**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Wstęp**

Wymagania ogólne dla dostarczanego sprzętu i oprogramowania (dotyczy wszystkich systemów opisanych w tym dokumencie):

1. Opisane parametry techniczne są wymaganiami minimalnymi i wykonawca może zaoferować urządzenia o parametrach lepszych niż wymagane,
2. Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
3. Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane,
4. Sprzęt musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczpospolitej Polskiej;
5. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
6. UWAGA! Zamawiający wymaga aby do oferty, jako przedmiotowe środki dowodowe, zostały załączone szczegółowe specyfikacje techniczne wraz z nazwą i modelem proponowanego urządzenia lub karty katalogowe potwierdzające spełnianie wymogów Zamawiającego.

**ZADANIE NR 1 – Dostawa środowiska serwerowo-macierzowego oraz usługa jego instalacji i konfiguracji**

**1. Serwer nr 1 – 1 sztuka:**

|  |  |
| --- | --- |
| Parametry techniczne | Minimalne wymagania |
| Obudowa | Rack 19’’ maks. 2U z możliwością instalacji 16 dysków hot-swap NVMe/SATA/SAS w rozmiarze 2.5”.  Na przednim panelu powinny się znajdować diody syngalizacyjne umożliwiające sprawdzenie statusu wentylatorów/przegrzania, aktywności dysków HDD, statusu połączeń. |
| Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów.  Płyta główna musi być zaprojektowana przez producenta serwera. Płyta musi obsługiwać procesory do 64 rdzeni/128 wątków. I obsługiwać procesory do 350W TDP.  Płyta ma mieć możliwość obsługi kart GPU co najmniej: H100, L40, RTX A6000, RTX A4000, L40S, A40, A16, A100. |
| Procesor | Zainstalowane dwa procesory o parametrach jak poniżej:  Procesor klasy x86, min. 16 rdzeniowy, zaprojektowany do pracy w serwerach, taktowany zegarem co najmniej 4,1 GHz (w trybie turbo), z pamięcią cache L3 co najmniej 37,5 MB.  Zaoferowana konfiguracja dwuprocesorowa musi uzyskiwać w teście SPECrate2017\_int\_base wynik nie mniejszy niż 310 punktów. W przypadku braku wyników dla zaoferowanej konfiguracji Zamawiający zaakceptuje wyniki dla innej konfiguracji dwuprocesorowej danego producenta zbudowanej w oparciu o zaoferowane procesory.  Wydruk z platformy SPECrate2017\_int dla platform oferowanego dostawcy należy dołączyć do oferty.  Zaoferowane procesory muszą umożliwiać migrację działających maszyn wirtualnych w posiadanym przez Zamawiającego środowisku wirtualnym zbudowanym w oparciu o serwery wyposażone w procesory Intel Xeon. |
| Pamięć RAM | Zainstalowane 16 kości ram minimum 32GB, kości minimum DDR5 5600MHz ECC  Musi być możliwość rozbudowy o kolejne 16 kości RAM. |
| Dyski | Zainstalowane minimum 2 dyski o pojemności nie mniejszej niż 480GB SSD SATA, dopuszczalne są nośniki klasy TLC lub lepsze, dyski o parametrach DWPD większe lub równie 1. |
| Kontroler RAID | Zainstalowany sprzętowy kontroler RAID o przepustowości min. 12 Gb/s z obsługą RAID 0, 1, 5, 6, 10, 50, 60 oraz z wsparciem dla trybu JBOD. Kontroler musi być wyposażony w pamięć Cache min. 4GB, z podtrzymaniem bateryjnym. |
| Interfejsy sieciowe | Minimum 2 porty 10GbE SFP+ obsadzone Gbic o prędkości 10Gbit SFP+;  Minimum 2 porty 10GbE Base-T, RJ45; |
| Kontrolery FC | Dwuportowa kart 32Gb/64Gb FC obsadzona wkładkami o prędkości min. 32Gb. |
| Porty | - min. 2 port USB 3.x,  - min. 2 port USD 2.0  - min. 1 port VGA,  - min. 1 port 1 GbE RJ-45 dedykowany do zdalnego zarządzania. |
| Zasilacze | - min 2 zasilacze typu hot-swap 1200 W AC. Certyfikowane jako 80 PLUS Titanium certified. |
| Zarządzanie | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0, SNMP.  Możliwość zdalnego restartu serwera i pełne zarządzanie serwerem poprzez połączenie w sieci TCP/IP przy użyciu przeglądarki internetowej,  Włączanie/wyłączanie serwera, reinstalację systemu operacyjnego, zdalne podłączenie napędów CD/DVD, dysków USB oraz obrazów dysków.  Monitoring oraz zażądanie mocą i jej zużyciem, monitoring sprzętu i usług uruchomionych na serwerze.  Oprogramowanie zarządzające powinno udostępniać wtyczki do używanego przez zamawiającego oprogramowania Vmware. Umożliwiając zarządzanie i monitorowanie serwerów poprzez wtyczkę do klienta Vmware vSphere z przeglądarki wykorzystując HTML5.  Integracja powinna obejmować aktualizację BIOS, firmware i BMC. |
| Wspierane systemy operacyjne | Co najmniej Windows Server 2022, Oracle Linux 9.0, RedHat Enterprise Linux (9.0),  ESXi 8.0, ESXi 7.0 U3. |
| Sloty PCIe | Oferowany serwer powinien pozwalać na instalację łącznie 5 kart PCIe 5.0 o pełnej wysokości.  Oferowana konfiguracja musi posiadać przynajmniej 3 sloty PCIe wolne do późniejszego obsadzenia. |
| Dodatkowe wymagania | Zainstalowany moduł TPM 2.0  Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi posiadać deklaracja CE – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami – wymagane oświadczenie wykonawcy lub producenta;  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022 – wymagane oświadczenie wykonawcy lub producenta;  Elementy, z których zbudowany jest serwer muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz cały musi być objęty gwarancją producenta – wymaganie oświadczenie wykonawcy lub producenta;  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; |
| Gwarancja | min. 24 miesiące gwarancji i serwisu producenta; Oferowany serwis musi zapewniać: wsparcie techniczne w reżimie 5x9, możliwość zgłaszania awarii 24x7.  Serwis musi zapewniać dostawę części i usługę inżyniera w miejscu instalacji sprzętu w trybie NBD.  Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. |
| Oprogramowanie | Wraz z serwerem należy dostarczyć licencję na Windows Server 2022 Datacenter. Ilość licencji zgodna z ilością rdzeni w zaoferowanych procesorach oraz 180 licencji Device Cal, lub oprogramowanie równoważne.  RÓWNOWAŻNOŚĆ:  Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Datacenter.  W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Datacenter, Zamawiający wymaga dostarczenia licencji dla serwerów oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:  1. Współpraca z procesorami o architekturze x86 – 64bit.  2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.  3. Możliwość budowania klastrów składających się z 64 węzłów.  4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.  5. Praca w roli klienta domeny Microsoft Active Directory.  6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.  7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.  8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).  9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.  10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.  11. Możliwość uruchomienia roli serwera stron WWW.  12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.  13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.  14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).  15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).  18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość  19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET  21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  22. Możliwość wykorzystania standardu http/2.  23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.  25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  26. Mechanizmy logowania w oparciu o: a) login i hasło,  a. karty z certyfikatami (smartcard),  b. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).  27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:  a. określonych grup użytkowników,  b. zastosowanej klasyfikacji danych,  c. centralnych polityk dostępu w sieci,  d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.  28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji  w dokumentach (Digital Rights Management).  32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.  b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  • podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  • ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  • odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  • bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,  c. zdalna dystrybucja oprogramowania na stacje robocze,  d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,  e. 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,  • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f. szyfrowanie plików i folderów,  g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,  i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  j. serwis udostępniania stron WWW,  k. wsparcie dla protokołu IP w wersji 6 (IPv6),  l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),  n. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  o. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover  z jednoczesnym zachowaniem pozostałej funkcjonalności.  p. mechanizmy wirtualizacji mające wsparcie dla:  • dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  • obsługi ramek typu jumbo frames dla maszyn wirtualnych.  • obsługi 4-KB sektorów dysków,  • nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  • możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.  q. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.  r. wsparcie dla rozwiązania Kubernetes.  s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz  z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  u. mechanizmy deduplikacji i kompresji na wolumenach.  v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  w. mechanizm konfiguracji połączenia VPN do platformy Azure.  x. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.  y. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.  z. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard). |

**2. Macierz – 1 sztuka:**

1. Macierz musi mieć możliwość zainstalowania w standardowej szafie 19”
2. Macierz musi cechować brak pojedynczego punktu awarii.
3. Macierz musi posiadać dwa redundantne kontrolery pracujące w trybie active-active, wymienialne bez przerywania pracy. Komunikacja pomiędzy parą kontrolerów macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia; nie dopuszcza się komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband oraz zewnętrznych portów macierzy.
4. Wysokość macierzy oraz półek dyskowych nie może być większa niż 2U, za wyjątkiem półek tzw. wysokiej gęstości.
5. Pamięć podręczna macierzy musi być nie mniejsza niż 64 GB (po 32 GB na każdy z kontrolerów).
6. W macierzy wymagane jest nie mniej niż 8 portów Fibre Channel 16 Gb/s w każdym z kontrolerów do połączeń od strony hostów. Macierz powinna posiadać dodatkowo 4 porty 10 GbE z interfejsem RJ45 do komunikacji z hostami poprzez protokół iSCSI. Wymagana jest możliwość wymiany adapterów z portami 16 Gb/s Fibre Channel na adaptery z portami 12 Gb/s SAS, 10 GbE, 25 GbE.
7. Macierz musi wspierać następujące protokoły komunikacji z serwerami: Fibre Channel, iSCSI, SAS.
8. Macierz powinien wpierać zasilanie z dwóch niezależnych źródeł prądu.
9. Macierz musi obsługiwać dyski 2,5” i 3,5” we właściwych obudowach. Macierz musi obsługiwać dyski 2,4 TB 10000 obr/min, dyski 8 TB, 12 TB, 16TB, 20TB 7200 rpm oraz 1,92TB, 3,84TB, 7,68TB, 15,36TB oraz 30,72 TB SSD. Macierz musi zapewniać możliwość używania różnych dysków tego samego typu – odpowiednio 2,5” i 3,5” – w ramach jednej obudowy. Wszystkie obsługiwane dyski muszą wykorzystywać interfejs połączeniowy SAS co najmniej 12 Gb/s oraz każdy powinien posiadać dwa porty SAS. Wymagana obsługa standardu hot-swap.
10. Macierz musi obsługiwać połączenia do półek dyskowych oraz do dysków w standardzie SAS 12 Gb/s.
11. Macierz musi obsługiwać co najmniej 400 dysków, z możliwością rozbudowy do co najmniej 800 dysków w systemie złożonym z dwóch lub więcej macierzy (klaster).
12. Macierz musi zostać wyposażona w minimum 18 dysków 3,84 TB SSD SAS. Macierz musi posiadać pojemność efektywną co najmniej 49 TiB widziane przez serwery, po uwzględnieniu DRAID6 i przestrzeni zapasowej zgodnie z najlepszymi praktykami producenta.
13. Macierz musi obsługiwać poziomy RAID 1, 5 i 6 dystrybuowane lub równoważne z rozdystrybuowaną zarówno przestrzenią zapasową jak i przestrzenią dla właściwego dla RAID poziomu ochrony.
14. Macierz musi wykorzystywać połączenia punkt-punkt do dysków twardych.
15. Macierz musi umożliwiać jednoczesne stosowanie półek dyskowych obsługujących dyski 2,5” oraz 3,5”. Półki dyskowe 2,5” muszą umożliwiać instalację co najmniej 24 napędów dyskowych 2,5”. Półki dyskowe 3,5” muszą umożliwiać instalację co najmniej 12 napędów dyskowych 3,5”. Macierz musi umożliwiać podłączenie półek dyskowych wysokiej gęstości tzn. o ilości dysków co najmniej 80 (zarówno NL-SAS, SAS i SSD) i gęstości upakowania co najmniej 18 dysków na każde U wysokości obudowy w szafie rack.
16. Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie musi być dostępne poprzez interfejs GUI w przeglądarce internetowej oraz interfejs linii poleceń (Command Line Interface). Dostęp do linii poleceń poprzez połączenie szyfrowane.
17. Musi istnieć możliwość bezpośredniego monitoringu stanu w jakim w danym momencie macierz się znajduje. Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI.
18. Musi istnieć funkcjonalność Cache dla procesu odczytu.
19. Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu.
20. Musi istnieć możliwość wyłączenia cache dla poszczególnych wolumenów.
21. Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający co najmniej taki sam czas przechowywania danych.
22. Macierz musi optymalizować wykorzystanie dysków SSD poprzez automatyczną identyfikację najbardziej obciążonych fragmentów wolumenów w zarządzanych zasobach dyskowych oraz ich automatyczną migracje na dyski SSD. Macierz musi również automatycznie rozpoznawać obciążenie fragmentów wolumenów na dyskach SSD i automatycznie migrować z dysków SSD nieobciążone fragmenty wolumenów. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami dysków – SSD, Enterprise (10K) oraz NL-SAS, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego wolumenu. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
23. Macierz musi obsługiwać funkcjonalności mapowania wolumenów do hostów lub grup hostów, tak aby inne hosty/grupy hostów nie miały do nich dostępu.
24. Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
25. Macierz musi obsługiwać min 255 kopi migawkowych per wolumen,
26. Macierz musi obsługiwać grupy spójności wolumenów do celów kopiowania i replikacji.
27. Macierz musi mieć możliwość wykonywania replikacji synchronicznej i asynchronicznej wolumenów logicznych pomiędzy tymi samymi modelami macierzy dyskowych. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (minimum SAS, SSD, NL-SAS). Replikacja musi być realizowana zarówno przy użyciu interfejsów Fibre Channel jak i protokołu IP. Przy replikacji z wykorzystaniem protokołu IP kontrolery macierzy musza zapewniać mechanizm optymalizacji transmisji danych po IP. Macierz musi umożliwiać kompresję w locie danych replikowanych po IP. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
28. Macierz musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami zasobów dyskowych wewnątrz macierzy, bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się aby zasoby źródłowe podlegające migracji oraz zasoby do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i być umiejscowione na różnych technologicznie dyskach stałych (SAS, SSD, NL-SAS). Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla maksymalnej konfiguracji.
29. Macierz musi posiadać funkcjonalność zarządzania ilością operacji wejścia-wyjścia wykonywanych na danym zasobie macierzy. Zarządzanie musi być możliwe poprzez określenie maksymalnej ilości operacji I/O na sekundę lub przepustowości określonej w MB/s dla danego zasobu lub poprzez oba te parametry jednocześnie. Wymagana jest możliwość określania ww. parametrów dla zasobów macierzy takich jak wolumen, grupa wolumenów, host, klaster hostów. Jeżeli funkcjonalność ta wymaga licencji należy ją dostarczyć dla maksymalnej konfiguracji macierzy.
30. Macierz musi posiadać funkcjonalność kompresji danych online, gdzie dane zapisywane w macierzy są kompresowane w locie i zapisywane na dyskach każdego wspieranego typu w postaci skompresowanej, a przy odczycie dane są również w locie dekompresowane i w takiej postaci przesyłane poza macierz. Operacja kompresji nie może wymagać alokacji innej przestrzeni dyskowej niż ta, która jest niezbędna do zapisania skompresowanych danych. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
31. Macierz musi posiadać funkcjonalność deduplikacji danych online, gdzie dane zapisywane w macierzy są deduplikowane w locie i zapisywane na dyskach każdego wspieranego typu w postaci po usunięciu duplikatów. Operacja deduplikacji nie może wymagać alokacji innej przestrzeni dyskowej niż ta, która jest niezbędna do zapisania zdeduplikowanych danych. Producent macierz musi udostępniać oprogramowanie pozwalające na estymację stopnia deduplikacji wolumenów. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
32. Kompresja i/lub deduplikacja muszą być możliwe do włączenia/wyłączenia z dokładnością do jednego wolumenu
33. Macierz musi posiadać funkcjonalność migracji danych z innych macierzy dyskowych z zachowaniem dostępu danych dla serwerów (import danych) z wykorzystaniem interfejsów FC, SAS i iSCSI. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla nieograniczonej ilości migrowanych macierzy.
34. Macierz musi umożliwiać stworzenie konfiguracji odpornej na awarię pojedynczej półki dyskowej
35. Macierz musi posiadać możliwość stworzenia aktywnego klastra, który przy wykorzystaniu dwóch urządzeń w dwóch lokalizacjach zapewni konfigurację wysokiej dostępności (HA-*high* availability) tzn. dostęp serwerów do tego samego zestawu LUNów prezentowanych z macierzy w każdej z lokalizacji. W sytuacji awarii jednej z dwóch macierzy wolumeny prezentowane do serwerów muszą być dostępne w sposób ciągły bez żadnej przerwy. Rozwiązanie musi być niezależne od platformy serwerowej i systemu operacyjnego. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
36. Macierz musi posiadać funkcjonalność wykonywania niezmienialnych (immutable) kopii lokalnych wolumenów dla potrzeb szybkiego odzyskiwania danych w przypadku np. celowego uszkodzenia danych (ransomware), tworzonych w wydzielonej przestrzeni na macierzy, wg. definiowalnych przez użytkownika polityk dotyczących częstotliwości wykonywania kopii i ich retencji. Jeżeli funkcjonalność wymaga licencji, należy taką licencję zaoferować dla całej macierzy w maksymalnej konfiguracji.
37. Macierz musi posiadać możliwość liniowej skalowalności parametrów wydajnościowych zasobów dyskowych oraz ilości obsługiwanych dysków (do co najmniej 800) poprzez dodanie do systemu kolejnej macierzy tego samego typu (łącznie co najmniej 2), przy zachowaniu jednolitego i wspólnego zarządzania zasobami dyskowymi.
38. Macierz musi obsługiwać minimum 5000 wolumenów oraz 256 hostów.
39. Sterowniki do obsługi wielościeżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu muszą być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych i/lub podłączanych serwerów zależnie od sposobu licencjonowania. Macierz może również wykorzystywać sterowniki systemu operacyjnego.
40. Macierz musi wspierać co najmniej systemy operacyjne MS Windows 2016 i nowsze, RHEL 8 i 9, VMWare vSphere 7 i nowsze, SLES 12 i nowsze, Ubuntu 18 i nowsze.
41. Wraz z macierzą należy dostarczyć kable zasilające oraz inne okablowanie wymagane dla prawidłowej pracy macierzy.
42. Macierz musi być fabrycznie nowa (data produkcji nie późniejsza niż 6 miesięcy przed dostawą), musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski i być objęta serwisem producenta na terenie RP.
43. Macierz musi być objęta serwisem gwarancyjnym przez okres 24 miesięcy ze zgłaszaniem problemów w trybie 9x5 oraz czasem naprawy w następnym dniu roboczym. W ramach serwisu muszą być dostępne nowe wersje oprogramowania dla macierzy.

**3. Przełącznik FC – 2 sztuki**

1. Przełącznik musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8 i 4Gb/s w zależności od rodzaju zastosowanych wkładek SFP+
2. Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji, gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 32 Gb/s. Całkowita przepustowość przełącznika FC musi wynosić minimum 768 Gb/s end-to-end.
3. Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900 ns.
4. Przełącznik FC musi posiadać minimum 24 porty FC z czego 8 aktywnych i obsadzonych wkładkami o prędkości minimum 32Gb/s SFP+ SWL
5. Rodzaj obsługiwanych portów co najmniej: E, F, Diagnostic Port
6. Przełącznik FC musi być przystosowany do montażu w szafie typu rack 19”, o wysokości maksymalnie 1U
7. Maksymalny dopuszczalny pobór mocy przełącznika FC wyposażonego w 24 aktywne porty 32Gb/s to 80W. Maksymalna ilość ciepła wydzielanego przez przełącznik FC wyposażony w 24 aktywne porty 32Gb/s to 215 BTU na godzinę.
8. Przełącznik FC musi być wyposażony w mechanizm agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 256 Gb/s (dla wkładek 32Gbps). Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC, a połączenie logiczne musi zachowywać kolejność przesyłanych ramek.
9. Przełącznik FC musi wspierać mechanizm balansowania ruchu pomiędzy co najmniej 16 różnymi połączeniami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID
10. Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID.
11. Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN
12. Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware’u zarówno na wyższą wersję jak i niższą w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC
13. Przełącznik FC musi wspierać mechanizmy zwiększające poziom bezpieczeństwa:
    1. uwierzytelnianie przełączników w sieci fabric za pomocą protokołów DH-CHAP i FCAP;
    2. mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric;
    3. uwierzytelnianie urządzeń końcowych w sieci fabric za pomocą protokołu DH-CHAP;
    4. szyfrowanie połączenia z konsolą administracyjną (wsparcie dla SSHv2);
    5. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control);
    6. definiowane kont administratorów w środowisku RADIUS i LDAP w MS Active Directory, Open LDAP, TACACS+;
    7. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS;
    8. obsługa minimum SNMP v3;
    9. IP Filter dla portu administracyjnego przełącznika;
    10. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP;
    11. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP
14. Przełącznik FC musi mieć możliwość konfiguracji przez polecenia tekstowe w interfejsie znakowym konsoli terminala oraz przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.
15. Interfejs graficzny oprogramowanie musi umożliwiać podstawową konfiguracje przełącznika, diagnostykę połączeń, konfiguracje portów, konfiguracje połączeń pomiędzy hostami a macierzami, analiza błędów ramek, wszystkich połączeń FC, które obsługuje przełącznik, tworzenie użytkowników, wykonywanie kopii konfiguracji przełącznika.
16. Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:
    1. logowanie zdarzeń poprzez mechanizm „syslog”,
    2. ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora (e-mail), wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych;
    3. port diagnostyczny tzw. D\_port, który umożliwia wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 32Gb/s oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5m dla wkładek SFP 32Gb/s (testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric);
    4. FCping;
    5. FC traceroute;
    6. kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika;
    7. mechanizm sprzętowego monitorowania przepływów danych dla wskazanych jak i automatycznie wykrywanych par urządzeń komunikujących się przez dany port przełącznika
    8. mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe
    9. mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy
    10. mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości, liczby zapisów i odczytów na sekundę oraz opóźnień operacji zapisu i odczytu.
17. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, port szeregowy oraz inband IP-over-FC
18. Przełącznik FC musi zapewniać obsługę interfejsu zarządzającego REST API.
19. Przełącznik FC musi zapewniać obsługę protokołu NVMe over FC
20. Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu. Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS\_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.
21. Wsparcie dla N\_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
22. Wszystkie opisane funkcje przełącznika mają być dostępne w urządzeniu na dzień składania ofert i być udokumentowane w publicznie dostępnej dokumentacji.
23. Gwarancja producenta na okres 24 miesięcy w miejscu instalacji. Możliwość zgłoszenia awarii w trybie 9x5 z czasem naprawy w następnym dniu roboczym. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z przełącznikiem oraz oprogramowania wewnętrznego przełącznika.
24. Serwis musi być realizowany przez producenta przełącznika w języku polskim.

**4. Biblioteka taśmowa – 1 sztuka:**

1. Obudowa typu RACK, wysokość maksymalna 1U.
2. Minimum 8 slotów na taśmy LTO.
3. Minimum 2 magazynki.
4. 1 slot i 1 czytnik kodów kreskowych.
5. 1 napęd taśmowy LTO8 8Gbs FC
6. Wraz z biblioteką należy dostarczyć: 24 taśmy LTO8, 1 taśmę czyszcząca.
7. Biblioteka wyposażona w minimum 1 zasilacz.
8. Interaktywny panel sterowania LCD.
9. Zdalne zarzadzanie poprzez osobny interfejs Ethernet RJ 45, Remote Management Interface przez HTTPS, wielojęzyczny.
10. Czas inicjalizacji 80-120s.
11. Średni czas wymiany nośników 45 s.
12. Zasilanie AC 100-240 Volt (50 – 60 Hz).
13. Ilość cykli między awariami 2.000.000.
14. Pobór energii 80W.
15. Kompatybilność z oprogramowaniem do wykonywania kopii bezpieczeństwa: Veritas BackupExec, Veeam, Acronis.
16. Gwarancja minimum 24 miesięcy.
17. Serwis świadczony w trybie „on site”, 5x9 z czasem reakcji w następnym dniu roboczym, przez producenta lub autoryzowanego przedstawiciela na terenie Polski.
18. Biblioteka musi być fabrycznie nowa (data produkcji nie późniejsza niż 6 miesięcy przed dostawą), musi pochodzić z autoryzowanego kanału dystrybucji producenta na terenie Polski i być objęta serwisem producenta na terenie RP.

**5. Serwer do kopii – 1 sztuka**

|  |  |
| --- | --- |
| Parametry techniczne | Minimalne wymagania |
| Obudowa | Rack 19’’ maks. 2U z możliwością instalacji 12 dysków w rozmiarze 3.5" oraz 2 dysków 2,5”, obudowa musi wspierać dyski hot-swap NVMe/SATA/SAS.  Na przednim panelu powinny się znajdować diody syngalizacyjne umożliwiające sprawdzenie statusu wentylatorów/przegrzania, aktywności dysków HDD, statusu połączeń. |
| Płyta główna | Płyta główna z możliwością zainstalowania dwóch procesorów.  Płyta główna musi być zaprojektowana przez producenta serwera. Płyta musi obsługiwać procesory do 64 rdzeni/128 wątków. Dodatkowo musi obsługiwać procesory do 270W TDP. |
| Procesor | Zainstalowane dwa procesory o parametrach jak poniżej:  Procesor klasy x86, min. 16 rdzeniowy, zaprojektowany do pracy w serwerach, taktowany zegarem co najmniej 4,1 GHz (w trybie turbo), z pamięcią cache L3 co najmniej 37,5 MB.  Zaoferowana konfiguracja dwuprocesorowa musi uzyskiwać w teście SPECrate2017\_int\_base wynik nie mniejszy niż 310 punktów. W przypadku braku wyników dla zaoferowanej konfiguracji Zamawiający zaakceptuje wyniki dla innej konfiguracji dwuprocesorowej danego producenta zbudowanej w oparciu o zaoferowane procesory.  Wydruk z platformy SPECrate2017\_int dla platform oferowanego dostawcy należy dołączyć do oferty. |
| Pamięć RAM | Zainstalowane 8 kości ram minimum 32GB, kości minimum DDR5 5600MHz ECC  Musi być możliwość rozbudowy o kolejne 8 kości RAM. |
| Dyski | Zainstalowane minimum 10 dysków hot-swap o pojemności nie mniejszej niż 14TB, SAS 12Gb/s, o prędkości obrotowej min, 7,2 tyś. obrotów/minutę.  Dwa dyski hot-swap NVMe o pojemności min. 960GB, dopuszczalne są nośniki klasy TLC lub lepsze, dyski o parametrach DWPD większe lub równie 1. System musi pozwalać na skonfigurowanie RAID 1/5/10 na nośnikach NVMe. |
| Kontroler RAID | Zainstalowany sprzętowy kontroler RAID o przepustowości min. 12 Gb/s z obsługą RAID 0, 1, 5, 6, 10, 50, 60 oraz z wsparciem dla trybu JBOD. Kontroler musi być wyposażony w pamięć Cache min. 4GB, z podtrzymaniem bateryjnym. |
| Interfejsy sieciowe | Minimum 2 porty 10GbE SFP+ obsadzone wkładkami o prędkości 10Gbit SFP+;  Minimum 2 porty 10GbE Base-T, RJ45; |
| Kontrolery FC | Dwuportowa karta 32Gb/64Gb FC obsadzona wkładkami o prędkości min. 32Gb. |
| Porty | - min. 4 port USB 3.x,  - min. 1 port VGA,  - min. 1 COM port (serial),  - min. 1 port 1 GbE RJ-45 dedykowany do zdalnego zarządzania. |
| Zasilacze | - min 2 zasilacze typu hot-swap 1200 W AC. Certyfikowane jako 80 PLUS Titanium certified. |
| Zarządzanie | Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarządzania zgodny ze standardem IPMI 2.0, SNMP.  Możliwość zdalnego restartu serwera i pełne zarządzanie serwerem poprzez połączenie w sieci TCP/IP przy użyciu przeglądarki internetowej,  Włączanie/wyłączanie serwera, reinstalację systemu operacyjnego, zdalne podłączenie napędów CD/DVD, dysków USB oraz obrazów dysków.  Monitoring oraz zażądanie mocą i jej zużyciem, monitoring sprzętu i usług uruchomionych na serwerze.  Oprogramowanie zarządzające powinno udostępniać wtyczki do używanego przez zamawiającego oprogramowania Vmware. Umożliwiając zarządzanie i monitorowanie serwerów poprzez wtyczkę do klienta Vmware vSphere z przeglądarki wykorzystując HTML5.  Integracja powinna obejmować aktualizację BIOS, firmware i BMC. |
| Wspierane systemy operacyjne | Co najmniej Windows Server 2022, RedHat Enterprise Linux (9.0).  Dostarczony system musi posiadać oficjalne wsparcie na stronie dostawcy oprogramowania lub być certyfikowane przez producenta serwera. |
| Sloty PCIe | Oferowany serwer powinien pozwalać na instalację łącznie 5 kart PCIe 5.0.  Oferowana konfiguracja musi posiadać przynajmniej 3 sloty PCIe wolne do późniejszego obsadzenia.  System musi pozwalać na instalację przynajmniej jednej karty GPU o parametrach wydajnościowych: FP32 min. 2,4TFLOPS, texture rate min. 78GTexel/s, Pixel Rate 44,5GPixel/s.  Karta GPU nie jest przedmiotem obecnego postępowania. |
| Dodatkowe wymagania | Zainstalowany moduł TPM 2.0  Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi posiadać deklaracja CE – wymagane oświadczenie wykonawcy lub producenta;  Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami – wymagane oświadczenie wykonawcy lub producenta;  Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2022 – wymagane oświadczenie wykonawcy lub producenta;  Elementy, z których zbudowany jest serwer muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz cały musi być objęty gwarancją producenta – wymaganie oświadczenie wykonawcy lub producenta;  Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;  Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; |
| Gwarancja | min. 36 miesięcy gwarancji i serwisu producenta; Oferowany serwis musi zapewniać: wsparcie techniczne w reżimie 5x9, możliwość zgłaszania awarii 24x7.  Serwis musi zapewniać dostawę części i usługę inżyniera w miejscu instalacji sprzętu w trybie NBD.  Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. |
| System operacyjny | Wraz z serwerem należy dostarczyć licencję na Windows Server 2022 Standard. Ilość licencji zgodna z ilością rdzeni w zaoferowanych procesorach, lub oprogramowania równoważnego.  RÓWNOWAŻNOŚĆ:  Warunki równoważności dla licencji systemu Microsoft Windows Server 2022 Standard.  W przypadku zaoferowania przez Wykonawcę licencji systemu równoważnego do systemu Microsoft Windows Server 2022 Standard, Zamawiający wymaga dostarczenia licencji dla serwerów oraz instalacji i migracji obecnego środowiska. Zamawiający wymaga, aby produkt równoważny spełniał niżej wymienione wymagania:  1. Współpraca z procesorami o architekturze x86 – 64bit.  2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym.  3. Możliwość budowania klastrów składających się z 64 węzłów.  4. Pojedyncza licencja musi obsłużyć serwer fizyczny wyposażony w 16 rdzeni.  5. Praca w roli klienta domeny Microsoft Active Directory.  6. Możliwość uruchomienia roli kontrolera domeny Microsoft Active Directory na poziomie funkcjonalności Microsoft Windows Server 2016.  7. Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.  8. Możliwość uruchomienia roli klienta i serwera czasu (NTP).  9. Możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.  10. Możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory.  11. Możliwość uruchomienia roli serwera stron WWW.  12. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera.  13. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego.  14. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).  15. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  16. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  17. Wbudowane wsparcie instalacji i pracy na wolumenach, które:  a. pozwalają na zmianę rozmiaru w czasie pracy systemu,  b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).  18. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość  19. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  20. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET  21. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  22. Możliwość wykorzystania standardu http/2.  23. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  24. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.  25. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.  26. Mechanizmy logowania w oparciu o: a) login i hasło,  a. karty z certyfikatami (smartcard),  b. wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM).  27. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla:  a. określonych grup użytkowników,  b. zastosowanej klasyfikacji danych,  c. centralnych polityk dostępu w sieci,  d. centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych.  28. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  29. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  30. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  31. Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji  w dokumentach (Digital Rights Management).  32. Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.  33. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  a. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC.  b. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  • podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  • ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  • odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  • bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.,  c. zdalna dystrybucja oprogramowania na stacje robocze,  d. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników,  e. 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,  • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.  f. szyfrowanie plików i folderów,  g. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  h. szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi,  i. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  j. serwis udostępniania stron WWW,  k. wsparcie dla protokołu IP w wersji 6 (IPv6),  l. wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  m. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie uruchomienie nieograniczonej liczby aktywnych środowisk wirtualnych systemów operacyjnych (liczba ograniczona parametrami fizycznymi serwera),  n. możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  o. możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover  z jednoczesnym zachowaniem pozostałej funkcjonalności.  p. mechanizmy wirtualizacji mające wsparcie dla:  • dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  • obsługi ramek typu jumbo frames dla maszyn wirtualnych.  • obsługi 4-KB sektorów dysków,  • nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  • możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.  q. możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów.  r. wsparcie dla rozwiązania Kubernetes.  s. możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz  z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  t. wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).  u. mechanizmy deduplikacji i kompresji na wolumenach.  v. mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  w. mechanizm konfiguracji połączenia VPN do platformy Azure.  x. wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.  y. mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.  z. możliwość instalacji i poprawnej pracy Systemu Bazodanowego (Microsoft SQL Server Standard). |

**6. Zasilacz awaryjny – 2 sztuki:**

|  |  |
| --- | --- |
| *Minimalne wymagania techniczne dla jednostki UPS* | Moc znamionowa jednostki nie mniej niż 3000VA / 2700W  Wersja do montażu w szafie Rack  Technologia Line Interactive  Temperatura eksploatacji 0 - 40 °C   * Wilgotność względna podczas pracy 0 - 95 % * Wysokość n.p.m. podczas pracy 0-3000 m * Hałas słyszalny w odległości 1 m od powierzchni urządzenia 55,0 dBA * Rozpraszanie ciepła w trybie online 184,00 BTU/h * Klasa energetyczna sprzętu przeciwprzepięciowego 645J * możliwość zimnego startu * automatyczne włączenie UPS-a po powrocie zasilania   automatyczna regulacja napięcia (AVR) z funkcją korekcji niskich i wysokich napięć |
| *Parametry wejściowe* | * Nominalne napięcie wejściowe 230V * Częstotliwość wejściowa 50/60 Hz +/-3 Hz (automatyczne wykrywanie) * Typ gniazda wejściowego: IEC-320 C14 * Zmienny zakres napięcia wejściowego w trybie podstawowym 140 - 280V * Inne napięcia wejściowe 220, 240 |
| *Parametry wyjściowe* | * Napięcie wyjściowe 230VAC * Częstotliwość na wyjściu (zsynchronizowana z siecią zasilającą) 57/63Hz +/- 3 Hz * Inne napięcia wyjściowe 220, 240 * Typ przebiegu sinusoida * Złącza/gniazda wyjściowe   (8) IEC 320 C13 (Zasilanie zapasowe)   * (1) IEC 320 C19 (Zasilanie zapasowe) |
| Akumulatory i czas podtrzymania | * Typ akumulatora bezobsługowy szczelny akumulator kwasowo-ołowiowy z elektrolitem w postaci żelu * Czas autonomii: 6 minut 15 sekund dla pełnego obciążenia 18 minut 3 sekundy dla połowy obciążenia * Czas autonomii z dodatkowym modułem bateryjnym: 31 minut dla pełnego obciążenia 70 minut dla połowy obciążenia * Typowy czas ładowania 3 godziny * Oczekiwana żywotność akumulatora (lata) 4 – 6 * Baterie wymieniane na gorąco * możliwość wymiany akumulatora przez użytkownika   automatyczny test akumulatora |
| *Komunikacja i zarządzanie* | * Gniazdo do montażu karty WEB/SNMP- Smart Slot x1 * Wstępnie zainstalowana karta zarządzania siecią do monitorowania i zarządzania UPS. * Moduł WEB/SNMP obsługiwane protokoły komunikacyjne:   IP v.6  SNMP v.3  Modbus TCP   * Porty komunikacyjne: RJ-45 Serial, SmartSlot, USB * Panel sterowania:   Wielofunkcyjna konsola sterownicza i informacyjna LCD  Alarm dźwiękowy: Alarm przy zasilaniu akumulatora: alarm przy bardzo niskim poziomie naładowania akumulatora: konfigurowalne opóźnienia   * Awaryjny wyłącznik zasilania (EPO) Tak |
| *Certyfikaty, zgodności oraz gwarancja* | * CSA, EAC, EN/IEC 62040-1, EN/IEC 62040-2, RCM, UL 1778, VDE, RoHS * 2 lata gwarancji naprawy lub wymiany (bez akumulatora) i 2 lata na akumulator |
| *Oprogramowanie* | * Dostępne oprogramowanie do zarządzania/monitorigu (niektóre wersje odpłatne) z VMware® ESXi (VMware® ESXi Server 6.5 Update 3 (vMA 6.5), VMware® ESXi Server 6.5 Update 2 (vMA 6.5)); Microsoft® Hyper-V (Windows® Hyper-V Server 2019, 2012 R2); Windows® Server 2019, 2016, 2012; Windows® 10, 7; Red Hat® Enterprise Linux; SuSE® Linux®. |
| *Dodatkowe* | Wraz z UPS należy dostarczyć kartę zarządzającą LAN |

**7. Usługa instalacji i konfiguracji:**

1. Montaż dostarczonych przełączników SAN, macierzy dyskowej, serwerów oraz biblioteki taśmowej.
2. Podłączenie dostarczonych urządzeń do sieci LAN, konfiguracja adresów IP służących do zarządzania dostarczonymi urządzeniami.
3. Podłączenie dostarczonych przełączników SAN do posiadanych przez Zamawiającego serwerów oraz macierzy dyskowej.
4. Podłączenie dostarczonych serwerów, macierzy dyskowej oraz biblioteki taśmowej do sieci SAN.
5. Konfiguracja zoningu na dostarczonych przełącznikach SAN. Prace związane z konfiguracją sieci SAN nie mogą mieć wpływu na ciągłość działania infrastruktury Zamawiającego.
6. Udostępnienie zasobów zainstalowanej macierzy dyskowej serwerom wchodzącym w skład posiadanego przez Zamawiającego środowiska wirtualizującego.
7. Instalacja systemu hypervisora na jednym z dostarczonych serwerów. Podłączenie serwera do posiadanego przez Zamawiającego środowiska wirtualizującego. Migracja wskazanych maszyn wirtualnych na zainstalowany system.
8. Podniesienie wersji posiadanego przez Zamawiającego środowiska wirtualizującego do najnowszej wspieranej wersji systemu.
9. Migracja posiadanego przez Zamawiającego systemu kopii bezpieczeństwa na dostarczony serwer. Konfiguracja zasobów dyskowych dostarczonego serwera w taki sposób by dane składowane na nim podlegały deduplikacji.
10. Konfiguracja obecnie posiadanego serwera kopii bezpieczeństwa jako dodatkowego repozytorium przechowujące kopie bezpieczeństwa. System musi działać pod kontrolą systemu operacyjnego Linux.
11. Podłączenie oraz konfiguracja dostarczonej biblioteki taśmowej jako dodatkowego repozytorium przechowującego kopię bezpieczeństwa.
12. Szkolenie dla 2 administratorów.

**ZADANIE NR 2 – dostawa UTM**

**1. UTM – 1 sztuka**

**Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 7 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

**Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

**Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:

* 8 portami Gigabit Ethernet RJ-45.
* 2 gniazdami SFP+ 10 Gbps.

1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System jest wyposażony w zasilanie AC.

**Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 28 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 25 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 2.5 Gbps.

**Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

**Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.

* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

**Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.

1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:

* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

**Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

**Funkcje SD-WAN**

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

**Zarządzanie pasmem**

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

**Ochrona przed malware**

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

**Ochrona przed atakami**

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

**Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

**Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

**Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia 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.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

**Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

**Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

**Testy wydajnościowe oraz funkcjonalne**

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

**Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.

**Gwarancja oraz wsparcie**

1. System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**ZADANIE NR 3 – dostawa przełączników sieciowych:**

**Przełącznik 1 – 2 sztuki**

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany z wysyłką w następnym dniu roboczym po potwierdzeniu przez producenta awarii.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów 8 portów 1GBaseT PoE+, 2 porty 1GBaseT oraz 2 x SFP
* Budzet PoE min. 125W
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 4000
* CPU klasy min. ARM A9 1.25Ghz
* Min. 2GB RAM
* Bufor 16Mb
* MTBF min. 778769 godzin
* Wydajność min. 17,86 Mp/s
* Przepustowość min. 24 Gb/s
* Możliwość wyłączenia wentylatorów z poziomu interfejsu web wspierane przez producenta w celu wyeliminowania hałasu generowanego przez przełącznik
* Port USB Type-C
* Port zarządzania Out-of-band oraz konsolowy RJ45
* Web GUI
* Interfejs web umożliwiający automatyczne przypisanie konfiguracji do portów właściwej dla protokołów czy też producenta: NVX, AMX, NDI, ZeeVee, Aurora, Kramer, LibAV, Dante Video, SDVoE, AES67, Q-SYS, Audio Dante, AVB
* Wymaga się aby powyższe szablony konfiguracji były stworzone przez producenta przełącznika a interfejs web w sposób jednoznaczny wskazywał że dany producent AV czy protokół jest obsługiwany przez dany szablon.
* Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH.
* Wymaga się aby w sposób manualny istniała możliwość wyboru trybu wykrywania urządzeń PoE. Jednym z takich trybów powinien być: 4ptdot3af
* HTTPs
* SSH
* Przełącznik powinien mieć możliwość montażu uchwytów rack z przodu lub z tyłu obudowy przełącznika. Dodatkowo w raz z przełącznikiem należy dostarczyć oryginalny zestaw do montażu w szafie rack, który umożliwi cofnięcie przełącznika o około 2 cale w celu zwiększenia przestrzeni na okablowanie sieciowe pomiędzy dziwami szafy a przełącznikiem.
* Przełącznik powinien mieć możliwość montażu za pomocą uchwytów w standardzie VESA
* Przełącznik powinien mieć możliwość montażu za pomocą pojedynczej śruby 1xM10
* Obsługa PTPv2
* STP, MTP, RSTP PV(R)STP
* IPv4/IPv6:
* PIM-SM
* PIM-DM
* SSM
* Kształtowanie ruchu na wejściu oraz wyjściu co 1 Kbps
* Radius
* TACACS+
* IGMPv1,v2 Querier
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014, EN 60950-1, EN 62368-1
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* CCC: GB4943.1-2011; YD/T993-1998; GB/T9254-2008 (Class A)
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A

**Przełącznik nr 2 – 7 sztuk**

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

Wymaga się aby urządzenie posiadało następujące porty, protokoły oraz spełniało następujące funkcje:

* Ilość portów 48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne
* Chłodzenie od przodu do tyłu obudowy
* Możliwość instalacji redundantnego zasilacza
* Tablica MAC min. 16K
* Tablica ARP/NDP min. 888
* Bufor 16Mb
* MTBF min. 578472 godzin
* Wydajność min. 130,9 Mp/s
* Przepustowość min. 176 Gb/s
* Port USB
* Port miniUSB
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Auto-VoIP
* Auto-iSCSI
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* PV(R)STP
* BPDU/STRG Root Guard
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min 800 Mhz
* Min 1GB RAM
* Min 256MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Non-stop forwarding (NSF)
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu
* Zasilacz z certyfikatem 80+
* CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014,
* Class A, EN 61000-3-3:2013, EN 55024:2010
* VCCI : VCCI-CISPR 32:2016, Class A
* RCM: AS/NZS CISPR 32:2013 Class A
* FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014
* ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014
* BSMI: CNS 13438 Class A

**Przełącznik nr 3 – 1 sztuka**

Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji.

* Ilość portów 36 x 1/2,5/5/10G PoE+, 4 x SFP28 10/25G
* Chłodzenie od przodu do tyłu obudowy
* Budżet PoE min.: 280W
* Tablica MAC min. 16K
* Tablica 4K ARP/ 512 NDP
* Bufor 64Mb
* Wydajność min. 684,48 Mpps
* Przepustowość min. 920 Gb/s
* Port USB-C
* Port zarządzania Out-of-band;
* Web GUI
* HTTPs
* CLI
* Telnet
* SSH
* SNMP
* MIB RSPAN
* Radius
* TACACS+
* DiffServ
* Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
* Interfejs web umożliwiający automatyczne przypisanie konfiguracji do portów właściwej dla protokołów czy też producenta: NVX, AMX, NDI, ZeeVee, Aurora, Kramer, LibAV, Dante Video, SDVoE, AES67, Q-SYS, Audio Dante, AVB, Crestron DigitalMedia AV, NUCLEUS Converged AV, Shure, Sonos, Visionary AV
* Wymaga się aby powyższe szablony konfiguracji były stworzone przez producenta przełącznika a interfejs web w sposób jednoznaczny wskazywał że dany producent AV czy protokół jest obsługiwany przez dany szablon.
* Wymaga się aby producent dostarczył kontroler w formie aplikacji umożlwiający przypisanie profilu AV do grupy przełączników w sposób automatyczny
* Wymaga się aby interfejs web miał możliwość wykonywania poleceń tekstowych CLI bez potrzeby tworzenia oddzielnego połączenia Telnet lub SSH.
* IPv4/IPv6 Multicast filtering
* IGMPv3 MLDv2 Snooping
* ASM & SSM
* IGMPv1,v2 Querier
* Policy-based routing (PBR)
* LLDP-MED
* Spanning Tree
* Green Ethernet
* STP
* MTP
* RSTP
* EEE (802.3az)
* GVRP/GMRP
* Q in Q,
* Private VLAN
* DOT1X
* MAB
* Captive Portal
* DHCP Snooping
* Dynamic ARP
* Inspection
* IP Source Guard
* CPU min ARMv8 1.8Ghz
* Min 2GB RAM
* Min 512MB Flash
* Min ilość obsługiwanych VLAN 4K
* DHCP Server min 2K rezerwacji
* sFlow
* Minimalna ilość przełączników w stosie: 8
* Możliwość łączenia w stos za pomocą interfejsów 25Gb/s
* Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
* Distributed Link Aggregation (LAGs across the stack)
* Ilość interfejsów IP 128
* Double VLAN Tagging (QoQ)
* Yes
* PIM-DM (Multicast Routing - dense mode)
* PIM-DM (IPv6)
* PIM-SM (Multicast Routing - sparse mode)
* PIM-SM (IPv6)
* RIPv1
* RIPv2
* OSPFv2
* RFC 2328
* RFC 1583
* OSPFv3
* OSPFv2 min. sąsiadów 400
* OSPFv3 min. sąsiadów 400
* OSPFv3 min. sąsiadów na interfejs 100
* UDLD
* LLPF
* DHCPv6 Snooping
* wysyłanie alertów na email
* MMRP
* Ilość ACL min. 100
* Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu

**ZADANIE nr 4 – dostawa access pointów:**

**1. Access Point – 4 sztuki**

**Punkt dostępu**

Cechy mechaniczne

Przeznaczony do montażu na suficie, kształt talerza, barwa jasna, budowa zewnętrzna z poliwęglanu, elementy montażowe ze stali nierdzewnej. Elementy montażowe w zestawie. Certyfikat wodoszczelności IP54.

Sprzęt

Interfejs sieciowy 1GbE RJ45

Interfejs do zarządzania: Ethernet, bluetooth

Zasilanie PoE+,

Pasywne PoE 48V

Obsługiwany przedział napięć 44-57V DC

Maksymalna pobór prądu: < 19W

Maksymalna moc nadawania:

* 2.4 GHz – 26dBm
* 5 GHz – 26 dBm

MIMO

* 2.4 GHz - 4x4 (SU-MIMO)
* 5 GHz - 4x4 (DL/UL MU-MIMO)

Maksymalna prędkość przesyłu danych:

* 2.4 GHz – 600 Mbps (pasmo 40 MHz)
* 5 GHz – 2.4 Gbps (pasmo 160MHz)

Wzmocnienie anteny

* 2.4 GHz – 4 dBi
* 5 GHz – 5.5 dBi

Sygnalizacja LED informująca o stanie pracy

Praca w temperaturze otoczenia: od -30C do +60C

Praca w wilgotności otoczenia: od 5% do 95%

Certyfikaty: CE, FCC, IC

**Oprogramowanie**

Standard WiFi: 802.11a/b/g/n/ac/ax (WiFi 6) lub nowszy

Ochrona WiFi: WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)

BSSID: 8 na radio

VLAN: 802.1Q

Zaawansowany QoS: Per-user rate limiting

Izolacja sieci dla gości

Ilość jednocześnie podłączonych urządzeń: > 350

Obsługiwane szybkości transmisji danych

* 802.11a 6, 9, 12, 18, 24, 36, 48, 54 Mbps
* 802.11b 1, 2, 5.5, 11 Mbps
* 802.11g 6, 9, 12, 18, 24, 36, 48, 54 Mbps
* 802.11n 6.5 Mbps to 600 Mbps (MCS0 - MCS31, HT 20/40)
* 802.11ac 6.5 Mbps to 1.7 Gbps (MCS0 - MCS9 NSS1/2/3/4, VHT 20/40/80)  
  6.5 Mbps to 1.7 Gbps (MCS0 - MCS9 NSS1/2, VHT 160)
* 802.11ax (WiFi 6) 7.3 Mbps to 2.4 Gbps (MCS0 - MCS11 NSS1/2/3/4, HE 20/40/80)  
  7.3 Mbps to 2.4 Gbps (MCS0 - MCS11 NSS1/2, HE 160)

Zarządzanie poprzez zewnętrzny kontroler, możliwość jednoczesnego zarządzania wszystkimi punktami dostępu z jednego kontrolera.

Dodatkowo dołączony odpowiedni zasilacz PoE+

**ZADANIE nr 5 –** **dostawa urządzenia NAS wraz z dyskami:**

**1. Urządzenie NAS wraz z dyskami:**

|  |  |
| --- | --- |
| Procesor | |
| Procesor liczba rdzeni | Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 4,633 punktów PassMark CPU Mark (https://www.cpubenchmark.net – oraz posiadać sprzętowe wsparcie technologii wirtualizacji.)  W przypadku braku zaoferowanego przez Wykonawcę procesora na w/w liście, Wykonawca obowiązany jest przeprowadzić test Passmarka i jego wynik załączyć do oferty. |
| Pamięć RAM | Nie mniej niż 4 |
| Pamieć RAM liczba slotów | Nie mniej niż 16GB |
| Pamięć RAM - możliwość rozszerzenia | Minimum 2 sloty |
| Pamięć Flash | Nie mniej niż do 64GB |
| Liczba zatok na dyski | Nie mniej niż 5 GB |
| Obsugiwane dyski | Minimum 4 zatoki 3,5" |
| Wbudowane w urządzenie interfejsy na dyski M2 | 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SATA SSD |
| Możliwość stosowania dysków twardych o pojemności | Wymagane min. 2 x M2 PCIe Gen3x1 |
| Możliwość podłączenia modułu rozszerzającego | do 18TB |
| Porty LAN 2,5 GbE | Tak, co najmniej 2 |
| Diody LED | Minimum 2 RJ-45 |
| Porty USB 3.2 Gen2 | Minimum Status, LAN, HDD |
| Port PCiE | Minimum 3 |
| Przyciski | Tak, minimum 2 Gen3x4 |
| Typ obudowy | Reset, Zasilanie |
| Dopuszczalna temperatura pracy | Tower |
| Wilgotność względna podczas pracy | od 0 do 40˚C |
| Zasilanie | 5-95% R.H. |
|  | Max. 250 W |
|  |  |
| Specyfikacja oprogramowania |  |
| Obsługa dwóch systemów operacyjnych | |
| Wymagania dla systemu operacyjnego opartego o system plików EXT4 | Możliwość wyboru w trakcie inicjalizacji urządzenia systemu operacyjnego opartego na systemach plików EXT4 lub ZFS |
| Agregacja łączy |  |
| Obsługiwane systemy plików | Tak |
| Możliwość podłączenia karty WLAN na USB | Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+, exFAT |
| Szyfrowanie udziałów | Tak |
| Szyfrowanie dysków zewnętrznych | Tak, min AES 256 |
| Zarządzanie dyskami | Tak |
| Wbudowana obsługa iSCSI | Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD,  Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek |
| Zarządzanie prawami dostępu | Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN |
| Obsługa Windows AD | 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 |
| Funkcje backup | Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP |
| Współpraca z zewnętrznymi dostawcami usług chmury | Oprogramowanie do tworzenia kopii bezpieczeństwa plików producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde, |
| Darmowe aplikacje na urządzenia mobilne | Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box |
| Minimum obsługiwane serwery | Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer  Dostępne na systemy iOS oraz Android |
| VPN | Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu |
| Administracja systemu | VPN client / VPN server  Obsługa PPTP, OpenVPN |
| Wirtualizacja | 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 automatyczna Możliwość aktualizacji oprogramowania ręcznie Ustawienia systemu: Kopia, Przywracanie, Resetowanie |
| Konteneryzacja | Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android.  Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych. |
| Zabezpieczenia | Możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker |
| Możliwość instalacji dodatkowego oprogramowania | 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 |
|  | Tak, sklep z aplikacjami; możliwość instalacji z paczek |
| Gwarancja |  |
|  | 3 lata – (podczas naprawy dyski twarde zostają u zamawiającego) |
| Dyski twarde | 4 dyski o pojemności **4TB** każdy, dedykowane do serwerów NAS |
|  |  |