarding
27. Routing statyczny
28. Obsługa routingu dynamicznego IPv4
    a. RIPv1/v2
    b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

Obsługa Routingu IPv6

29. Sprzętowa obsługa routingu IPv6 – forwarding
30. Routing statyczny
31. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
32. Telnet Serwer/Klient dla IPv6
33. SSH2 Serwer/Klient dla IPv6
34. Ping dla IPv6
35. Tracert dla IPv6
36. Obsługa MLDv1 (Multicast Listener Discovery version 1)

Obsługa Multicastów

37. Filtrowanie IGMP
38. Obsługa Multicast VLAN Registration - MVR
39. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo

40. Obsługa Network Login
    a. IEEE 802.1x - RFC 3580
    b. Web-based Network Login
    c. MAC based Network Login
41. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
42. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
43. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
44. Obsługa Guest VLAN dla IEEE 802.1x
45. Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
46. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
47. Obsługa Identity Management
48. Wbudowana obrona procesora urządzenia przed atakami DoS
49. Obsługa TACACS+
50. Obsługa RADIUS Authentication (RFC 2138)
51. Obsługa RADIUS Accounting (RFC 2139)
52. RADIUS and TACACS+ per-command Authentication
53. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
54. Możliwość wyłączenia MAC learning
55. Obsługa SNMPv1/v2/v3
56. Klient SSH2
57. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection

c. Zabezpieczenei CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania

58. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    a. Adres MAC źródłowy i docelowy plus maska
    b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    d. Numery portów źródłowych i docelowych TCP, UDP
    e. Zakresy portów źródłowych i docelowych TCP, UDP
    f. Identyfikator sieci VLAN - VLAN ID
    g. Flagi TCP
    h. Obsługa fragmentów
59. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
60. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI
61. Obsługa bezpiecznego transferu plików SCP/SFTP
62. Obsługa DHCP Option 82
63. Obsługa IP Security - Gratuitous ARP Protection
64. Obsługa IP Security – Trusted DHCP Server
65. Obsługa IP Security – DHCP Secured ARP/ARP Validation
66. Obsługa IP Security – IP Source guard
67. Ograniczanie przepustowości (rate limiting) na portach wyjściowych

Bezpieczeństwo sieciowe

68. Możliwość konfiguracji portu głównego i zapasowego
69. Obsługa redundancji routingu VRRP - RFC 2338
70. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
71. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
72. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
73. Obsługa PVST+
74. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
75. Obsługa G.8032
76. Obsuga Link Aggregation IEEE 802.3ad wraz z LACP - 128 grup po 8 portów
77. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników

Zarządzanie

78. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
79. Obsługa synchronizacji czasu NTP
80. Zarządzanie przez SNMP v1/v2/v3
81. Zarządzanie przez przeglądarkę WWW – protokół http i https
82. Możliwość zarządzania przez protokół XML
83. Możliwość zarządzania przełącznikiem z aplikacji Cloud
84. Możliwość zarzadzania przełącznikiem z dedykowanej aplikacji zarządzającej
85. Możliwość zarzadzania przełącznikiem z poziomu CLI
86. Wsparcie dla Zero-touch provisioning
87. Telnet Serwer/Klient dla IPv4 / IPv6
88. SSH2 Serwer/Klient dla IPv4 / IPv6
89. Ping dla IPv4 / IPv6
90. Traceroute dla IPv4 / IPv6

91. Obsługa SYSLOG z możliwością definiowania wielu serwerów
92. Sprzętowa obsługa sFlow
93. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
94. Obsługa RMON2 (RFC 2021)

Inne

95. Zakres temperatury pracy 0-50 °C
96. Obsługa skryptów CLI
97. Obsługa skryptów w języku Python
98. Obsługa funkcji TCL/Tk w skryptach CLI
99. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
100. Obsługa AVB (Audio Video Bridging) - możliwość rozszerzenia przez licencje
101. Obsługa OpenFlow – możliwość rozszerzenia przez licencje
102. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym

6.3 Przełącznik dostępowy – szt. 4

1. Przełącznik posiadający 24 porty 10/100/1000BASE-T
2. Przełącznik posiadający 8 portów 1GBE SFP
3. Przełącznik posiadający 2 porty 10GBE SFP+ z możliwością rozbudowy o kolejne 2
4. Wysokość urządzenia 1U
5. Nieblokująca architektura o wydajności przełączania min. 128 Gb/s
6. Szybkość przełączania min. 95 Milionów pakietów na sekundę
7. Posiada porty umożliwiające łącznie przełączników w stos. Wydajność połączenia w stos min. 40 Gb/s.
8. Możliwość łączenia do 8 przełączników w stos
9. Tablica MAC adresów min. 16k
10. Pamięć operacyjna: min. 1 GB pamięci DRAM
11. Pamięć flash: min. 4 GB pamięci Flash
12. Bufor pakietów 3MB
13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
14. Obsługa sieci wirtualnych protokołowych IEEE 802.1v
15. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
16. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
17. Obsługa Q-in-Q IEEE 802.1ad
18. Obsługa Quality of Service
    a. IEEE 802.1p
    b. DiffServ
    c. 8 kolejek priorytetów na każdym porcie wyjściowym
19. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
20. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)

21. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
22. Przełącznik musi umożliwiać doposażenie w przyszłości w redundantny system zasilania.
23. Wbudowany DHCP Serwer i klient
24. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
25. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
26. Możliwość monitorowania zajętości CPU
27. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
28. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.
29. Obsługa CDPv2 z obsługą Voice VLAN

Obsługa Routingu IPv4

30. Sprzętowa obsługa routingu IPv4 – forwarding
31. Routing statyczny
32. Obsługa routingu dynamicznego IPv4
    a. RIPv1/v2
    b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania

Obsługa Routingu IPv6

33. Sprzętowa obsługa routingu IPv6 – forwarding
34. Routing statyczny
35. Obsługa routingu dynamicznego dla IPv6
    a. RIPng
    b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
36. Telnet Serwer/Klient dla IPv6
37. SSH2 Serwer/Klient dla IPv6
38. Ping dla IPv6
39. Tracert dla IPv6
40. Obsługa MLDv1 (Multicast Listener Discovery version 1)

Obsługa Multicastów

41. Filtrowanie IGMP
42. Obsługa Multicast VLAN Registration - MVR
43. Obsługa IGMP v1/v2/v3 snooping
44. Obsługa PIM snooping
45. Obsługa PIM-SM - możliwość rozszerzenia przez licencję oprogramowania

Bezpieczeństwo

46. Obsługa Network Login

d. IEEE 802.1x - RFC 3580
e. Web-based Network Login
f. MAC based Network Login

47. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
48. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
49. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
50. Obsługa Guest VLAN dla IEEE 802.1x
51. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
52. Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
53. Obsługa Identity Management
54. Wbudowana obrona procesora urządzenia przed atakami DoS
55. Obsługa TACACS+ (RFC 1492)
56. Obsługa RADIUS Authentication (RFC 2138)
57. Obsługa RADIUS Accounting (RFC 2139)
58. RADIUS and TACACS+ per-command Authentication
59. Bezpieczeństwo MAC adresów
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
60. Możliwość wyłączenia MAC learning
61. Obsługa SNMPv1/v2/v3
62. Klient SSH2
63. Zabezpieczenie przełącznika przed atakami DoS

6.4 Networks Ingress Filtering RFC 2267

6.5 SYN Attack Protection

6.6 Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania

64. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
    a. Adres MAC źródłowy i docelowy plus maska
    b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
    c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
    d. Numery portów źródłowych i docelowych TCP, UDP
    e. Zakresy portów źródłowych i docelowych TCP, UDP
    f. Identyfikator sieci VLAN - VLAN ID
    g. Flagi TCP
    h. Obsługa fragmentów
65. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
66. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania
67. Obsługa bezpiecznego transferu plików SCP/SFTP
68. Obsługa DHCP Option 82
69. Obsługa IP Security - Gratuitous ARP Protection
70. Obsługa IP Security - Trusted DHCP Server
71. Obsługa IP Security - DHCP Snooping
72. Obsługa IP Security - DHCP Secured ARP/ARP Validation
73. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 64 kb/s

Bezpieczeństwo sieciowe

74. Możliwość konfiguracji portu głównego i zapasowego

75. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
76. Obsługa redundancji routingu VRRP na dwóch urządzeniach agregacyjnych pracujących w ramach MLAG w trybie Active-Active (obydwa urządzenia przeprowadzają routing) - możliwość rozszerzenia przez licencję oprogramowania
77. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D
78. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
79. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
80. Obsługa PVST+
81. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
82. Obsługa G.8032 v1/v2
83. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.
84. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.
85. Obsługa LACP w ramach MLAG

Zarządzanie

86. Obsługa synchronizacji czasu NTP
87. Zarządzanie przez SNMP v1/v2/v3
88. Zarządzanie przez przeglądarkę WWW – protokół http i https
89. Możliwość zarządzania poprzez protokół XML
90. Możliwość zarządzania przełącznikiem z aplikacji Cloud
91. Możliwość zarzadzania przełącznikiem z dedykowanej aplikacji zarządzającej
92. Możliwość zarzadzania przełącznikiem z poziomu CLI
93. Wsparcie dla Zero-touch provisioning
94. Telnet Serwer/Klient dla IPv4 / IPv6
95. SSH2 Serwer/Klient dla IPv4 / IPv6
96. Ping dla IPv4 / IPv6
97. Traceroute dla IPv4 / IPv6
98. Obsługa SYSLOG z możliwością definiowania wielu serwerów
99. Sprzętowa obsługa sFlow
100. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
101. Obsługa RMON2 (RFC 2021)

Inne

102. Zakres temperatury pracy 0-50 °C
103. Obsługa skryptów CLI
104. Obsługa skryptów w języku Python
105. Obsługa funkcji TCL/Tk w skryptach CLI
106. Możliwość edycji skyptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
107. Obsługa OpenFlow – możliwość rozszerzenia przez licencje
108. Obsługa AVB (Audio Video Bridging) – możliwość rozszerzenia przez licencje
109. Możliwość uruchamiania skryptów
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym

6.4 Oprogramowanie zarządzające – szt. 1

1. Aplikacja musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera
    a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
    b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.
2. Aplikacja musi zarządzać siecią przewodową i bezprzewodową
3. Aplikacja zarządzająca musi obsługiwać minimum 10 urządzeń (adresów IP)
4. Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników.
5. Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego
6. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
7. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
8. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
9. Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
10. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
12. Aplikacja musi posiadać wbudowaną przeglądarkę SNMP MIB
13. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
14. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
15. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla danych urządzeń sieciowych.
16. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
17. Aplikacja musi posiadać wbudowany Syslog serwer
18. Aplikacja musi posiadać wbudowany BootP serwer
19. Aplikacja musi wspierać protokół IPv4 oraz IPv6
20. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
21. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
22. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
23. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
    a. połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości
    b. stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów
    c. konfiguracji sieci VLAN

    d. konfiguracji protokołu routingu OSPF
24. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https
25. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a. adres IP urządzenia
    b. adresu MAC urządzenia
    c. nazwy urządzenia
    d. wersji oprogramowania
    e. wersji bootrom
    f. lokalizacji urządzenia
    g. danych kontaktowych administratora
    h. numeru seryjnego
26. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
    b. możliwość odtworzenia wskazanej konfiguracji urządzenia
    c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych
    d. możliwość obsługi urządzeń sieciowych różnych producentów
27. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
28. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
29. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp.
31. Tworzona polityka musi zawierać możliwość:
    a. blokowania lub zezwalania ruchu na podstawie
        i. źródłowy i docelowy adres MAC
        ii. źródłowy i docelowy adres IP
        iii. źródłowy i docelowy adres IP podsieci
        iv. źródłowy i docelowy port TCP/UDP
        v. źródłowy i docelowy zakres portów TCP/UDP
        vi. typ protokołu
        vii. pole IP TOS
    b. przydziału parametrów QoS
        i. priorytety
        ii. ograniczenia przepustowości
        iii. przydziału użytkownika do wskazanej sieci VLAN
        iv. przekierowania ruchu do zewnętrznego systemu analizującego pakiety
32. Aplikacja musi mieć możliwość wdrażania polityk bezpieczeństwa w całej sieci, dla urządzeń przewodowych i bezprzewodowych za pomocą jednego kliknięcia.
33. Aplikacja musi pozwalać na łatwą modyfikację i ponowne wdrożenie na wszystkich urządzeniach przewodowych i bezprzewodowych
34. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
    a. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
    b. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
    c. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.

d. generowanie raportów

35. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
    a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
    b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac
    c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
        i. adres IP kontrolera
        ii. liczba obsługiwanych klientów
        iii. szczytowe wartości zajmowanego pasma
        iv. wersja oprogramowania
    d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
        i. adres IP punktu dostępowego
        ii. MAC adres punktu dostępowego
        iii. wersja oprogramowania
        iv. typ punktu dostępowego
        v. kanały pracy poszczególnych interfejsów radiowych
        vi. szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
    e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
        i. adres IP klienta
        ii. MAC adres klienta
        iii. nazwa użytkownika
        iv. nazwa punktu dostępowego, do którego dołączony jest użytkownik
        v. BSSID, do którego dołączony jest użytkownik
        vi. SSID, do którego dołączony jest użytkownik
    f. Musi być zapewniona możliwość tworzenia map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
        i. zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
        ii. zaznaczenie kanałów pracy urządzeń
        iii. lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
36. Aplikacja zarządzająca musi być zintegrowana z systemem zapewniającym widoczność zautoryzowanych klientów w sieci z zapewnieniem widzialności następujących informacji:
    a. adresu MAC
    b. adresu IP
    c. nazwy komputera
    d. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
    e. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
    f. adres IP urządzenia, do którego dołączony jest klient.
    g. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
    h. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
    i. nazwa przydzielonej polityki bezpieczeństwa.
37. System zapewniający widoczność zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.

38. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
39. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List
40. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
41. System zapewniający widoczność zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
    a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
    b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
    c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
    d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
    e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
42. System zapewniający widoczność zautoryzowanych klientów jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 500 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 100 punktów dostępowych oraz min. 10 przełączników sieciowych. System musi umożliwiać w przyszłości rozbudowę do minimum 250 urządzeń sieciowych. System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7.
43. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów, w tym wymagana jest integracja z firewall'ami Fortinet.

6.5 Moduły optyczne SFP+ - szt. 14

Wykonawca musi zaoferować moduły optyczne 10Gb SFP+ dla światłowodów jednomodowych kompatybilne z zaoferowanymi przełącznikami.

6.6 Moduły optyczne SFP - szt. 6

Wykonawca musi zaoferować moduły optyczne 1Gb SFP dla światłowodów jednomodowych kompatybilne z zaoferowanymi przełącznikami.