Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest:

1. Dostawa platformy do stworzenia prywatnej chmury o funkcjonalnościach wyszczególnionych poniżej, określonej w OPZ jako **„System”**. System musi zostać dostarczony w modelu hiperkonwergentnym tzn. z wykorzystaniem serwerów z procesorami Intel x86, posiadającymi dyski wewnętrzne, które tworzą warstwę storage.
2. Dostawa systemu backupowego o parametrach i funkcjonalnościach wyszczególnionych poniżej, określonego w OPZ jako **„System backupu”**.
3. Dostawa sprzętu sieciowego w ilości i parametrach wyszczególnionych poniżej, wraz z oprogramowaniem do monitorowania tegoż nowopowstałego środowiska sieciowego określonych całościowo w OPZ jako **„Sprzęt sieciowy”**.
4. Przeprowadzenie szkolenia z zakresu administrowania dostarczoną platformą, systemem oraz sprzętem sieciowym dla wskazanych przez Zamawiającego osób z zespołu IT. Szkolenie zostanie przeprowadzone w siedzibie Zamawiającego na uruchomionym w ramach zamówienia Systemie, sprzęcie sieciowym oraz systemie backupowym. Dopuszcza się zorganizowanie i przeprowadzenie części szkolenia na tożsamym środowisku testowym we wskazanym przez Wykonawcę miejscu. Alternatywne środowisko testowe powinno mieć identyczne parametry jak środowisko uruchamiane. Wykonawca przeprowadzi w siedzibie Zamawiającego szkolenie w zakresie dotyczącym cyberbezpieczeństwa dla minimum 10 wskazanych przez Zamawiającego pracowników Urzędu Miasta Jarosławia bądź pracowników jednostek podległych.

1. **System**

**Chmura prywatna**

1. rozwiązanie (sprzęt serwerowy x86, wirtualizator, pamięć masowa zdefiniowana programowo, ochrona i zabezpieczenie danych, zintegrowane zarządzanie) musi być dostarczone, zaprojektowane, zintegrowane oraz wspierane przez jednego dostawcę,
2. wszystkie komponenty rozwiązania (sprzęt serwerowy x86, wirtualizator, pamięć masowa zdefiniowana programowo, ochrona i zabezpieczenie danych) muszą być zarządzane z jednego miejsca, za pomocą wbudowanego i zintegrowanego narzędzia,
3. rozwiązanie musi być certyfikowane na serwerach co najmniej 3 globalnych producentów serwerów,
4. rozwiązanie musi być niezależne od sprzętu (nie może być ograniczone do określonego dostawcy sprzętu x86). Wymagana jest możliwość przenoszenia licencji lub subskrypcji pomiędzy wszystkimi wspieranymi platformami x86,
5. platforma sprzętowa w zaproponowanej konfiguracji musi być certyfikowana przez producenta Systemu i znajdować się na publicznie dostępnej liście kompatybilności,
6. możliwość wykonywania i monitorowania aktualizacji wszystkich komponentów rozwiązania za pomocą pojedynczego narzędzia zarządzania. Narzędzie musi wykonywać automatyczną weryfikację kompatybilności wersji oprogramowania,
7. rozwiązanie musi być samo naprawialne. Oznacza to, że musi utrzymywać określony poziom odporności na awarie oraz stałą wydajność w przypadku awarii, bez konieczności interwencji administratora. Musi także przywrócić odporność tak szybko jak tylko możliwe,
8. rozwiązanie musi być niezależne od sieci, nie może wymagać określonego typu sprzętu sieciowego,
9. rozwiązanie musi zapewniać wbudowaną funkcję udostępniania usług pamięci masowej dla maszyn wirtualnych, kontenerów oraz zewnętrznych serwerów jako:
* blokowe zasoby iSCSI,
* plikowe zasoby – poprzez protokoły NFS i SMB,
* zasoby obiektowe – kompatybilne z Amazon S3,
1. rozwiązanie musi zapewniać możliwość udostępniania pamięci masowej jako LUN-y iSCSI, do maszyn wirtualnych uruchomionych na zasobach rozwiązania,
2. rozwiązanie musi umożliwiać uruchamianie klastrów Kubernetes za pomocą kreatora (tzw. wizard), spełniając następujące kryteria:
* musi umożliwiać udostępnienie usług pamięci masowej dla klastra Kubernetes,
* pamięć masowa musi obsługiwać plugin CSI (Container Storage Interface),
* musi zapewnić możliwość uruchomienia nieograniczonej liczby podów Kubernetes,
* musi zapewnić wbudowane zarządzanie i orkiestrację kontenerów,
1. Rozwiązanie musi wspierać różne warstwy pamięci masowej:
* SSD i NVMe jako warstwa wydajnościowa,
* NL-SAS/SATA/SSD jako warstwa pojemnościowa,
1. Rozwiązanie musi zapewniać zautomatyzowane, działające w czasie rzeczywistym, wielowarstwowe składowanie danych (ang. tiering) pomiędzy nośnikami SSD/NVMe (warstwa buforująca i wydajnościowa) oraz HDD/SSD (warstwa pojemnościowa), w celu zapewnienia optymalnej wydajności. Jeśli wielowarstwowe składowanie (ang. tiering) nie jest dostępne, wówczas rozwiązanie musi być w całości zbudowane w oparciu o odpowiednio NVMe lub SSD, a także musi zostać dostarczona gwarancja ceny nośnika SSD/NVMe w całym okresie trwania kontraktu. W przypadku rozwiązania opartego o technologię cache’owania danych, wymagany współczynnik warstwy wydajnościowej do warstwy pojemnościowej to 30%. W przypadku rozwiązania opartego o technologie cache’owania danych, zamawiający wymaga odpowiedniej wydajności 100 000 zapisów/sec oraz wytrzymałości na poziomie 20 000 TBW,
2. jeśli system plików w wyniku założeń projektowych architektury lub jako najlepsza praktyka nie powinien być całkowicie zapełniany przez dane użytkownika, wówczas niezbędna wolna przestrzeń (ang. slack space) powinna zostać uwzględniona dodatkowo i doliczona do pojemności surowej węzła,
3. rozwiązanie musi umożliwiać utworzenie kontenera danych bez współczynnika odporności tzw. RAID 0 lub Resiliance Factor 1, który będzie przeznaczony dla aplikacji i baz danych posiadające wewnętrzne mechanizmy replikacji danych,
4. wszystkie węzły muszą być hiperkonwergentne, a lokalne (wewnętrzne) dyski wszystkich węzłów muszą stanowić klaster prezentowany jako pojedyncza i rozproszona pula zasobów dostępna dla wszystkich węzłów kontrolowanych przez wirtualizator. Węzły obliczeniowe nie są akceptowane,
5. rozwiązanie musi umożliwiać dodawanie serwerów typu Storage Node, które powiększają sumaryczną pojemność klastra, lecz nie umożliwiają uruchomiania maszyn wirtualnych na tych serwerach,
6. rozwiązanie musi zapewniać usługę kompresji danych, w trybie online, w ramach dostarczonej licencji. Wymaganie dotyczy zarówno konfiguracji hybrydowych, jak i All-Flash,
7. poniższe usługi i parametry pamięci masowej muszą być konfigurowalne osobno dla każdej maszyny wirtualnej lub kontenera danych:
* kompresja,
* deduplikacja,
* Resilience Factor (współczynnik odporności na awarie): N+1,
1. rozwiązanie musi zapewniać funkcję tworzenia kopii migawkowych oraz klonów maszyn wirtualnych, także z zapewnieniem spójności z punktu widzenia aplikacji (co najmniej dla systemów operacyjnych Windows oraz Linux). Funkcja ta musi być wbudowana w platformę i realizowana na poziomie pamięci masowej,
2. w przypadku awarii pojedynczego serwera lub dysku, system musi wskazywać przewidywany czas potrzebny do odbudowania danych,
3. platforma musi zapewniać bliskość danych względem miejsca ich przetwarzania (ang. data locality). Oznacza to, że zastosowana architektura i wykorzystywane algorytmy rozkładania danych pomiędzy węzły platformy, muszą nieustannie zmierzać do umieszczenia danych należących do maszyny wirtualnej na lokalnych zasobach pamięci masowej węzła, na którym uruchomiona jest dana maszyna wirtualna.

**Bezpieczeństwo**

1. system musi wspierać dyski SED;
2. system musi wspierać dwuskładnikowe uwierzytelnienie do Systemu,
3. system musi posiadać tzw. STIG, regularnie aktualizowane i udostępniane przez producenta,
4. system musi posiadać mechanizm automatycznego wykrywania odchyleń od STIG i automatycznie je naprawiać, zarówno w warstwie wirtualizacji jak i storage

**Odporność na awarię, wysoka dostępność, backup, Disaster Recovery**

1. system musi być odporny na jednoczesną awarię co najmniej jednego z dowolnych komponentów Systemu, nie powodując przerwy w pracy Systemu,
2. system musi umożliwiać replikację maszyn wirtualnych między ośrodkami z RPO = 60 minut w ramach dostarczonych licencji,
3. system musi wspierać odtwarzanie pojedynczych plików ze Snapshotów,
4. system musi umożliwiać replikację z RPO = 60 minut oraz scenariusze Disaster Recover dla różnych hypervisorów w dwóch ośrodkach

**Usługi plikowe**

1. system musi posiadać wbudowane, rozproszone usługi plikowe,
2. system musi zapewniać usługi plikowe poprzez protokół NFS v3/v4 oraz SMB,
3. system musi umożliwiać jednoczesny dostęp do plików za pomocą NFS oraz SMB,
4. system musi umożliwiać rozbudowę usług plikowych w modelu scale-out, poprzez dokładanie kolejnych węzłów. Dodatkowe węzły muszą zwiększać zarówno pojemność usług plikowych jak i ich wydajność,
5. system musi posiadać możliwość replikacji zasobów plikowych pomiędzy klastrami z RPO = 60 minut,
6. system usług plikowych musi integrować się z Active Directory oraz rozwiązaniami Antywirus za pomocą protokołu ICAP,
7. system usług plikowych musi wspierać CFT (Change File Tracking)
8. system musi obsługiwać szyfrowanie danych dla zasobów plikowych (tzw. data at rest encryption),
9. jeżeli System nie posiada wbudowanych usług plikowych, wymagane jest dostarczenie oddzielnego rozwiązania usług plikowych w modelu scale-out, o liczbie węzłów oraz pojemności zgodnych z wymaganiami Systemu, spełniającego wszystkie pozostałe zapisy powyżej,
10. w ramach rozwiązania należy dostarczyć licencje umożliwiającą uruchomienie systemu plikowego o pojemności 1 TiB.

**Usługi obiektowe**

1. system musi posiadać wbudowane, rozproszone usługi obiektowe,
2. system musi zapewniać usługi obiektowe poprzez protokół S3,
3. system musi umożliwiać rozbudowę usług obiektowych w modelu scale-out, poprzez dokładanie kolejnych węzłów. Dodatkowe węzły muszą zwiększać zarówno pojemność usług plikowych jak i ich wydajność,
4. system musi posiadać możliwość replikacji zasobów plikowych pomiędzy klastrami z RPO = 1 minuta,
5. system usług obiektowych musi integrować się z Active Directory,
6. system usług obiektowych musi zapewniać WORM (Write Once Read Many) oraz wersjonowanie obiektów,
7. system musi obsługiwać szyfrowanie danych dla zasobów plikowych (tzw. data at rest encryption)
8. system musi obsługiwać REST API,
9. jeżeli System nie posiada wbudowanych usług obiektowych, wymagane jest dostarczenie oddzielnego rozwiązania usług obiektowych w modelu scale-out, o liczbie węzłów i pojemności zgodnych z wymaganiami Systemu, spełniającego wszystkie pozostałe zapisy powyżej,
10. w ramach rozwiązania należy dostarczyć licencje umożliwiającą uruchomienie systemu obiektowego o pojemności 2 TiB

**Zarządzanie**

1. zarządzanie Systemem musi odbywać się z pojedynczej konsoli
2. system musi umożliwiać bezprzerwową rozbudowę klastra, poprzez dołożenie kolejnych węzłów. System musi automatycznie rozłożyć równomiernie dane w klastrze, bez ingerencji administratora,
3. konsola zarządzania Systemem musi umożliwiać podnoszenie wersji Systemu (sterowniki serwerów, hypervisor, podsystem storage) bez przerwy w pracy Systemu.
4. system musi automatycznie sprawdzać kompatybilność podnoszonych elementów Systemu (sterowniki serwerów, hypervisor, podsystem storage) eliminując możliwość omyłkowego podniesienia jednego z komponentów do niewłaściwej wersji,
5. system musi udostępniać szczegółowe informacje na temat maszyn wirtualnych:
* wydajność maszyn wirtualnych (utylizacja CPU/RAM/IOPS oraz opóźnienie/latency),
* rekomendacje w temacie przypisanych zasobów (za mało / za dużo CPU lub RAM)
1. system musi wspierać REST API dla całej platformy.

**Hypervisor**

1. do zaproponowanego systemu należy dostarczyć licencje na oprogramowanie wirtualizacyjne na każdy dostarczony serwer,
2. oprogramowanie wirtualizacyjne musi zapewniać mechanizmy przenoszenia maszyn wirtualnych bezprzerwowo pomiędzy węzłami w klastrze,
3. oprogramowanie wirtualizacyjne musi zapewniać mechanizmy HA w obrębie pojedynczego klastra,
4. oprogramowanie wirtualizacyjne musi posiadać mechanizm inteligentnego umiejscowienia nowych maszyn wirtualnych na serwerach o najmniejszym obciążeniu,
5. oprogramowanie wirtualizacyjne musi posiadać mechanizm Affinity Rules,
6. oprogramowanie wirtualizacyjne musi umożliwiać tworzenie i zarządzanie wirtualnymi sieciami,
7. oprogramowanie wirtualizacyjne musi automatycznie przenosić bezprzerwowo maszyny wirtualne pomiędzy węzłami w klastrze w zależności od ich obciążenia,
8. oprogramowanie wirtualizacyjne musi być w pełni zintegrowane z dostarczoną platformą chmury prywatnej i posiadać wspólną konsole zarządzania,
9. oprogramowanie wirtualizacyjne musi posiadać mechanizmy klonowania maszyn wirtualnych. Klonowanie maszyn wirtualnych musi integrować się z podsystem dyskowym w celu szybkiego wykonywania klonów,
10. oprogramowanie wirtualizacyjne musi posiadać wirtualny przełącznik sieciowy, umożliwiający konfigurację ustawień sieci per klaster,
11. oprogramowanie wirtualizacyjne musi wspierać UEFI dla maszyn wirtualnych,
12. oprogramowanie wirtualizacyjne musi wspierać karty GPU,

**Podsystem serwerowy**

1. system musi być łącznie wyposażony w 6 procesorów 8-rdzeniowych klasy high-end posiadających wynik min 19 000 w benchmarku PassMark - CPU Mark znajdującym się na stronie internetowej <http://www.cpubenchmark.net/high_end_cpus.html>,
2. system musi być łącznie wyposażony w minimum 1152 GB pamięci RAM,
3. system musi być łącznie wyposażony w dyski SSD o łącznej pojemności min. 45 TB.
4. system musi być łącznie wyposażony w minimum 12 portów 10Gb Ethernet SFP+ wraz z kablami o długości min. 1,5 metra,
5. system musi być wyposażony w minimum 3 porty o prędkości minimum 10/100 Base-T Ethernet do zarządzania IPMI,
6. zamawiający wymaga aby rozbudowa systemu była liniowa.

**Oprogramowanie systemowe**

1. Microsoft Windows Server 2022 Datacenter na min. 48 rdzeni CPU z licencją wieczystą dla oferowanej konfiguracji serwerów modułowych lub równoważne,
2. licencja ma umożliwiać downgrade do wcześniejszej wersji licencji (2016, 2012 R2) oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń,
3. oprogramowanie równoważne musi charakteryzować się:
4. licencją wieczystą i nie narażającą Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu,
5. Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i nielimitowanej liczby wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji,
6. serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy:
* posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM dla jednego modułu serwerowego w środowisku fizycznym,
* posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny dla jednego modułu serwerowego,
* posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.
* posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci,
* posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,
* posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,
* posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,
* posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
1. wbudowane wsparcie instalacji i pracy na wolumenach, które:
* pozwala na zmianę rozmiaru w czasie pracy systemu,
* umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
* umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, umożliwiają zdefiniowanie list kontroli dostępu (ACL),
1. posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,
2. posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji,
3. posiada możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,
4. posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,
5. posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,
6. graficzny interfejs użytkownika,
7. zlokalizowane w języku polskim, następujące elementy:
* menu,
* przeglądarka internetowa,
* pomoc,
* komunikaty systemowe.
1. posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),
2. posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,
3. dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,
4. pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management),
5. posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
* podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
* usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
* podłączenie SSO 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,
* zdalna dystrybucja oprogramowania na stacje robocze,
* praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,
* Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
* dystrybucję certyfikatów poprzez http,
* konsolidację CA dla wielu lasów domeny,
* automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen,
* szyfrowanie plików i folderów,
* szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),
* posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów,
* serwis udostępniania stron WWW.
* wsparcie dla protokołu IP w wersji 6 (IPv6),
* wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
* wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają 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,
* posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)
* posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
1. wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),
2. posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,
3. posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,
4. posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

**Serwis gwarancyjny**

1. wymagany jest serwis gwarancyjny dla Systemu świadczony przez minimum 5 lata,
2. wymagany jest dostęp bezpośredni do Centrum serwisowego producenta rozwiązania poprzez: email, web, telefon,
3. dostępność serwisu 24 godz. x 7 dni x 365 dni,
4. serwis musi wspierać w rozwiązywanie problemów ze sprzętem i oprogramowaniem Systemu oraz z dostarczonym wirtualizatorem,
5. wymiana uszkodzonych podzespołów – NBD od momentu potwierdzenia usterki,
6. dostęp do poprawek (patch, hotfix, update) i nowych wersji oprogramowania (upgrade) w ramach wykupionego serwisu gwarancyjnego przez okres 3 lat.

**Usługi wdrożeniowe**

1. w zakresie infrastruktury sieciowej Wykonawca musi wykonać następujące prace:
2. analiza środowiska sieciowego Zamawiającego, wizja lokalna,
3. projekt techniczny,
4. montaż przełączników w szafie rack, podłączenie zasilania, podłączenie okablowania zgodnie z wykonanym wcześniej projektem technicznym,
5. w zakresie konfiguracji przełączników sieciowych:
6. aktualizacja firmware urządzeń,
7. konfiguracja stosu przełączników oraz agregacja połączeń,
8. konfiguracja dostępu zdalnego,
9. konfiguracja stp, vlanów,
10. implementacja adresacji IP oraz routingu,
11. w zakresie konfiguracji firewalli:
12. aktualizacja firmware,
13. implementacja klastra HA,
14. konfiguracja dostępu zdalnego,
15. konfiguracja interfejsów,
16. konfiguracja stref oraz polityk bezpieczeństwa,
17. konfiguracja NAT oraz styku z siecią Internet,
18. włączenie funkcjonalności AV/IPS/URL Filtering,
19. konfiguracja L2TP/SSL VPN w celu dostępu zdalnego,
20. dokumentacja powykonawcza,
21. instruktaż powdrożeniowy z obsługi dostarczonych rozwiązań,
22. w zakresie infrastruktury hiperkonwergentnej:
23. instalacja rozwiązania w szafie rack Zamawiającego,
24. podłączenie okablowania sieciowego do dostarczonego rozwiązania,
25. podłączenie rozwiązania do zasilania energetycznego,
26. wykonanie pełnej inicjalizacji klastra w tym:
* wykonanie konfiguracji HA,
* wykonanie konfiguracji sieciowej,
* wykonanie konfiguracji dyskowej,
* konfiguracja powiadomień,
* dodanie użytkowników oraz uprawień,
* aktualizacja software oraz firmware,
* migracja maszyn wirtualnych z obecnie posiadanego środowiska Hyper-V;
* weryfikacja poprawności działania środowiska,
* przygotowanie dokumentacji;

Zamawiający wymaga aby dostarczone rozwiązanie było w pełni redundantne i kompletne, jeżeli do spełnienia wymagań, wymagane są dodatkowe licencje lub komponenty należy je dostarczyć. Wykonawca zapewni jednego inżyniera posiadającego certyfikat o jeden niższy od maksymalnego możliwego certyfikatu u danego producenta oferowanego rozwiązania.

1. **System backupu**

Pojęcie system backupu wskazuje na rozwiązanie zabezpieczające dane stanowiące jedno, spójne rozwiązanie, zarządzane z poziomu jednej konsoli. Nie dopuszcza się rozwiązań pochodzących od różnych producentów, a co za tym idzie nie całkowicie zintegrowanych pomiędzy sobą, wymagających wykorzystywania różnych konsol dla zarządzania czy konfiguracji. Zamawiający rozumie archiwizację danych, jako proces przenoszenia zasobów plikowych lub pocztowych do archiwum (repozytorium dyskowe lub taśmowe) po skopiowaniu tych zasobów system musi tworzyć skróty oraz kasować zarchiwizowane dane. Obie funkcjonalności: kasowanie danych i tworzenie skrótów musi być dostępne co najmniej dla archiwizowanych danych plikowych i maili z systemów Exchange Onpremis i Exchange Online. Jeśli przy danym punkcie wymogu występuje informacja „jako opcja” oznacza to, iż zaproponowany system posiada daną funkcjonalność, a jej uruchomienie może wymagać zakupu dodatkowych licencji – Zamawiający nie oczekuje oferty na nią a jedynie chce mieć możliwość w przyszłości rozbudowy o tę funkcjonalność. W celu weryfikacji funkcjonalności oferowanych przez proponowany system, Zamawiający zastrzega sobie możliwość wezwania do przeprowadzenia wybranych testów funkcjonalnych potwierdzających zadeklarowane funkcjonalności w ciągu 5 dni od daty wezwania. W razie odmowy przeprowadzenia testów lub ich wyniku negatywnego - pozwala Zamawiającemu odrzucić proponowaną ofertę bez podania przyczyny.

Wymogi podstawowe

1. rozwiązanie musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer medialny oraz klient), taka architektura pozwoli na elastyczną skalowalność rozwiązania bez względu na dynamikę przyrostu danych,
2. oprogramowanie nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest aby funkcjonalności związane z zabezpieczaniem i archiwizacją danych były w jakikolwiek sposób związane czy zależne od konkretnego typu czy producenta urządzenia,
3. jeśli system korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go: na serwerze fizyczny (minimum 2xCPU po 8 core), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware i Hyper-V,
4. licencje muszą pozwalać na stworzenie dla serwera zarządzającego rozwiązania wysokodostępnego z czasem przełączenia nie dłuższym niż 15 minut. Jeśli do stworzenia takowego rozwiązania potrzebne są licencje replikacyjne, klastrowe, współdzielona przestrzeń dyskowa to muszą zostać zaoferowane. Licencje muszą pozwalać na skonfigurowanie serwerów zarządzających oraz ich replikację dla co najmniej trzech lokalizacji, gdzie pierwsza jest lokalizacją produkcyjną, druga i trzecia są typu standby dla serwera zarządzającego,
5. przełączenie serwera zarządzającego musi odbywać się w pełni automatycznie poprzez administratora, który decyduje kiedy ma ono nastąpić, przełączanie serwera zarządzającego musi być możliwe pomiędzy różnymi typami infrastruktury:
* serwer fizyczny -> serwer fizyczny
* serwer fizyczny -> serwer wirtualny (onpremis)
* serwer fizyczny -> serwer wirtualny (AWS, Azure, Google)
* serwer wirtualny (onpremis) -> serwer fizyczny
* serwer wirtualny (onpremis) -> serwer wirtualny (onpremis)
* serwer wirtualny (onpremis) -> serwer wirtualny (AWS, Azure, Google)
1. rozwiązanie musi zapewnić interfejs graficzny do zarządzania i instalacji,
2. oprogramowanie musi umożliwiać zdalne instalowanie i odinstalowywanie klienta systemu z centralnego serwera dla systemów Windows, Linux, Unix oraz Macintosh – musi być to możliwe z jednego serwera pełniącego rolę cache dla wszystkich binarii klienckich,
3. system musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii bezpieczeństwa i archiwów,
4. system musi posiadać możliwość nieodwracalnego kasowania danych – funkcjonalność ta musi być częścią oprogramowania,
5. dla dowolnego transferu danych z klienta musi istnieć możliwość definiowania/ograniczania pasma dla transferu danych – funkcjonalność ta musi być dostępna także przy włączonej deduplikacji na kliencie,
6. system musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego. Składowane dane na taśmach muszą być w formie nie zdeduplikowanej (nawodnione) po to by była możliwość odtwarzania ich bezpośrednio, a więc bez konieczności pośrednictwa dysków, buforów czy importu,
7. system musi pozwalać na zarządzanie całością działania systemu (backup, archiwizacja, backup laptopów, backup desktopów) z jednej konsoli administracyjnej oraz także z konsoli webowej,
8. agenci systemu muszą posiadać funkcjonalność komunikowania się poprzez jeden port TCP/IP, celem zabezpieczenia komunikacji z środowisk typu DMZ,
9. automatyczne tunelowanie komunikacji TCP/IP pomiędzy agentami systemu – jeśli agent systemu wykryje ograniczenia w komunikacji, wtenczas automatycznie zestawia połączenie tunelowe,
10. system musi umożliwiać konfigurację, którymi kartami sieciowymi ma przebiegać komunikacja i transfer danych, wybór interface musi odbywać się co najmniej poprzez nazwę domeny, subnet, zakres IP,
11. komunikacja agentów systemu z serwerami musi odbywać się poprzez SSL – konfiguracja tego typu transferu nie może powodować konieczności instalowania dodatkowego oprogramowania,
12. system musi pozwalać na współdzielenie napędów taśmowych w środowisku sieci SAN,
13. system musi umożliwić przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie systemu na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta. Pojedynczy serwer systemu musi umożliwiać przechowywanie danych po deduplikacji minimum do 500 TB (rozbudowa do tej wielkości może nastąpić tylko poprzez dodanie dodatkowej przestrzeni do składowania danych poprzez dodanie dysków, półki dyskowej a nie przez wymianę urządzenia),
14. włączenie funkcjonalności deduplikacji na kliencie musi być możliwe dla różnych systemów operacyjnych: Windows, Linux, Unix i Macintosh,
15. logiczna globalna deduplikacja – system musi oferować deduplikację globalną co oznacza iż niezależnie z jakich klientów dane będą deduplikowane (serwery fizyczne, hosty wirtualne, bazy i aplikację) – deduplikacja musi opierać się na jednej logicznej centralnej bazie deduplikacyjnej,
16. włączenie funkcjonalności deduplikacji nie może generować wymogu instalacji dodatkowych modułów programowych po stronie klienckiej lub serwera systemu. Niedopuszczalne jest łączenie systemu z dodatkowym oprogramowaniem czy sprzętem (appliance) dla uzyskania funkcjonalności deduplikacji danych,
17. deduplikacja blokowa musi obejmować dane nie tylko backupowane ale i archiwizowane, przy czym wielkość bloku nie może być większa niż 128KB,
18. system musi zapewniać wspólny stopień deduplikacji (jedna baza deduplikacyjna) dla danych czy to z backupu czy archiwizacji,
19. system musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych (dla dowolnych danych: czy to z procesu backupu czy archiwizacji). A więc replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu systemu,
20. proces przesyłania danych (replikacji) na inny serwer systemu celem tworzenia dodatkowej kopii danych nie może być zależny od warstwy sprzętowej, a więc dowolny producent serwera, dowolny producent macierzy/półki dyskowej,
21. system musi pozwalać na instalację bazy deduplikacyjnej w układzie wysokiej dostępności (minimum na dwóch serwerach) w taki sposób aby awaria pojedynczego serwera nie powodowała utraty możliwości backupu z deduplikacją i odtwarzania wcześniejszych kopii danych,
22. system musi pozwalać na odtwarzanie zdeduplikowanych danych nawet w momencie, gdy baza deduplikacyjna jest niedostępna. Proces odtwarzania (nawadniania) zdeduplikowanych danych nie korzysta z bazy deduplikacyjnej,
23. na jednym serwerze systemu (na jednej instancji systemu operacyjnego) musi być zainstalowane minimum dwie bazy deduplikacyjne pozwalające zwiększyć skalowalność systemu,
24. system musi zapewniać dostęp zintegrowany z usługą katalogową, minimum to Active Directory, a więc tak zwany „single sign on” – pojedyncze logowanie: użytkownik po zalogowaniu do domeny AD, nie potrzebuje wykonywać następnego logowania aby zarządzać systemem poprzez konsolę administracyjną,
25. system musi zapewniać zintegrowane logowanie dla użytkownika końcowego poprzez tzw. social media (minimum poprzez Google),
26. system musi zapewniać elastyczne delegowanie uprawnień oraz audytowanie działań użytkowników. Z tym, że delegowanie uprawnień musi pozwalać na przydział uprawnień per serwer czy grupa serwerów, przydział uprawnień musi pozwalać na definiowanie uprawnień dla grup użytkowników z domeny AD,
27. system musi pozwalać na zarządzanie poprzez „cmd” z tym, że uruchomienie jakiejkolwiek komendy/polecenia musi zostać poprzedzone koniecznością zalogowania (autentyfikacji) do systemu, funkcjonalność musi dotyczyć dowolnej platformy (minimum Windows/Linux) i nie może polegać na konieczności instalowania czy konfigurowania dodatkowych komponentów np. SSH,
28. komunikacja pomiędzy agentem a serwerem systemu musi opierać się na certyfikatach,
29. system musi posiadać funkcjonalność blokowania danych do odczytu dla administratora, to znaczy, że administrator systemu nawet mając pełne uprawnienia nie może odtworzyć danych, jeśli nie jest ich właścicielem, funkcjonalność ta musi być dostępna nie tylko dla danych z laptopów/desktopów ale i dla serwerów (także dla danych plikowych i bazodanowych),
30. system musi pozwalać na skonfigurowanie mechanizmu podwójnej autentyfikacji administratora – do uruchomienia konsoli administracyjnej systemu potrzebne jest nie tylko logowanie, ale i dodatkowy tymczasowy kod wysyłany do administratora np. poprzez mail,
31. szyfrowanie danych musi pozwalać na wybór algorytmu (minimum dwa algorytmy: Blowfish, AES) także dla danych deduplikowanych na kliencie systemu,
32. możliwość szyfrowania musi pozwalać na elastyczny wybór miejsca szyfrowania: szyfrowanie danych na kliencie, szyfrowanie danych na serwerze backupowym i szyfrowanie tylko transmisji pomiędzy klientem backupowym a serwerem,
33. system musi wspierać mechanizm szyfrowania danych na napędach taśmowych LTO,
34. system musi pozwalać na ustawianie haseł dostępu do nośników tzw: media password,
35. system musi pozwalać na integrację z zewnętrznymi repozytoriami do przechowywania kluczy szyfrujących – minimum dla:
* Safenet
* Amazon Web Services (AWS) key management service
* Microsoft Azure Key Vault,
1. system musi umożliwiać składowanie kopii bazy katalogowej w chmurze producenta oprogramowania, funkcjonalność ta musi być w cenie produktu i pozwalać na automatyczne składowanie kopii bazy,
2. system musi mieć wbudowane mechanizmy zabezpieczające przed złośliwym oprogramowaniem (Ransomware), minimum to:
* zabezpieczenie ścieżek dostępu do danych składowanych (kopii backupowych) na dyskach – tylko procesy systemu mogą zapisywać i modyfikować dane,
* monitorowanie nietypowych aktywności na serwerach za pomocą np. metody: Honeypot,
* monitorowanie nietypowych aktywności na serwerach plikowych i desktopach, monitorowanie musi odbywać się nie rzadziej, niż co 5 minut i każdy niestandardowy wynik jest automatycznie wysyłany w postaci alertu lub notyfikacji,
* Air Gap (izolowanie i segmentowanie składowanych kopii backupowych) – musi polegać na wbudowanym automatycznym mechanizmie wyłączania komunikacji pomiędzy pozostałymi komponentami systemu backupowego. Tak więc komunikacja z wybranym segmentem środowiska backupowego odbywa się tylko w określonym przedziale czasowym dla potrzeb replikacji kopii backupowych, natomiast przez pozostały czas żadne procesy systemu backupowego nie mają możliwości komunikacji z tym środowiskiem,
* możliwość definiowania serwerów komunikacyjnych (tzw. bram/gateway) przez które wykonywana jest komunikacja pomiędzy modułami systemu backupowego, w szczególności pomiędzy serwerem zarządzającym a serwerem medii czy serwerem z dowolnym agentem backupowym,
* możliwość definiowania kierunków inicjalizowania komunikacji sieciowej pomiędzy komponentami systemu backupowego,
* możliwość zablokowania zmiany retencji (czas przechowywania kopii backupowych) na krótszą dla kopii backupowych składowanych na dowolnych typach nośników w tym na dyskach i taśmach,
1. system musi posiadać rozbudowany system powiadamiania o zdarzeniach poprzez email,
2. system musi automatycznie wysyłać informacje o alertach, zdarzeniach oraz informacjach audytowych do syslog serwera,
3. automatyczne monitorowanie stanu systemu poprzez wiadomości SMS na urządzeniach mobilnych i telefonach,
4. system musi posiadać rozbudowany system raportowania dla administratorów, minimalny zestaw dostępnych raportów to:
* raport zmian/wzrostu środowiska systemu
* raport wykorzystania licencji
* raport wykonanych zadań backupowych
1. system musi mieć możliwość automatycznego wysyłania dowolnych raportów do wybranych użytkowników poprzez mail
2. system musi mieć możliwość automatycznego zapisywania raportów w formacie minimum: PDF, HTML i CSV,
3. system musi pozwalać na definiowanie alertów per zadanie backupowe lub zadanie odtwarzania danych przy spełnieniu minimum kryteriów:
* czas zadania dłuższy niż zadany
* ilość danych większa niż ….
* ilość danych mniejsza niż ….
* ilość nie zbackupowanych plików większa niż
* ilośc nie zbackupowanych plików większa niż …%
* wielkośc backupowanych danych wieksza niż …
1. notyfikacje alertów muszą być wysyłane minimum poprzez mail,
2. raport spełnienia wymogów SLA dla parametrów:
* ilości dodatkowych kopii backupowych,
* RTO
* RPO
1. system musi zapewniać funkcjonalność wznawiania zadań backupowych,
2. system musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanych – inline copy (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywania danych,
3. system musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami – tzw. multistreaming. Polega ona na tym, iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe. Funkcjonalność ta musi być dostępna dla dowolnych typów danych: backup plikowy, bazodanowy,
4. funkcjonalność multistreamingu musi być dostępna dla deduplikacji bez względu czy następuje na kliencie czy na serwerze systemu,
5. system musi zapewniać funkcjonalność multipleksowania kilku strumieni danych na nośniku taśmowym – tzw. multiplexing. Wydajny zapis wielu strumieni danych na taśmy bez pośrednictwa dysków,
6. rozwiązanie musi posiadać możliwość wykonywania backupu pełnego, przyrostowego, różnicowego oraz syntetycznego,
7. system musi oferować funkcjonalność backupu blokowego, polegającego na tym, iż agent buduje własną bazę zmian bloków danych, przez co backup przyrostowy nie wymaga odczytu całych plików tylko zmienionych bloków wielokrotnie przyspieszając backup. Funkcjonalność ta musi być dostępna dla backupu danych plikowych,
8. system musi posiadać funkcję szyfrowania i kompresji danych transmitowanych przez LAN, możliwość wykorzystania szyfrowania i kompresji musi być dostępna w dowolnej kombinacji,
9. system ma realizować procesy backupu oraz odzyskiwania danych, procesy te muszą być uruchamiane ręcznie i poprzez wbudowany kalendarz, możliwość definiowania zadań poprzez wbudowany w system kalendarz musi być możliwa nie tylko dla zadań backupowych ale także dla zadań odtwarzania danych a więc restore,
10. system musi dla backupu środowiska AWS oferować:
* bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików,
* możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym,
* możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej EC2,
* możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją,
* możliwość wykonywania jednoprzebiegowego konsystentnego backupu maszyn wirtualnych EC2, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory,
* backup i odtwarzanie danych z baz danych RDS: MS SQL, MySQL, PostgreSQL, Firebird oraz Oracle (eksport danych na storage backupowy),
* możliwość wykonywania snapshotów baz danych AWS RDS: Aurora, MariaDB, Microsoft SQL Server, MySQL, PostgreSQL, Firebird,
* backup oraz odtwarzanie danych składowanych w usłudze S3, EFS oraz FSx,
* możliwość zapisu danych zdeduplikowanych bezpośrednio w usłudze S3, bez konieczności używania dodatkowego cache’u oraz rozwiązań typu appliance,
* możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych EC2, na których zainstalowano oprogramowanie serwera backupowego,
* możliwość konwersji maszyn wirtualnych Microsoft Hyper-V, Vmware oraz Azure do maszyn wirtualnych EC2,
* możliwość konwersji maszyn wirtualnych EC2 do maszyn typu Vmware oraz Azure,
* możliwość wykonywania backupu usługi AWS DynamoDB,
* możliwość backupu środowiska VMWare Cloud on AWS,
* możliwość automatycznego wyłączania i włączania serwerów backupowych,
* możliwość automatycznej replikacji maszyn wirtualnych Vmware do AWS EC2,
* możliwość wykorzystania EBS Direct Read API w czasie backupu maszyn wirtualnych EC2,
* możliwość integracji z AWS KMS w celu zarządzania kluczami szyfrującymi,
* możliwość backupu maszyn wirtualnych EC2 z innego konta Amazon (Cross-account backup),
* możliwość migracji zdeduplikowanych danych do chmury AWS za pomocą urządzenia Snowball,
* możliwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP HANA, Microsoft SQL Server, DB2, MongoDB, MySQL, PostgreSQL oraz pliki na systemach Windows oraz Linux,
1. system musi dla backupu środowiska Azure oferować:
* bezagentowy backup całych maszyn wirtualnych Azure VM i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików,
* możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym,
* możliwość odtworzenia pojedynczego dysku wirtualnej maszyny i podłączenie go do innej maszyny wirtualnej w Azure VM,
* możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją,
* możliwość wykonywania jednoprzebiegowego konsystentnego backupu maszyn wirtualnych Azure VM, na których pracują systemy Microsoft Exchange, Microsoft Sharepoint, Microsoft SQL Server, MySQL, Oracle lub Active Directory,
* backup i odtwarzanie danych z baz danych (PaaS): MS SQL, MySQL, PostgreSQL, Firebird (eksport danych na storage backupowy),
* backup oraz odtwarzanie danych składowanych w Azure Blob oraz Azure File Shares oraz Azure Data Lake Storage Gen2,
* możliwość zapisu danych zdeduplikowanych bezpośrednio na Azure Blob Storage, bez konieczności używania dodatkowego cache’u oraz rozwiązań typu appliance,
* możliwość automatycznego włączania oraz wyłączania maszyn wirtualnych Azure, na których zainstalowano oprogramowanie serwera backupowego,
* możlwość wykonywania konsystentnych snapshotów dysków wirtualnych podłączonych do maszyn wirtualnych Azure VM, na których składowane są dane systemów Oracle, SAP for Oracle, SAP HANA, Microsoft SQL Server, DB2 oraz pliki na systemach Windows oraz Linux,
* możliwość migracji zdeduplikowanych danych do chmury Azure za pomocą Azure Data Box,
* możliwość automatycznego wyłączania i włączania serwerów backupowych,
* możliwość integracji z Azure Key Vault w celu zarządzania kluczami szyfrującymi,
* możliwość automatycznej replikacji maszyn wirtualnych Hyper-V i Vmware do Azure,
* możliwość automatycznej replikacji maszyn wirtualnych Azure pomiędzy regionami,
* możliwość backupu bazy danych Cosmos DB (Core SQL API),
* możliwość konwersji backupu systemu operacyjnego Windows wraz z danymi do maszyny wirtualnej Azure,
* możliwość backupu Azure DevOps and GitHub,
1. System musi dla backupu środowiska GCP oferować:
* bezagentowy backup całych maszyn wirtualnych i ich odtwarzanie wraz z odtwarzaniem pojedynczych plików,
* możliwość zapisu backupu maszyn wirtualnych na dowolnym nośniku backupowym,
* możliwość wykonywania migawek (snapshotów) wirtualnych maszyn i automatyczne zarządzanie ich retencją,
* backup i odtwarzanie danych z baz danych Cloud SQL: MySQL, PostgreSQL oraz Firebird (eksport danych na dowolny storage backupowy),
* backup oraz odtwarzanie danych składowanych w usłudze GCP Cloud Storage,
* możliwość zapisu danych zdeduplikowanych bezpośrednio w usłudze GCP Cloud Storage, bez konieczności używania dodatkowego cache’u oraz rozwiązań typu appliance,
1. system musi posiadać (jako opcja) zintegrowane w systemie mechanizmy indeksowania pełnokontekstowego i wyszukiwania danych. Indeksowaniu powinny podlegać dane zbackupowane i zarchiwizowane już znajdujące się w systemie,
2. system musi realizować funkcjonalność weryfikacji wykonanych kopii,
3. system powinien umożliwiać wykorzystanie funkcjonalności Bare Metal Restore dla odtwarzania systemu po awarii, wsparcie musi być dostępne dla systemów:
* Windows,
* Linux: Debian/Oracle Linux/RHEL/CentOs/SuSe/Ubuntu,
* Unix: AIX,
* OpenVMS,
1. system musi umożliwiać integrację z mechanizmami kopii migawkowych czołowych producentów pamięci masowych minimum: HDS, Dell, HP, NetApp, EMC, IBM, Pure Storage, Nimble Storage, Tintri, Kaminario, z tym że takowy backup sterowany przez system a wykonywany przez daną macierz dyskową musi być dostępny nie tylko dla zasobów plikowych ale i aplikacji,
2. dla producentów: NetApp, EMC i HDS system musi umożliwiać nie tylko integrację z mechanizmami tworzenia kopii migawkowych (tzw. Snapshot) ale musi integrować się także z mechanizmami replikacyjnymi, a więc sterować replikami wykonywanymi przez macierze,
3. system musi posiadać możliwość wykonywania kopii oraz archiwów na urządzenia dyskowe i taśmowe,
4. system powinien umożliwiać (jako opcja) obsługę urządzeń składowania danych w chmurze, minimum: Azure, Amazon, Google Cloud, jeśli do włączenia tej funkcjonalności potrzebne są jakieś dodatkowe komponenty to muszą być zaoferowane,
5. system musi umożliwiać odtwarzanie danych plikowych pomiędzy systemami operacyjnymi np. odtwarzanie danych plikowych Linux na systemie Windows,
6. system musi pozwalać na odtwarzanie tylko samych uprawnień do plików,
7. system musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL),
8. system (jako opcja) powinien umożliwiać analizę logów z systemów zewnętrznych, na bazie zdefiniowanych kryteriów powinien generować alarmy lub akcje. Minimalne wsparcie to: Windows Event Log,
9. możliwość (jako opcja) odtwarzania backupów plikowych poprzez udostepnienia CIFS lub NFS. A więc dostęp do zbackupowanych danych widocznych jako udostępnione przez sieć zasoby CIFS/NFS,
10. system musi posiadać wbudowany mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux,
11. system musi wspierać wykonanie kopii na systemach klasy Windows, Linux i Unix,
12. system musi posiadać szerokie wsparcie dla środowisk Linux, minimum: RHEL, SuSe, Debian, Fedora, Gentoo, Mandriva, Oracle Linux, Red Flag Linux, Scientific Linux, Ubuntu, Slackware,
13. system musi posiadać szerokie wsparcie dla środowisk Unix, minimum: AIX, FreeBSD, HP-UX, Solaris,
14. system musi umożliwiać uruchamianie skryptów przed i po backupie, z tym iż musi posiadać mechanizm definiowania konta użytkownika na którym te skrypty byłyby uruchamiane. Mechanizm ten musi być centralnie zarządzany poprzez konsolę administracyjną. Niedopuszczalna jest konieczność np. zmiany konta serwisowego dla danego agenta – konta serwisowe muszą być centralnie definiowane i zarządzane.
15. system musi wspierać backup całym maszyn wirtualnych/kontenerów dla czołowych rozwiązań wirtualizacyjnych, kontenerowych i chmurowych:
* Alibaba Cloud (only in Command Center - streaming only),
* Amazon (streaming and IntelliSnap),
* Citrix Xen (streaming only),
* Google Cloud Platform (streaming and IntelliSnap),
* Huawei FusionCompute (streaming only),
* Microsoft Azure (streaming and IntelliSnap),
* Microsoft Azure Stack Hub (streaming and IntelliSnap),
* Microsoft Azure Stack HCI (only in Command Center - streaming only),
* Microsoft Hyper-V (streaming and IntelliSnap),
* Kubernetes (only in Command Center - streaming only),
* Nutanix Acropolis Hypervisor (AHV) (streaming and IntelliSnap),
* OpenStack (streaming only),
* Oracle Cloud Classic (streaming only),
* Oracle Cloud Infrastructure (only in Command Center - streaming only),
* Oracle VM (streaming only),
* Red Hat Virtualization (streaming only),
* vCloud Director (streaming only),
* VMware (streaming and IntelliSnap),

To znaczy musi posiadać dedykowany komponent do backupu minimum całej maszyny wirtualnej/kontenera/aplikacji/wolumenu bez konieczności instalowania agenta wewnątrz np. maszyny z możliwością granualnego odtwarzania pojedynczych plików,

1. system musi wspierać wersje środowisk VMware 5.1.x, 5.5, 5.5.1, 5.5.2, 5.5.3, 6.0, 6.0.1, 6.5, 6.7, 7.0 poprzez integrację z vStorage API,
2. dla backupu i odtwarzania środowisk wirtualnych opartych o Vmware musi być możliwość wyboru różnych transportów: SAN, Hot-add, NBD, SSL, NAS - gdzie transport NAS pozwala na bezpośredni odczyt i zapis danych maszyny wirtualnej z urządzenia NAS,
3. system musi wspierać środowisko Hyper-V dla:
* Microsoft Windows Server 2012 R2,
* Microsoft Hyper-V Server 2012 R2,
* Microsoft Windows Server 2016 (z Core Edition),
* Microsoft Hyper-V Server 2016 (z Core Edition),
* Microsoft Windows Server, version 1709 (z Core Edition),
* Microsoft Hyper-V Server, version 1709 (z Core Edition),
* Microsoft Windows Server 2019 (z Core Edition),
* Microsoft Hyper-V Server 2019 (z Core Edition),
* Microsoft Windows Server 2022 (z Core Edition),
* Microsoft Hyper-V Server 2022 (z Core Edition),
1. system musi zapewniać automatyczne wykrywanie i dodawanie do polityki backupu nowych maszyn wirtualnych,
2. system musi umożliwiać odzyskanie i uruchomienie maszyn wirtualnych z kopii zapasowej bez oczekiwania na pełne przywrócenie maszyny wirtualnej minimum dla Vmware i Hyper-V,
3. system musi umożliwiać konwertowanie maszyn wirtualnych pomiędzy wirtualizatorami, minimum:
* Vmware do: Hyper-V, Azure, Amazon, Google Cloud Platform, Openstack, Oracle Cloud Infrastructure,
* Hyper-V do: Azure, Amazon, Vmware,
* Amazon do: Azure, Vmware,
* Azure do: Amazon, Hyper-V, Vmware,
1. system musi wspierać mechanizm CBT (change block tracking) minimum dla Vmware i Hyper-V,
2. system musi umożliwiać konwersję zbackupowanego serwera Windows i Linux do maszyny wirtualnej w środowisku:
* Hyper-V,
* Vmware,
1. możliwość (jako opcja) synchronizacji maszyn wirtualnych Vmware do środowiska Amazon, Azure,
2. system musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL, Postgress, Oracle, Informix, Firebird na dowolnej platformie systemu operacyjnego (Windows/Linux/Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywać się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisu na dany nośnik,
3. system musi umożliwiać wykonanie kopii na gorąco bazy danych MS SQL, Oracle, MySQL, Postgress, DB2, Informix, Firebird. Konfiguracja agenta nie może powodować konieczności tworzenia skryptów uruchamianych po stronie klienta niezależnie czy jest to serwer fizyczny czy wirtualny. Brak skryptów musi dotyczyć dowolnych typów backupów: backup automatyczny uruchamiany poprzez harmonogram, backup manualny,
4. odtwarzanie danych z backupu bazodanowego (MS SQL, Oracle, MySQL, Postgress, DB2, Informix) musi odbywać się poprzez konsolę administracyjną bez konieczności konfigurowania skryptów,
5. dla silników bazodanowych MS SQL, Oracle i SAP HANA musi istnieć mechanizm backupu logów tranzakcyjnych z częstotliwością co 1 minuta nawet w przypadku gdy serwer zarządzający systemem backupowym jest niedostępny,
6. konfiguracja agentów backupowych dla: MS SQL, Oracle, mySQL musi odbywać się poprzez interface graficzny, jakakolwiek modyfikacja zasobów do backupu (np. dodanie nowej bazy) nie może powodować konieczności modyfikacji skryptów czy to dla backupów planowanych czy wykonywanych na żądanie,
7. system musi umożliwiać wykonanie kopii na gorąco Active Directory a następnie odzyskania pojedynczych obiektów AD wraz z hasłami użytkowników,
8. system musi umożliwiać odtwarzanie backupu wykonywanego online dedykowanym agentem, do pliku celem późniejszego odtwarzania bez udziały systemu. Funkcjonalność ta musi być dostępna minimum dla MS SQL, Oracle i Exchange,
9. system musi umożliwiać wykonanie kopii na gorąco aplikacji MS Exchange a następnie odzyskania pojedynczych wiadomości. Dedykowany agent do backupu Exchange musi wspierać backup środowiska Exchange DAG poprzez nazwę DAG nawet w konfiguracji bez adresu IP,
10. system musi umożliwiać odtwarzanie pojedynczych tabel dla minimum: Oracle, DB2, PostgreSQL, MySQL, Informix, MS SQL, Firebird,
11. dla minimum mySQL i PostgresSQL musi istnieć mechanizm backupu z wykorzystaniem mechanizmu backupu blokowego,
12. automatyczny backup logów transakcyjnych dla baz danych w oparciu o procent wolnego miejsca na systemie plikowym, minimum dla: Oracle, SQL, Notes, SAP/Oracle,
13. dla MS SQL możliwość skonfigurowania rozszerzenia pozwalającego backupować i odtwarzać bazy bezpośrednio z konsoli Management Studio,
14. wsparcie dla backupu online dla minimum MS SQL Server 2022/2016/2014/2012/2008/2005,
15. dedykowany agent bazodanowy dla backupu MS SQL na platformie Linux: Ubuntu, SuSe, RHEL,
16. możliwość (jako opcja) archiwizacji danych z baz Oracle do plików XML,
17. odtwarzanie baz SAP opartej na silniku Oracle do pliku, a więc odtwarzanie backupu online na dysk (tzw. application free restore),
18. dedykowani agenci (jako opcja) do backupu systemów Big Data: Hadoop, Greenplum, GPFS, Splunk,
19. możliwość integracji kopii migawkowych dla backupu konsystentnego aplikacji i baz danych minimum: Vmware, Hyper-V, MS SQL, Exchange, mySQL, Oracle – zarządzanie kopiami migawkowymi musi odbywać się z konsoli administracyjnej systemu backupowego a integracja zarządzania nie może odbywać się na bazie skryptów,
20. możliwość backupu i odtwarzania (jako opcja) dedykowanym agentem dokumentów i maili dla Office 365 z:
* SharePoint Online,
* Exchange Online,
* OneDrive,
* Teams,
1. możliwość (jako opcja) pełnokontekstowego indeksowania i wyszukiwania treści z danych backupowanych (dokumenty i maile) z O365,
2. system musi zapewniać (jako opcja) backup laptopów i desktopów – funkcjonalność ta musi być w pełni zintegrowana z systemem (ta sama konsola, to samo repozytorium danych, ta sama deduplikacja) o funkcjonalnościach:
* dystem musi umożliwiać backup laptopów czy desktopów z systemami Windows, Linux i Macintosh,
* dostęp do danych zbackupowanych z laptopów czy desktopów musi być możliwy z urządzeń mobilnych poprzez dedykowanego klienta minimum dla IOS i Android,
* dla backupu laptopów i desktopów system backupowy musi oferować dedykowanego agenta, który pozwala skonfigurować zadanie backupowe tak by było wykonane w przedziale czasowym bez podawania konkretnej daty czy czasu jego uruchomienia, agent nie może tworzyć kopii danych na lokalnych zasobach stacji/laptopa,
* system musi zapewniać współdzielenie plików pochodzących z backupu laptopów i destopów z użytkownikami z domeny AD oraz z użytkownikami spoza domeny,
* system musi oferować możliwość synchronizacji wybranego katalogu/foldera z stacji roboczej celem automatycznego backupu danych w nim zapisanych (backup ciągły),
* każdy użytkownik desktopa czy laptopa musi posiadać możliwość zarządzania własnymi danymi, minimalna oczekiwana funkcjonalność to:
* odtwarzanie własnych danych,
* uruchomienie backupu,
* wstrzymanie backupu,
* możliwość zdefiniowania innego okna backupowego,
* możliwość monitorowania postępu działania zadania,
* możliwość przeglądania danych z stacji roboczej czy laptopa poprzez dedykowanego klienta dla urządzeń mobilnych, a więc użytkownik posiadając jedynie urządzenie mobilne może nie tylko odczytywać dane z backupowej kopii ale także przeglądać dane na stacji roboczej nawet w momencie gdy jest poza siedzibą firmy – korzysta jedynie z dostępu do Internetu (do przeglądania danych nie jest potrzebne żadne dodatkowe połączenie VPN),
* zabezpieczenie przed kradzieżą, system musi posiadać możliwość zdalnego zaszyfrowania danych w przypadku kradzieży laptopa, to znaczy iż w przypadku utraty urządzenia administrator lub użytkownik włącza opcję szyfrującą i jeśli urządzenie pojawi się w sieci wtenczas automatycznie dane zostaną zaszyfrowane,
* możliwość archiwizowania danych plikowych na stacji roboczej: jeśli dane pliki spełniają kryteria archiwizacyjne to dany pliki zostaje skasowany albo zamieniony na skrót (stub),
1. rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawiania znaczników (stub) na zasobach produkcyjnych (dla zasobów plikowych Windows\Linux\Unix) serwerów fizycznych, archiwizacja musi korzystać z tej samej architektury systemu co backup i korzystać z tego samego repozytorium danych,
2. system musi posiadać funkcjonalności archiwizacyjne (archiwizacja plikowa) takie jak:
* oprogramowanie musi wspierać archiwizację zgodnych z wyznaczonymi kryteriami danych z systemów produkcyjnych na inne tańsze pamięci masowe. Mechanizm ten pozwoli na zmniejszenie ilości danych na systemach produkcyjnych,
* oprogramowanie musi obsługiwać strategię wielowarstwowego aktywnego archiwum. Na przykład, umożliwiać przenoszenie zarchiwizowanych plików pomiędzy różnorodnymi urządzeniami pamięci masowej, w sposób zautomatyzowany przez politykę do wykonania krótko-, średnio- i długoterminowe okresów retencji, przy zachowaniu przejrzystego jedno- krokowego odzyskiwania dla użytkowników końcowych,
* oprogramowanie musi być zintegrowane z modułem do tworzenie kopii zapasowych w celu redukcji czasu okien backupowych przy zabezpieczaniu dużej ilości danych,
* oprogramowanie musi wspierać proces archiwizacji bezpośrednio na taśmy,
* oprogramowanie musi umożliwiać deduplikację danych archiwizowanych na poziomie bloków w celu redukcji ilości przestrzeni na dyskach fizycznych,
* oprogramowanie musi umożliwiać globalną deduplikację dla archiwizacji i kopii zapasowych w celu minimalizowania zużycia pamięci masowej,
* oprogramowanie musi zapewniać przezroczysty dostęp użytkowników do danych archiwalnych poprzez mechanizm skrótów,
1. system musi (jako opcja) umożliwiać rozbudowę o archiwizację poczty (minimum Exchange), archiwizacja poczty musi umożliwiać archiwizowanie maili z skrzynek pocztowych oraz archiwizowanie ruchu pocztowego (journaling oraz SMTP journaling),
2. oprogramowanie musi umożliwiać (jako opcja) pełnokontekstowo indeksować maile wraz z załącznikami oraz posiadać centralną konsolę do wyszukiwania danych i monitorowania zgodności z przepisami/normami bezpieczeństwa (compliance),
3. system musi umożliwiać (jako opcja) pełnokontekstowe indeksowania treści danych dla wybranych typów plików, indeksacja musi odbywać się dla danych znajdujących się już w systemie,
4. system musi umożliwiać (jako opcja) przeprowadzanie wielu wyszukiwań (eDiscovery) i zbierać wszystkie wyniki w jednej lokalizacji,
5. system musi oferować mechanizm składowania kopii backupowych (retencja danych) oparty o czas i cykle. Oznacza to iż kopia backupowa jest przechowywana w repozytorium przez określony czas (np. tydzień, miesiąc, rok….) a jej automatyczne skasowanie jest wykonane jeśli spełniony jest jednocześnie warunek ilości cykli a więc ilość backupów typu pełnego lub backupów syntetycznych znajdujących się w systemie,
6. musi istnieć dedykowany agent do backupu online aplikacji MongoDB,
7. system musi oferować integrację z mechanizmami deduplikacyjnymi urządzeń typu appliance minimalne wsparcie to Catalyst i urządzenie StoreOnce. Integracja z StoreOnce musi być dostępna nie tylko dla Windows ale także dla Unix i Linux,
8. system (jako opcja) musi oferować rozbudowę o funkcjonalność przeszukiwania i analizy zasobów plikowych dla maszyn wirtualnych (minimum Vmware) całość działać związanych musi odbywać się na kopiach backupowych maszyn wirtualnych a nie na środowisku produkcyjnym,
9. musi istnieć możliwość zarządzania systemem poprzez Windows PowerShell,
10. Agent do spójnego backupu bazy HBASE – backup pełny i przyrostowy,
11. Agent do backupu systemów plikowych: Lustre, GlusterFS,
12. wsparcie (jako opcja) dla replikacji maszyn wirtualnych Vmware z wykorzystaniem VIAO (VSphere APIs for I/O),
13. system musi zamierać moduł do monitorowania i zarządzania taśmami wynoszonymi z bibliotek taśmowych o funkcjonalnościami minimum:
* identyfikacja taśm, które muszą być wyciągnięte z biblioteki,
* identyfikacja taśm, które można z powrotem wstawić do biblioteki taśmowej,
* automatyczne przenoszenie taśm w bibliotece i notyfikacja administratorów,
* identyfikacja i monitorowanie nośników (taśm) w trakcie transportu,
1. monitorowanie i alertowanie klientów systemu, którzy są w trybie offline, a więc komunikacja z nimi przez system backupowy nie jest możliwa,
2. możliwość backupu (jako opcja) skrzynek pocztowych Google i dokumentów z Google Drive,
3. możliwość backupu baz Oracle bez instalacji oprogramowania backupowego natomiast dane zbackupowane muszą być składowane i zarządzane przez system backupowy,
4. system musi posiadać integrację z ServiceNow o funkcjonalnościach:
* dedykowany plugin do ServiceNow,
* możliwość zgłaszania zdarzeń backupowych i odtworzeniowych bezpośrednio z konsoli Service Now,
1. możliwość (jako opcja) rozbudowy środowiska o moduł VTL dla backupu danych po sieci SAN i LAN na dowolnym sprzęcie typu x86,
2. możliwość włączenia backupu pojedynczego pliku wieloma strumieniami,
3. możliwość zwiększenia bezpieczeństwa systemu poprzez integrację z CyberArk,
4. możliwość anonimizacji danych wrażliwych (data masking) w logach systemu wysyłanych np. do wsparcia,
5. wymogi dla licencjonowania:
* niedopuszczalne jest aby licencjonowanie było zależne od ilości składowanych danych (kopii backupowych) na dowolnych nośnikach (np. dysk, taśma VTL…) czy to z deduplikacją czy bez,
* niedopuszczalne jest aby licencjonowanie było zależne od ilości komponentów środowiska backupowego, które będą wykorzystywane w procesie backupu czy odtwarzania danych,
* niedopuszczalne jest aby licencjonowanie zależne było od ilości serwerów fizycznych czy ich mocy (ilości procesorów) niezależnie czy dane są z nich backupowane bezpośrednio czy tworzą platformę wirtualizacyjną, która jest backupowana,
* zaoferowane licencje nie mogą ograniczać wielkości przestrzeni do składowania danych czy replik ich do innych lokalizacji. Jakakolwiek rozbudowa przestrzeni dyskowej czy to w siedzibie podstawowej czy innej nie może wymagać zakupu jakichkolwiek licencji dla systemu,
* oferowana licencja oraz architektura systemu musi pozwalać na backup danych na:
* nielimitowaną ilość bibliotek taśmowych i napędów fizycznych,
* nielimitowaną przestrzeń w rozwiązaniach chmurowych (minimum: AWS, Azure, Google),
* w przypadku wielu lokalizacja licencja musi pozwalać na nielimitowaną replikację danych po deduplikacji pomiędzy lokalizacjami,
* do dostarczonych licencji jest wymagane 60 miesięczne wparcie producenta (pierwsza i druga linia wsparcia świadczona w języku polskim) zapewniające wsparcie techniczne w trybie dni roboczych oraz dostęp do bezpłatnych ewentualnych poprawek i uaktualnień. Oferowane wsparcie serwisowe musi być świadczone przez producenta rozwiązania lub autoryzowanego partnera serwisowego producenta na terenie Polski. W przypadku serwisu świadczonego przez autoryzowanego partnera serwisowego producenta na terenie Polski wymagane jest potwierdzenie jakości świadczonych usług poprzez certyfikat ISO 9001:2015 na świadczone usługi serwisowe,
* przez cały okres wsparcia dostarczać niezbędne poprawki i uaktualnienia,
* zaoferowane licencje na system muszą zapewnić backup danych z środowiska o wielkości min.:
* środowisko maszyn wirtualnych wraz z aplikacjami i bazami: ilość maszyn wirtualnych 20 sztuk,
* środowisko laptopów i desktopów w ilości 10 użytkowników,
1. Wykonawca w ramach systemu backupu zapewni:
* spotkanie projektowe – opracowanie wymagań platformy do backupu,
* opracowanie założeń hardware oraz software dotyczącego serwera platformy backup oraz chronionych komponentów,
* instalacja modułu centralnego zarządzania środowiskiem,
* konfigurację deduplikacji,
* konfigurację Storage oraz retencji,
* instalację serwerów proxy do backupu środowiska wirtualnego,
* konfigurację klienta do ochrony środowiska infrastruktury Klienta,
* instalację agentów do ochrony urządzeń końcowych (laptopów, desktopów) – maksymalnie 10 sztuk,
* konfigurację agentów plikowych,
* instalację agentów MS SQL Server do ochrony baz danych opartych na MS SQL Server – 1 sztuka (baza standalone),
* konfigurację agenta MS SQL Server,
* wykonanie pierwszych pełnych kopii zapasowych,
* wykonanie testowego odtworzenia trzech wskazanych maszyn wirtualnych,
* wykonanie testowego odtworzenia plików z jednego laptopa, desktopa,
* weryfikację poprawności wykonania kopii i ewentualne poprawienie konfiguracji,
* stworzenie dedykowanych haromonogramów ochrony danych,
* konfigurację alertów i raportów,
* konfigurację uprawnień dostępu do stworzonej platformy,
* wprowadzanie poprawek, performance oraz security tuning,
* zainstalowanie licencji,
* wykonanie dokumentacji technicznej przedstawiającej konfigurację platformy backup wraz z podstawowymi procedurami administracyjnymi,
* zapewni dwóch inżynierów z najwyższym certyfikatem technicznym u danego producenta oferowanego rozwiązania,
1. **Sprzęt sieciowy**

**Przełącznik sieciowy o poniższych parametrach – 2 szt. (minimalne wymagania)**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej,
2. Wymagane parametry fizyczne:
* możliwość montażu w stelażu/szafie 19”,
* wysokość maksymalna 1U,
* minimum jeden zasilacz 230V AC, moc zasilacza zapewniająca budżet mocy dla portów PoE minimum 380W,
* zakres temperatur pracy ciągłej co najmniej od 0°C do +45°C,
* zakres wilgotności pracy co najmniej 5% - 90%,
* port USB umożliwiający podłączenie zewnętrznej pamięci flash (gniazdo musi być dostępne od frontu urządzenia),
* waga urządzenia nie większa niż 3,5kg,
1. Przełącznik musi posiadać minimum:
* 24 porty 10/100/1000BASE-T PoE+ zgodnych z 802.3at oraz 802.3af,
* 4 porty 10GE SFP+

Wszystkie powyższe porty muszą być dostępne od frontu urządzenia,

1. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
* zarządzanie stosem poprzez jeden adres IP,
* do min. 9 jednostek w stosie,
* magistrala stackująca o wydajności minimum 40Gb/s,
* możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation),
* stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree,
* jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia,
* Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink 10G SFP+. W ramach niniejszego postępowania musi zostać dostarczony kabel producenta umożliwiający podłączenia urządzeń w stos, minimum 1m 10G SFP+,
1. Układ przełączający o wydajności min. 128 Gbps, wydajność przełączania przynajmniej 90 Mpps,
2. Obsługa min. 32 000 adresów MAC,
3. Wbudowana pamięć RAM min. 512MB, procesor minimum dwurdzeniowy,
4. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 512 MB,
5. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ),
6. Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie,
7. Obsługa ramek jumbo o wielkości min. 9216 bajtów,
8. Obsługa standardów IEEE:
* CFM zgodny z 802.1ag,
* EFM zgodny z 802.3ah,
1. Obsługa protokołu GVRP lub GARP,
2. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP,
3. Obsługa min. 4 000 tras dla routingu IPv4,
4. Obsługa min. 1 000 tras dla routingu IPv6,
5. Obsługa protokołów routingu OSPF, OSPFv3, RIP, RIPng, PIM-SM, PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania,
6. Obsługa wirtualnych tablic routingu-forwardingu (VRF),
7. Obsługa protokołów LLDP i LLDP-MED,
8. Przełącznik musi posiadać funkcjonalność DHCP Server,
9. Obsługa ruchu multicast:
* IGMP v1, v2 i v3,
* IGMP Snooping v1, v2 i v3,
1. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
* min. 4 poziomy dostępu administracyjnego poprzez konsolę,
* autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL,
* możliwość utworzenia minimum 2000 list ACL,
* możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www,
* zarządzanie urządzeniem przez HTTPS, SNMPv3 i SSHv2 za pomocą protokołów IPv4 i IPv6,
* możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP,
* obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard,
* możliwość synchronizacji czasu zgodnie z NTP,
1. Obsługa funkcjonalności UDLD lub równoważnej,
2. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
* klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP
* wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR,
1. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania,
2. Wymagane opcje zarządzania:
* możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN,
* plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC),
* urządzenie musi posiadać wbudowany port USB znajdujący się od strony portów, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych,
* dedykowany port konsoli, musi się znajdować od strony portów i być zgodny ze standardem RS-232,
1. Wraz z urządzeniami muszą zostać dostarczone:
* pełna dokumentacja w języku polskim lub angielskim,
* dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana,
1. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu jego poprawnej pracy,
2. Zamawiający wymaga, aby przełącznik posiadał 5-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia,
3. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń,

**Przełącznik sieciowy o poniższych parametrach – 8 szt. (minimalne wymagania)**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. System operacyjny (firmware) dostarczony przez producenta urządzenia. Zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej,
2. Wymagane parametry fizyczne:
* możliwość montażu w stelażu/szafie 19”,
* wysokość maksymalna 1U,
* minimum jeden zasilacz 230V AC,
* zakres temperatur pracy ciągłej co najmniej od 0 do +45 °C,
* zakres wilgotności pracy co najmniej 5% - 90%,
* port USB umożliwiający podłączenie zewnętrznej pamięci flash (gniazdo musi być dostępne od frontu urządzenia),
* ochrona przed przepięciami: ±4 kV,
* waga urządzenia nie większa niż 3,5kg,
1. Przełącznik musi posiadać minimum:
* 48 portów 10/100/1000BASE-T,
* 4 porty 10GE SFP+,

Wszystkie porty muszą być dostępne od frontu urządzenia,

1. Maksymalny pobór mocy nie większy niż 55W,
2. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
* zarządzanie stosem poprzez jeden adres IP,
* do min. 8 jednostek w stosie,
* magistrala stackująca o wydajności minimum 40Gb/s,
* możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation),
* stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree,
* jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia.

Zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink 10G SFP+. W ramach niniejszego postępowania musi zostać dostarczony kabel producenta umożliwiający podłączenia urządzeń w stos, minimum 1m 10G SFP+,

1. Układ przełączający o wydajności min. 176 Gbps, wydajność przełączania przynajmniej 132 Mpps,
2. Obsługa min. 32 000 adresów MAC,
3. Wbudowana pamięć RAM min. 512MB, procesor minimum dwurdzeniowy,
4. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 500 MB,
5. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ),
6. Możliwość skonfigurowania min. 1000 interfejsów vlan interface SVI działających równocześnie,
7. Obsługa ramek jumbo o wielkości min. 9216 bajtów,
8. Obsługa standardów IEEE:
* CFM zgodny z 802.1ag,
* EFM zgodny z 802.3ah,
1. Obsługa protokołu GVRP lub GARP, obsługa mechanizmu VTP lub równoważnego (innego niż GVRP lub GARP),
2. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP,
3. Obsługa min. 4 000 tras dla routingu IPv4,
4. Obsługa min. 1 000 tras dla routingu IPv6,
5. Obsługa protokołów routingu OSPF, OSPFv3, RIP, RIPng, PIM-SM, PIM-DM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania,
6. Obsługa wirtualnych tablic routingu-forwardingu (VRF),
7. Obsługa protokołów LLDP i LLDP-MED,
8. Przełącznik musi posiadać funkcjonalność DHCP Server oraz DHCP Snooping,
9. Obsługa ruchu multicast:
* IGMP v1, v2 i v3,
* IGMP Snooping v1, v2 i v3,
1. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
* min. 4 poziomy dostępu administracyjnego poprzez konsolę,
* autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL,
* możliwość utworzenia minimum 2000 list ACL,
* możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www,
* zarządzanie urządzeniem przez HTTPS, SNMPv3 i SSHv2 za pomocą protokołów IPv4 i IPv6,
* możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP,
* obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard,
* możliwość synchronizacji czasu zgodnie z NTP,
* możliwość uwierzytelnienia wielu użytkowników na jednym porcie z możliwością przydzielenia różnych VLANów dla każdego użytkownika z osobna,
1. Obsługa funkcjonalności UDLD lub równoważnej,
2. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
* klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP,
* wsparcie dla mechanizmów QoS z wykorzystaniem algorytmu karuzelowego, np.: WRR, WDRR, DRR,
1. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania,
2. Wymagane opcje zarządzania:
* możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN,
* plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC),
* urządzenie musi posiadać wbudowany port USB znajdujący się od strony portów, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych,
* dedykowany port konsoli, musi się znajdować od strony portów i być zgodny ze standardem RS-232,
* możliwość zarządzania urządzeniem z wykorzystaniem protokołu Netconf/Yang
* wsparcie dla mechanizmów Zero Touch Provisioning, w tym możliwość dokonania automatycznej aktualizacji oraz konfiguracji urządzenia poprzez podłączenie urządzenia typu pendrive (pamięć flash) do portu USB, zawierającego nową wersją oprogramowania oraz docelową konfiguracją. Funkcjonalność ma na celu wyeliminowanie konieczności manualnej konfiguracji urządzenia przez administratora, tym samym znacząco przyspieszając proces implementacji,
* wsparcie dla RMON, RMON2,
1. Wraz z urządzeniami muszą zostać dostarczone:
* pełna dokumentacja w języku polskim lub angielskim,
* dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana,
1. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu jego poprawnej pracy,
2. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski,
3. Zamawiający wymaga, aby przełącznik posiadał 5-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia,
4. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres serwisu gwarancyjnego dla urządzeń,

**Przełącznik sieciowy o poniższych parametrach – 2 szt. (minimalne wymagania)**

1. Przełącznik musi być dedykowanym urządzeniem sieciowym przystosowanym do zainstalowania w szafie rack. Wraz z urządzeniem należy dostarczyć niezbędne akcesoria umożliwiające instalację przełącznika w szafie rack. Przełącznik musi posiadać system operacyjny (firmware) dostarczony przez producenta urządzenia; zamawiający nie dopuszcza dostarczenia urządzenia z zainstalowanym systemem operacyjnym firmy trzeciej,
2. Wymagane parametry fizyczne:
* możliwość montażu w stelażu/szafie 19”,
* dwa wewnętrzne redundantne zasilacze 230V AC typu hot-swap (nie dopuszcza się rozwiązania zewnętrznego). Urządzenie musi zostać dostarczone z 2 zasilaczami umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap),
* zakres temperatur pracy ciągłej co najmniej od 0 do +45 °C,
* zakres wilgotności pracy co najmniej 5% - 90%,
* port USB umożliwiający podłączenie zewnętrznej pamięci flash,
* wymiary urządzenia nie większe niż (WxD): 442mm x 435mm,
* ochrona przed przepięciami: ±4 kV,
* MTBF: minimum 60 lat,
* maksymalny pobór mocy: 260W,
* waga urządzenia nie większa niż 9kg,
1. Przepływ powietrza przód-tył (od strony portów w kierunku zasilaczy),
2. Urządzenie musi być wyposażone w 2 moduły wentylatorów umożliwiające wymianę w trakcie pracy urządzenia (ang. hot-swap),
3. Przełącznik musi posiadać:
* 24 portów 10GE SFP+,
* 6 portów QSFP28 40/100G (Jeśli obsługa portów 100GE wymaga dodatkowej licencji to Zamawiający nie wymaga jej dostarczenia, ale zastrzega, aby była możliwość rozbudowy w przyszłości),

Wszystkie powyższe porty muszą być dostępne od frontu urządzenia.

1. Przełącznik musi umożliwiać łączenie w stosy z zachowaniem następującej funkcjonalności:
* zarządzanie stosem poprzez jeden adres IP,
* do min. 8 jednostek w stosie,
* magistrala stackująca o wydajności 160Gb/s,
* możliwość tworzenia połączeń link aggregation zgodnie z 802.3ad dla portów należących do różnych jednostek w stosie (ang. cross-stack link aggregation),
* stos przełączników powinien być widoczny w sieci jako jedno urządzenie logiczne z punktu widzenia protokołu Spanning-Tree,
* jeżeli realizacja funkcji łączenia w stosy wymaga dodatkowych interfejsów stackujących to w ramach niniejszego postępowania Zamawiający wymaga ich dostarczenia,
* zamawiający dopuszcza, aby możliwość łączenia w stosy była realizowana za pomocą portów typu uplink QSFP28. Zamawiający wymaga dostarczenia kabla stackującego 40G o długości 1m od producenta,
1. Układ przełączający o wydajności min. 1,68 Tbps, wydajność przełączania przynajmniej 450 Mpps,
2. Obsługa min. 380 000 adresów MAC,
3. Wbudowana pamięć RAM min. 4 GB, procesor wielordzeniowy,
4. Urządzenie musi mieć wbudowaną pamięć flash o pojemności min. 2 GB,
5. Obsługa min. 4000 sieci VLAN jednocześnie oraz obsługa 802.1Q tunneling (QinQ),
6. Możliwość skonfigurowania min. 1024 interfejsów vlan interface SVI działających równocześnie,
7. Obsługa ramek jumbo o wielkości min. 9216 bajtów,
8. Obsługa protokołu GVRP,
9. Wsparcie dla protokołów IEEE 802.1w Rapid Spanning Tree oraz IEEE 802.1s Multi-Instance Spanning Tree. Wymagane wsparcie dla min. 64 instancji protokołu MSTP,
10. Obsługa min. 192 000 tras dla routingu IPv4,
11. Obsługa min. 80 000 tras dla routingu IPv6,
12. Obsługa protokołów routingu OSPF, OSPFv3, IS-IS, IS-ISv6, BGPv4, BGPv4+, RIP, RIPng, PIM-SM, PIM-DM i SSM. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania,
13. Obsługa min. 16 wirtualnych tablic routingu-forwardingu (VRF),
14. Obsługa protokołów LLDP i LLDP-MED,
15. Obsługa MPLS wraz ze wsparciem dla L3VPN oraz VPLS. Jeżeli do obsługi powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć w ramach niniejszego postępowania,
16. Przełącznik musi posiadać funkcjonalność DHCP Server,
17. Obsługa ruchu multicast:
* IGMP v1, v2 i v3,
* IGMP Snooping v1, v2 i v3,
1. Mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
* min. 4 poziomy dostępu administracyjnego poprzez konsolę,
* autoryzacja użytkowników w oparciu o IEEE 802.1x z możliwością przydziału VLANu oraz dynamicznego przypisania listy ACL,
* możliwość utworzenia minimum 6000 list ACL,
* możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC oraz poprzez portal www,
* zarządzanie urządzeniem przez HTTPS, SNMP i SSHv2 za pomocą protokołów IPv4 i IPv6,
* możliwość filtrowania ruchu w oparciu o adresy MAC, IPv4, IPv6, porty TCP/UDP,
* obsługa mechanizmów Port Security, Dynamic ARP Inspection, IP Source Guard, voice VLAN oraz private VLAN (lub równoważny),
* możliwość synchronizacji czasu zgodnie z NTP,
1. Obsługa funkcjonalności UDLD lub równoważnej,
2. Implementacja co najmniej ośmiu kolejek sprzętowych QoS na każdym porcie wyjściowym z możliwością konfiguracji dla obsługi ruchu o różnych klasach:
* klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy adres MAC, docelowy adres MAC, źródłowy adres IP, docelowy adres IP, źródłowy port TCP, docelowy port TCP,
* wsparcie dla mechanizmów QoS opartych o algorytm karuzelowy, np.: DRR, SP, DRR+SP,
1. Urządzenie musi posiadać mechanizm do badania jakości połączeń (IP SLA) z możliwością badania takich parametrów jak: jitter, opóźnienie, straty pakietów dla wygenerowanego strumienia testowego UDP. Urządzenie musi mieć możliwość pracy jako generator oraz jako odbiornik pakietów testowych IP SLA. Urządzenie musi umożliwiać konfigurację liczby wysyłanych pakietów UDP w ramach pojedynczej próbki oraz odstępu czasowego pomiędzy kolejnymi wysyłanymi pakietami UDP w ramach pojedynczej próbki. Jeżeli funkcjonalność IP SLA wymaga licencji to Zamawiający wymaga jej dostarczenia w ramach niniejszego postępowania,
2. Wymagane opcje zarządzania:
* możliwość lokalnej i zdalnej obserwacji ruchu na określonym porcie, polegająca na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu oraz poprzez określony VLAN,
* plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC),
* urządzenie musi posiadać wbudowany port USB, pozwalający na podłączenie zewnętrznej pamięci FLASH w celu przechowywania obrazów systemu operacyjnego, plików konfiguracyjnych lub certyfikatów elektronicznych,
* dedykowany port konsoli zgodny ze standardem RS-232,
* dedykowany port zarządzający out-of-band Ethernet 10/100Base-T,
1. Wraz z urządzeniami muszą zostać dostarczone:
* pełna dokumentacja w języku polskim lub angielskim,
* dokumenty potwierdzające, że proponowane urządzenia posiadają wymagane deklaracje zgodności z normami bezpieczeństwa (CE), lub oświadczenie, że deklaracja nie jest wymagana,
1. Urządzenie musi być fabrycznie nowe i nieużywane wcześniej w żadnych projektach, wyprodukowane nie wcześniej niż 6 miesięcy przed dostawą i nieużywane przed dniem dostarczenia z wyłączeniem używania niezbędnego dla przeprowadzenia testu ich poprawnej pracy,
2. Wsparcie dla funkcjonalności VXLAN. Jeżeli obsługa powyżej funkcjonalności wymaga dodatkowej licencji to w ramach niniejszego postępowania Zamawiający nie wymaga jej dostarczenia,
3. Przełącznik musi umożliwiać obsługę funkcjonalności kontrolera WLAN celem zarządzania punktami dostępowymi WiFi tego samego producenta. Możliwość zarządzania minimum 1000 access-pointów. Jeżeli powyższa funkcjonalność wymaga licencji to w ramach niniejszego postępowania Zamawiający nie wymaga dostarczenia,
4. Urządzenie musi posiadać funkcjonalności WLAN:
* obsługę punktów dostępowych (access-point) pracujących w standardzie: 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 1, 802.11ac wave 2, 802.11ax.
* obsługę standardów: 802.11e, 802.11h, 802.11k, 802.11r.
* mechanizmów uwierzytelniania: WPA/WPA2 with PSK, EAP-MD5, EAP-TLS, PEAP,
1. Urządzenia muszą pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego produktu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z urządzeniami oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski,
2. Zamawiający wymaga, aby przełącznik posiadał 5-letni serwis gwarancyjny, świadczony przez Wykonawcę na bazie wsparcia serwisowego producenta. Wymiana uszkodzonego elementu w trybie 9x5xNBD. Okres gwarancji liczony będzie od daty sporządzenia protokołu zdawczo-odbiorczego przedmiotu zamówienia,
3. Bezpłatny dostęp do najnowszych wersji oprogramowania na stronie producenta przez cały okres eksploatacji urządzeń,

**Urządzenia typu firewall – 2 szt. (minimalne wymagania)**

1. Wydajność firewalla dla pakietów o wielkości 1518/512/64B – 4/4/3.5 Gbps,
2. Wydajność modułu IPS – 2Gbps,
3. Ilość jednoczesnych połączeń – 3 800 000,
4. Ilość nowych połączeń na sekundę – 76 000,
5. Wydajność VPN IPSec – 3.9 Gbps,
6. Ilość jednoczesnych tuneli IPsec – 4 000,
7. Możliwość utworzenia 15 000 polityk bezpieczeństwa,
8. Ilość tuneli SSL VPN – min. 100. Możliwość licencyjnego rozszerzenia do 900. Jeżeli funkcjonalność SSL VPN wymaga licencji to należy dostarczyć wraz z urządzeniem licencję na obsługę minimum 100 równoległych sesji SSL VPN,
9. Urządzenie wyposażone w redundantne zasilacze typy 230V AC z możliwością wymiany w trakcie pracy urządzenia (ang. hot-swap). Nie dopuszcza się rozwiązań z zewnętrznym redundantnym zasilaczem,
10. Urządzenie wyposażone w wymienny moduł wentylatora,
11. Dedykowany system operacyjny firewalla opracowany przez producenta urządzenia,
12. Architektura systemu - dedykowana platforma sprzętowa opracowana przez producenta wykorzystującej wielordzeniową architekturę sprzętową,
13. Urządzenie musi posiadać następującą ilość interfejsów:
* minimum 2 porty 10G SFP+. Obsługa modułów optycznych 10G-SR, 10G-LR,
* minimum 8 portów typu Combo 1G,
* minimum 2 porty 10/100/1000Base-T,
* port konsoli szeregowej,
* minimum jeden port USB
* dedykowany port do zarządzania Out-Of-Band 10/100/1000Base-T
1. Możliwość uruchomienia firewalla w trybie routingu, transparentnym lub hybrydowym (oba tryby uruchomione jednocześnie),
2. Mechanizmy ochrony sieci IP w wersji IPv6,
3. Obsługa protokołów routingu dla IPv6: BGP4+, IS-ISv6, OSPFv3 oraz RIPng,
4. Obsługa protokołów routingu dla IPv4: RIP, OSPF, BGP, IS-IS, obsługa rutingu multicast'owego (MSDP, PM-DM, PM-SM, IGMP oraz statycznego rutingu multicast'owego),
5. Możliwość uruchomienia funkcjonalności IPS, AV, URL filtering oraz AS. Wraz z urządzeniem ma być dostarczona subskrypcja na aktualizację wszystkich funkcjonalności UTM minimum na 5 lat,
6. Możliwość uruchomienia przynajmniej 50 wirtualnych firewalli. Jeśli jest wymagana licencja urządzenie powinno być dostarczone z licencją na przynajmniej 10 wirtualnych firewalli,
7. Możliwość uruchomienia funkcjonalności NAT w tym translacja adresu IP źródłowego, translacja adresu IP przeznaczenia, PAT, translacja statyczna i translacje puli adresów IP,
8. Wsparcie dla funkcjonalności ASPF. Inspekcja różnych protokołów w celu przepuszczenia odpowiedniego ruchu w tym FTP, H323, SIP, RTSP, NetBios,
9. Możliwość konfiguracji kontroli dostępu na podstawie adresów źródłowych i docelowych, portów, typu protokołu, czasu, TOS, użytkownika oraz aplikacji rozpoznawalnej przez analizę warstwy siódmej,
10. Integracja z wewnętrzną i zewnętrzna bazą użytkowników (local, RADIUS, TACACS, AD, LDAP),
11. Ochrona przed atakami typu SYN flood, ICMP Flood, IP spoofing, UDP Flood, Land, Fraggle, Smurf, Winnuke, Ping of Death, Tear Drop, skanowanie adresów oraz portów, IP Option control, IP fragment, large ICMP packet, ICMP redirect packet, ICMP unreachable,
12. Ograniczanie pasma dla ruchu P2P poprzez tworzenie odpowiednich polityk. Możliwość tworzenia różnych polityk ograniczania pasma dla ruchu przychodzącego i ruchu wychodzącego,
13. Wykrywanie i kontrolowanie ruch P2P poprzez identyfikację aplikacji typu P2P,
14. Możliwość statycznej konfiguracji tzw. blacklisty jak i mechanizmu dynamicznego wpisu adresów do blacklisty na podstawie wykrytych źródeł ataku oraz połączenie ACL z blacklistą,
15. Możliwość uruchomienia firewalla w trybie redundantnej pracy dla zwiększenia niezawodności. Możliwość pracy w trybie active/active oraz active/standby,
16. Wsparcie dla mechanizmu redundancji systemu (klaster urządzeń) w trybie routingu jak i transparentnym,
17. Wsparcie dla funkcjonalności Policy Based Routing (PBR),
18. Wsparcie dla protokołów tunelowania: SSL VPN, IPSec VPN, L2TP VPN, GRE VPN, L2TP over IPSec oraz GRE over IPSec,
19. Wsparcie dla mechanizmu redundancji dla połączeń IPSec VPN,
20. Wsparcie dla funkcjonalności IPS. Wykrywanie anomalii w różnych protokołach, w tym w: HTTP, SMTP, FTP, POP3, IMAP4, NETBIOS, SMB, MS\_SQL, Telnet, IRC oraz DNS,
21. Wykrywanie rodzaju protokołu poprzez zawartość danych: HTTP, SMTP, FTP, POP3, IMAP4, MSRPC, NETBIOS, SMB, MSSQL, Telnet, IRC, TFTP, eMule oraz eDonkey,
22. Grupowanie sygnatur IPS na kategorie,
23. Możliwość definiowania sygnatur IPS przez użytkownika,
24. Automatyczna aktualizacja bazy sygnatur IPS poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji,
25. Możliwość powiązania polityk IPS z regułami ACL i przypisania polityk IPS do strefy,
26. Możliwość włączania i wyłączania jednej lub wszystkich reguł IPS w polityce oraz konfiguracji rodzaju reakcji na zdarzenie,
27. Możliwość włączenia i wyłączenia funkcji IPS globalnie dla całego urządzenia,
28. Możliwe rodzaje reakcji na zdarzenie IPS: logowanie i blokowanie pakietów,
29. Wysyłanie logów z modułu IPS do zewnętrznego serwera oraz generowanie różnych rodzajów raportów umożliwiających sprawdzenie najczęściej występujących ataków, ich źródeł i przeznaczenia,
30. W zależności od ustawień przesłanie danych dalej lub blokada w przypadku przeciążenia modułu IPS,
31. Wsparcie dla funkcjonalności antywirus (AV). Skanowaniu różnych protokołów w celu wykrycia wirusów. Wsparcie dla wykrywania wirusów w plikach przesyłanych przez HTTP, SMTP, POP3,IMAP,NFS,SMB oraz FTP,
32. Dekompresja wielokrotnie skompresowanych plików od 2 do 8 poziomów w celu skanowania AV,
33. Możliwość automatycznej aktualizacji bazy wirusów poprzez sieć, definiowanie czasu aktualizacji, ręczna aktualizacja offline, przywracanie poprzedniej wersji,
34. Możliwość wylistowania wirusów zawartych w bazie AV,
35. Możliwość usunięcia wirusa, wyświetlenie strony alarmującej, oznaczanie wiadomości mailowej oraz logowanie,
36. Możliwość powiązania polityk AC z regułami ACL i przypisania polityk AV do strefy,
37. Możliwość włączenia i wyłączenia funkcji AV globalnie dla całego urządzenia,
38. Możliwość wysyłania logów z modułu AV do serwera syslog. Możliwość wygenerowania raportów z modułu AV,

**Oprogramowanie do monitorowania nowopowstałego środowiska**

1. oferowany system musi pochodzi od tego samego producenta co oferowane urządzenia typu przełączniki szkieletowe, przełączniki dystrybucyjne, przełączniki dostępowe, access-pointy, kontroler sieci bezprzewodowej, system bezpieczeństwa dostępu do sieci LAN w celu zapewnienia jak najlepszej integracji i wykorzystaniu jak największej ilości funkcjonalności oferowanych przez taki system,
2. pełna kompatybilność wymaganych funkcjonalności z oferowanymi urządzeniami typu przełączniki szkieletowe, przełączniki dystrybucyjne, przełączniki dostępowe, access-pointy, kontroler sieci bezprzewodowej,
3. obsługa minimum 20 urządzeń sieciowych, w tym urządzeń dostarczonych w ramach niniejszego postępowania (przełączniki szkieletowe, przełączniki dystrybucyjne, przełączniki dostępowe, kontroler sieci bezprzewodowej). Możliwość rozbudowy systemu do min. 5000 urządzeń,
4. dostarczone licencje na ilość obsługiwanych urządzeń sieciowych muszą posiadać wsparcie i być bezterminowe,
5. wymagana jest architektura serwer-klient z dostępem do systemu przez przeglądarkę WWW,
6. wymagany interfejs użytkownika w języku polskim lub angielskim,
7. obsługiwana lokalna baza administratorów systemu,
8. możliwość stworzenia kopii zapasowej danych systemu zarządzania i odtworzenia tych danych z kopii,
9. w przypadku, gdy oprogramowanie korzysta z systemu licencjonowania powinna być zapewniona możliwość sprawdzenia zainstalowanej licencji oraz zmiany licencji,
10. monitorowanie wykorzystania licencji i informowanie użytkownika systemu o zbliżającej się dacie wygasania licencji, bądź przekroczenia limitów zainstalowanej licencji (np. ilość obsługiwanych urządzeń),
11. dostępna w systemie zarządzającym dokumentacja w języku polskim lub angielskim,
12. możliwość automatycznego alarmowania opartego o zadane progi alarmowe,
13. system musi obsługiwać minimum 3 kategorie alarmów,
14. możliwość automatycznego alarmowania o przekroczeniu obciążenia interfejsu z uwzględnienie dwóch progów - ostrzegawczy i alarmowy,
15. możliwość określenia listy osób i grup osób powiadamianych przy poszczególnych poziomach alertów,
16. możliwość wykorzystania następujących kanałów powiadomienia dla poszczególnych poziomów alarmów,
* konsola operatora
* e-mail
* SMS
1. zapisywanie informacji o czynnościach wykonanych przez użytkowników systemu,
2. możliwość przeszukiwania dziennika czynności pod kątem użytkownika, adresu IP, z którego nastąpiło logowanie, czasu i rodzaju czynności,
3. zapisywanie informacji o zdarzeniach systemowych,
4. możliwość przeszukiwania dziennika zdarzeń systemowych pod kątem czasu i rodzaju zdarzenia,
5. podstawowe zarządzanie wszelkimi urządzeniami zgodnymi z protokołem SNMP,
6. możliwość ręcznego dodania urządzenia poprzez podanie jego adresu IP i parametrów SNMP i telnet,
7. automatyczne wyszukiwanie i dodawanie urządzeń w ramach zdefiniowanego zakresu adresów IP,
8. możliwość importowania listy urządzeń z pliku,
9. możliwość podglądu podstawowych informacji o urządzeniu,
10. możliwość wizualizowania panelu urządzenia,
11. możliwość wyświetlenia listy interfejsów urządzenia i włączenia/wyłączenia poszczególnych interfejsów,
12. wyświetlanie adresu IP urządzenia,
13. możliwość zdefiniowania parametrów SNMP i SSH dla danego urządzenia,
14. możliwość przeprowadzenia testów ping dla wybranego urządzenia,
15. możliwość dodawania, kasowania i modyfikacji nowych urządzeń,
16. możliwość definiowania alarmów dla monitorowanych urządzeń,
17. możliwość tworzenia kopii zapasowych konfiguracji urządzeń oraz odtwarzania zapisanej konfiguracji,
18. wyświetlanie topologii sieci z urządzeniami i łączami pomiędzy nimi,
19. możliwość powiększania i zmniejszania widoku topologii,
20. obrazowanie statusu dostępności urządzeń i łączy,
21. możliwość zdefiniowania obrazu tła dla mapy topologii sieci,
22. możliwość zdefiniowania różnych lokalizacji na mapie sieci,
23. zbieranie alarmów i zdarzeń w dzienniku zdarzeń,
24. możliwość wyświetlenia informacji o alarmach, nazwy, źródła, poziomu alarmu, czasu wystąpienia,
25. możliwość potwierdzenia alarmu przez użytkownika, możliwość wyłączenia alarmu,
26. możliwość eksportu danych o alarmach do pliku,
27. możliwość wyświetlenia historii alarmów zawierającej nazwę alarmu, jego źródło, poziom, status i czas wygenerowania. Możliwość filtrowania wyświetlanej listy przy pomocy powyżej podanych parametrów,
28. możliwość generowania powiadomienia o alarmach w postaci email,
29. możliwość zdefiniowania reguł powiadamiania,
30. monitorowanie obciążenia procesora i zajętości pamięci urządzenia, stanu dostępności urządzenia i opóźnienia,
31. możliwość monitorowania informacji o przesyłanym przez urządzenie ruchu,
32. możliwość generowania alarmu w przypadku przekroczenia zdefiniowanych wartości,
33. możliwość przechowywania historycznych danych wydajnościowych z ostatnich 30 dni,
34. możliwość obrazowania danych historycznych na wykresach,
35. możliwość eksportu danych historycznych do pliku,
36. automatyczne wyszukiwanie łączy przy wykorzystaniu informacji dostępu z protokołu LLDP oraz z adresacji IP,
37. możliwość generowania raportów na temat urządzeń, modułów, portów i łączy oraz statystyk nt. rodzajów urządzeń,
38. możliwość generowania raportów wydajnościowych dotyczących urządzeń oraz ich interfejsów,
39. możliwość tworzenia, wyświetlania, edytowania i kasowania zadań raportowych,
40. możliwość eksportu raportu do pliku PDF,
41. możliwość automatycznego generowania raportów w cyklach: dziennym, tygodniowym, miesięcznym, kwartalnym, półrocznym i rocznym,
42. możliwość generowania raportów w formatach np. PDF lub CSV,
43. możliwość automatycznego wykonywania w określonym czasie kopii zapasowych konfiguracji urządzeń w trybie dziennym, tygodniowym i miesięcznym,
44. możliwość podglądu i porównania różnych wersji plików konfiguracyjnych, w tym z aktualną konfiguracją urządzenia,
45. możliwość konfiguracji urządzeń, w tym list kontroli dostępu, ustawień QoS, VLAN, poprzez wysłanie szablonów konfiguracyjnych do wielu urządzeń,
46. możliwość definiowania ww. szablonów konfiguracyjnych,
47. możliwość integracji z usługą serwera wiadomości SMS,
48. możliwość rozbudowy o funkcjonalność konfiguracji i monitorowania urządzeń WLAN oraz zarządzania kontrolerami sieci bezprzewodowych, punktów dostępowych,
49. oprogramowanie do zarządzania siecią należy dostarczyć wraz z serwisem gwarancyjnym na minimum 5 lat,
50. serwis ten musi zapewniać dostęp do zdalnego wsparcia technicznego producenta przez całą dobę, 7 dni w tygodniu,
51. serwis musi zapewniać bezpłatny dostęp do poprawek i nowych wersji oprogramowania przez minimum 5 lat,
52. system musi mieć możliwość zainstalowania na wirtualizacji używanej przez Zamawiającego. Jeśli wymagane jest dostarczenie systemu operacyjnego na którym jest instalowany system do zarządzania to należy dostarczyć odpowiednie licencje z możliwością pełnego użytkowania przez okres 5 lat,
53. system musi pochodzić z autoryzowanego kanału dystrybucji producenta przeznaczonego na teren Unii Europejskiej, a korzystanie przez Zamawiającego z dostarczonego systemu nie może stanowić naruszenia majątkowych praw autorskich osób trzecich. Zamawiający wymaga dostarczenia wraz z systemem oświadczenia przedstawiciela producenta potwierdzającego ważność uprawnień gwarancyjnych na terenie Polski.