Platforma serwerowa

Wymagania dotyczące oprogramowania do wirtualizacji serwerów:

- Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta będącego licencjodawcą oprogramowania na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę.
- Wirtualizacja serwerów fizycznych musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym, nie może być częścią innego systemu operacyjnego oraz musi spełniać poniższe warunki:
- Warstwa wirtualizacji nie może dla własnych celów alokować więcej niż 200MB pamięci operacyjnej RAM serwera fizycznego
- Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym musi potrafić obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych od 1 do 128 procesorowych
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowe, 3 porty równoległe i 20 urządzeń USB
- Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług
- Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Windows Server 2019, SLES, RHEL, Solaris wersja 10 dla platformy x86, NetWare 6.5, Debian, CentOS, FreeBSD, Asianux, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X
- Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji
- Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na zasobach dyskowych
- Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna powinna mieć możliwość działania zarówno jako aplikacja na maszynie fizycznej lub wirtualnej, jak i jako gotowa, wstępnie skonfigurowana maszyna wirtualna tzw. virtual appliance
- Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.
- Rozwiązanie musi umożliwiać składowanie logów z min. 25 maszyn wirtualnych i konsoli zarządzającej na serwerze Syslog. Serwer Syslog w dowolnej implementacji musi stanowić integralną część rozwiązania
- Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji
- Rozwiązanie musi zapewniać zdalny i lokalny dostęp administracyjny do wszystkich serwerów fizycznych poprzez protokół SSH, z możliwością nadawania uprawnień do takiego dostępu nazwanym użytkownikom bez konieczności wykorzystania konta root
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej
- Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Microsoft Active Directory, Open LDAP

- Rozwiązanie musi zapewniać możliwość dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie ilości procesorów, pamięci operacyjnej i przestrzeni dyskowej
- Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia CPU/MEM serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
- Oprogramowanie do wirtualizacji musi zapewniać mechanizm pozwalający tworzyć profil (szablon konfiguracji) wybranego serwera wirtualizującego, a następnie wymuszać ten profil/konfigurację na innych serwerach lub sprawdzać zgodność konfiguracji pomiędzy zdefiniowanym wcześniej profilem a wskazanym serwerem fizycznym
- System musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE
- System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych
- System musi posiadać funkcjonalność wirtualnego przełącznika (virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów
- Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej
- Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN)
- Rozwiązanie musi umożliwiać utworzenie jednorodnego, wirtualnego przełącznika sieciowego, rozproszonego na wszystkie serwery fizyczne platformy wirtualizacyjnej. Przełącznik taki musi zapewniać możliwość konfiguracji parametrów sieciowych maszyny wirtualnej z granulacją na poziomie portu tego przełącznika. Pojedyncza maszyna wirtualna musi mieć możliwość wykorzystania jednego lub wielu portów przełącznika z niezależną od siebie konfiguracją
- Przełącznik rozproszony musi współpracować z protokołem NetFlow
- Przełącznik rozproszony musi umożliwiać funkcjonalność duplikowania ruchu sieciowego dowolnego jego portu wirtualnego na inny port
- Przełącznik musi mieć wbudowane mechanizmy składowania kopii konfiguracji, przywracania tej kopii a także mechanizmy automatycznie zapobiegające niewłaściwej konfiguracji sieciowej, które w całości lub w części mogą eliminować błędy ludzkie i utratę łączności sieciowej
- Rozwiązanie musi zapewniać możliwość konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi
- Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi
- System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu sieciowego oraz ustalania priorytetów w zależności od jego rodzaju na poziomie konkretnych maszyn wirtualnych
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane maksymalnie sprzed roku
- Rozwiązanie musi zapewnić możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych
- Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie
- Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych
- Musi istnieć możliwość odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem
- Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć możliwość przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii

- Rozwiązanie musi zapewniać możliwość replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania
- Rozwiązanie replikujące musi gwarantować współczynnik RPO na poziomie minimum 5 minut
- Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi, wolumenami dyskowymi, klastrami, centrami przetwarzania danych bez przerywania pracy usług
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, pamięciami masowymi niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych oraz pomiędzy różnymi Centrami Przetwarzania Danych platformamy wirtualnej
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy różnymi Centralnymi Konsolami Zarządzającymi platformy wirtualnej
- Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury
- Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury bez utraty danych
- Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania
- Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersja bez potrzeby wyłączania wirtualnych maszyn
- Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci
- Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć możliwość określenia przez administratora czasu po jakim taka decyzja jest wykonywana
- Rozwiązanie musi wspierać pracę bez przestojów dla wybranych maszyn wirtualnych (o maksymalnie czterech procesorach wirtualnych), niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych
- Rozwiązanie musi zapewniać natywne mechanizmy HA w niezawodnej architekturze Active-Passive-Witness dla wszystkich składowych komponentów centralnej konsoli graficznej zarządzającej platformą wirtualną
- Rozwiązanie powinno posiadać proaktywnie działający mechanizm, który wymigruje wirtualne maszyny po wykryciu potencjalnego problemu z serwerem fizycznym, zanim on ulegnie awarii
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek
- Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB
- System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn
- System musi mieć możliwość grupowania pamięci masowych o podobnych parametrach w grupy i przydzielania ich do wirtualnych maszyn zgodnie z ustaloną przez administratora polityką
- System musi mieć możliwość równoważenia obciążenia i zajętości pamięci masowych wraz z pełną automatyką i przenoszeniem plików wirtualnych maszyn z bardziej zajętych na mniej zajęte przestrzenie dyskowe lub/i z przestrzeni dyskowych bardziej obciążonych operacjami I/O na mniej obciążone
- Rozwiązanie jako funkcja wirtualizatora (jądra) musi umożliwiać szyfrowanie wirtualnych maszyn oraz szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy
- System musi zapewniać mechanizm weryfikujący integralność komponentów systemowych i plików hosta wirtualizującego i wirtualnej maszyny podczas ich uruchamiania (ochrona systemu hypervisor i OS wirtualnej maszyny na wypadek sfałszowania lub podmiany)

- Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej
- Rozwiązanie musi umożliwiać konfiguracje HA dla każdego swojego komponentu w celu unikania awarii pojedynczego elementu
- System musi umożliwiać uruchamianie kontenerów zbudowanych w topologii Docker Image w wirtualnych maszynach
- System musi umożliwiać instalowanie uruchamianie i zarządzanie aplikacjami Big Data oraz Hadoop z poziomu platformy wirtualizującej
- Platforma musi wspierać technologię rozproszonego udostępniania procesora graficznego Nvidia Grid vGPU do maszyn wirtualnych
- System musi wspierać mechanizmy zaawansowanego uwierzytelniania do systemu operacyjnego wirtualnej maszyny za pomocą technologii Smart Card Reader

Wirtualizacja Macierzy

- Oferowane rozwiązanie musi umożliwiać zbudowanie wspólnej przestrzeni dyskowej w oparciu o dyski wewnętrzne serwerów fizycznych. Wymagane wsparcie dla konfiguracji sprzętowej serwera opartej o dyski SSD i HDD oraz dla konfiguracji serwera opartej wyłącznie o dyski SSD
- Rozwiązanie musi zapewniać możliwość optymalizacji wydajności poprzez wbudowaną funkcjonalność „cache'owania" operacji odczytu / zapisu (Read/Write IO) po stronie serwerów fizycznych
- Rozwiązanie musi posiadać możliwość budowania własnych schematów konfiguracji dyskowej dla przestrzeni akcelerującej operacje Read/Write (cache) oraz dla przestrzeni budującej pojemność. Wymagana jest możliwość zmiany konfiguracji zarówno pod kątem dostępności, wydajności jak i pojemności "w locie"
- Rozwiązanie musi być zintegrowane z warstwą wirtualizacji w sposób bezpośredni, niewymagający instalacji/konfiguracji dodatkowych komponentów sprzętowych oraz dodatkowego oprogramowania / dodatkowych maszyn wirtualnych
- Konfiguracja, zarządzanie i monitoring ww. przestrzeni dyskowej muszą być zintegrowane z konsolą zarządzającą platformą wirtualizacyjną
- Narzut definiowany jako moc procesora i zużycie pamięci RAM fizycznego serwera podczas działania rozwiązania tj. podczas udostępniania zasobów dyskowych dla min. 50 maszyn wirtualnych, gdzie każda korzysta z min. 400GB przestrzeni dyskowej i generująca min. 800 IO/sek, nie może być większy niż 10% zasobów fizycznego serwera dostarczonego w ramach postępowania. W przypadku braku oficjalnych testów na stronie producenta rozwiązania Zamawiający zastrzega sobie prawo do przeprowadzenia testów wydajności na etapie analizy ofert oraz odbiorów rozwiązania
- Rozwiązanie musi zapewniać możliwość budowy wspólnej wysokowydajnej i wysoko dostępnej przestrzeni dyskowej z wykorzystaniem dysków wewnętrznych udostępnianych przez minimalnie 2 serwery fizyczne, oraz umożliwiać rozbudowę w ramach jednej logicznej puli do minimum 64 serwerów fizycznych
- Rozwiązanie musi zapewniać obsługiwanie dysków wirtualnych maszyn do rozmiaru min. 62TB
- Rozwiązanie musi zapewniać wysoką dostępność oraz odporność na awarie usług uruchomionych na serwerach z zainstalowanym oprogramowaniem do udostępniana przestrzeni dyskowej. Wysoka dostępność musi być realizowana w oparciu o wbudowane mechanizmy oprogramowania i nie dopuszcza się stosowania produktów firm trzecich lub dedykowanych komponentów sprzętowych aby zapewnić ciągłość działania w przypadku awarii komponentów takich jak: serwer fizyczny i jego komponenty takie jak: dysk cache'ujący, dysk pojemnościowy
- Rozwiązanie nie może w żaden sposób ograniczać funkcjonalności platformy wirtualizacyjnej zarówno w warstwie mechanizmów niezawodnościowych, wydajnościowo-optymalizacyjnych jak i zarządzania.
- Rozwiązanie musi posiadać konfigurowalne mechanizmy zabezpieczania danych na wypadek niedostępności danych lub awarii sprzętowej w taki sposób, aby zabezpieczane dane można było rozlokować na min. poniższych poziomach: między różnymi lokalizacjami, między różnymi centami przetwarzania danych, między różnymi szafami rack/chassis
- Rozwiązanie musi zapewniać możliwość rozbudowy i skalowania zarówno mocy obliczeniowej, pojemności przestrzeni cache, jak i pojemności przestrzeni dyskowej

- Rozwiązanie musi zapewniać możliwość rozbudowy oferowanej przestrzeni dyskowej (dodanie pojedynczego dysku, dodanie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych
- Rozwiązanie musi zapewniać możliwość ochrony danych przed utratą ich integralności (np.: sfałszowaniem) za pomocą weryfikacji sum kontrolnych
- Rozwiązanie musi wspierać utworzenie wysokodostępnego klastra przestrzeni dyskowej w scenariuszu dla tzw. „oddziału zdalnego", zbudowanego w oparciu o min. 2 serwery fizyczne i min. dwie lokalizacje. Architektura systemu musi mieć możliwość dołączania kolejnych lokalizacji „oddziałów zdalnych" w ilości min. 64.
- Rozwiązanie nie może wymagać instalacji dodatkowych komponentów i maszyn wirtualnych na serwerach wykorzystywanych do udostępniania przestrzeni dyskowych.
- Musi zostać dostarczony wirtualizator (Hypervisor) posiadający wbudowane mechanizmy typu Multi-Processor Fault Tolerance
- W ramach rozwiązania musi zostać dostarczony wirtualizator (Hypervisor) pracujący niezależnie od systemów operacyjnych jakie wspiera.
- Oprogramowanie do wirtualizacji podsystemu dyskowego (SDS) musi być wspierane przez producenta oferowanego rozwiązania do automatyzacji procesów (Automatyzacja), wirtualizacji serwerów (Hypervisor) oraz wirtualizacji sieci IP (SDN) na wszystkich poziomach wsparcia (L1-L3).
- Rozwiązanie musi zapewniać możliwość zmniejszanie przestrzeni dyskowej (odjęcie pojedynczego dysku, odjęcie serwera/serwerów fizycznych) w sposób niewymagający przestoju i przerwy w dostępie do działających usług wirtualnych
- System musi posiadać możliwość udostępniania swojej przestrzeni dyskowej również dla fizycznych systemów operacyjnych w oparciu o technologię iSCSI i umożliwiać zarządzanie dostępnością, pojemnością i wydajnością w locie
- Rozwiązanie musi posiadać interfejs API umożliwiający automatyzowanie wdrażania/modyfikacji konfiguracji systemu
- Rozwiązanie musi współdzielić zasób dyskowy dla platformy wirtualizacyjnej oraz musi umożliwiać wykorzystanie ww. przestrzeni dyskowej przez serwery fizyczne nie posiadające dysków wewnętrznych
- Rozwiązanie musi zapewniać możliwość tworzenia i konfigurowania polityk niezawodnościowych, wydajnościowych i pojemnościowych przypisanych do maszyn wirtualnych tak, aby można było określić min.: liczbę serwerów fizycznych, które mogą ulec awarii jednocześnie, liczbę operacji I/O, użycie funkcji thin-provisioning, użycie deduplikacji czy kompresji danych
- Rozwiązanie powinno wspierać mechanizmy optymalizacji wykorzystania przestrzeni dyskowych. Wymagane wsparcie dla min.: technologii deduplikacji oraz technologii implementującej RAID5 i RAID6 za pomocą oprogramowania
- Rozwiązanie musi wspierać utworzenie jednej przestrzeni dyskowej jako „rozciągniętego klastra geograficznego" realizującego scenariusze Disaster Recovery/Disaster Avoidence, zbudowanego w oparciu o dyski wewnętrzne serwerów fizycznych umieszczonych w dwóch różnych lokalizacjach fizycznych, gwarantując tym samym dostępność danych na wypadek awarii całego pojedynczego Data Center oraz dowolnego elementu w dowolnej lokalizacji.
- Rozwiązanie musi wspierać szyfrowanie wirtualnych maszyn zlokalizowanych z zbudowanym w oparciu o rozwiązanie zasobie dyskowym oraz musi umożliwiać również szyfrowanie maszyny wirtualnej podczas przenoszenia bez przerywania jej pracy na innych host lub zasób dyskowy
- Wszystkie licencje powinny być dostarczone wraz z 3-letnim wsparciem, świadczonym przez producenta, będącego licencjodawcą oprogramowania, na pierwszym, drugim i trzecim poziomie, które powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę

Wymagania platformy sprzętowej

Parametr	Charakterystyka (wymagania minimalne)	Parametry techniczne
Obudowa	Obudowa przeznaczona do montażu w szafie „rack" 19" o wysokości max 1U z możliwością instalacji 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli.	Zgodnie z wymaganiami Zamawiającego
Płyta główna	Płyta główna z możliwością zainstalowania minimum jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	Zgodnie z wymaganiami Zamawiającego
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych	Zgodnie z wymaganiami Zamawiającego
Procesor	Zainstalowany jeden procesor dwudziestocztero-rdzeniowy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 210 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org	Zgodnie z wymaganiami Zamawiającego *Procesor:*..... ***/wpisać producenta, model, symbol procesorów/*** *Umożliwiający osiągnięcie przez zaoferowany serwer wyniku:* ***...../wpisać ile/*** punktów w teście SPEC CPU2017 Floating Point Speed Results, w kolumnie „Baseline", opublikowany i ogólnie dostępny na stronie https://www.spec.org/cgi-bin/osgresults?conf=cfp2017
RAM	Zainstalowane 8 x 64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 8 wolnych slotów przeznaczonych do rozbudowy pamięci. Płyta główna powinna obsługiwać do min 1TB pamięci RAM.	Zgodnie z wymaganiami Zamawiającego
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling	Zgodnie z wymaganiami Zamawiającego
Gniazda PCI	Min. 2 sloty generacji 3 o prędkości x16.	Zgodnie z wymaganiami Zamawiającego
Interfejsy sieciowe	Wbudowane dwa interfejsy sieciowe 10Gb Ethernet w standardzie SFP+ - dodatkowe dwa interfejsy sieciowe 10/25Gb Ethernet w standardzie SFP28	Zgodnie z wymaganiami Zamawiającego
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 1x 800GB SSD DWPD min. 10 Zainstalowane trzy dyski 3,84TB SSD DWPD min. 1.	Zgodnie z wymaganiami Zamawiającego Zainstalowane ..... dyski /wpisać ile O pojemności ...../wpisać pojemność Zainstalowane ..... dyski /wpisać ile O pojemności ...../wpisać pojemność

	Zainstalowane dwa dyski M.2 SATA o pojemności min. 480GB z możliością konfiguracji RAID 1.	Zainstalowane ..... dyski /wpisać ile O pojemności...../wpisać pojemność
SAS HBA	Możliwe konfiguracje poziomów RAID: No RAID Pass-Thru	Zgodnie z wymaganiami Zamawiającego
System operacyjny	Brak systemu operacyjnego	Zgodnie z wymaganiami Zamawiającego
Wbudowane porty	5xUSB, min. 1 port USB 2.0 oraz 3 porty USB 3.0, 1 port VGA, min. 1 port RS232	Zgodnie z wymaganiami Zamawiającego
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024	Zgodnie z wymaganiami Zamawiającego
Wentylatory	Redundantne	Zgodnie z wymaganiami Zamawiającego
Zasilacze	Redundantne, Hot-Plug min. 550W	Zgodnie z wymaganiami Zamawiającego
Bezpieczeństwo	Zintegrowany z płytą główną moduł TPM 2.0 Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.	Zgodnie z wymaganiami Zamawiającego
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika • możliwość podmontowania zdalnych wirtualnych napędów • wirtualną konsolę z dostępem do myszy, klawiatury • wsparcie dla IPv6 • wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz. • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • możliwość zarządzania bezpośredniego poprzez złącze	Zgodnie z wymaganiami Zamawiającego

	microUSB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram.	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016, Microsoft Windows 2019	Zgodnie z wymaganiami Zamawiającego
Warunki gwarancji	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365. Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat.	Zgodnie z oświadczeniem w formularzu ofertowym
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.	Zgodnie z wymaganiami Zamawiającego
Licencje i wsparcie techniczne	Wszystkie licencje dla rozwiązania są zapewnione dla jego maksymalnej możliwej pojemności w ramach oferowanego klastra. Wszystkie licencje dla rozwiązania są zapewnione tak aby obejmować całkowitą wymaganą dla danego ukompletowania funkcjonalność rozwiązania.	Zgodnie z wymaganiami Zamawiającego

	Wszystkie oferowane licencje powinny być bezterminowe i dostarczone na wszystkie węzły klastra wraz z 3-letnim wsparciem, świadczonym przez producenta rozwiązania na pierwszym i drugim poziomie w języku polskim. Oferowane wsparcie powinno umożliwiać zgłaszanie problemów 7 dni w tygodniu przez 24h na dobę. Czas reakcji w ciągu 4 godzin. Producent rozwiązania musi udostępniać aktualizacje, do wszystkich opisanych komponentów i muszą być one dostępne bezpłatnie podczas całego okresu wsparcia.	
Funkcjonalność	Wymagane jest regularne (przez cały czas trwania wykupionego wsparcia serwisowego) dostarczanie przez producenta rozwiązania pełnego zestawu aktualizacji jako kompletu poprawek do wszystkich jego komponentów: oprogramowania wirtualizacyjnego serwerów, oprogramowania do zarządzania pamięcią masową Software Defined Storage, oprogramowania do zarządzania systemem wirtualizacji, jak i serwerów stanowiących węzły klastra (BIOS, procesor serwisowy, firmware kart storage, firmware kart sieciowych, firmware dysków, sterowniki do dysków). Poprawki te muszą być każdorazowo przetestowane przez producenta rozwiązania dla środowiska zgodnego z oferowanym rozwiązaniem.	Zgodnie z wymaganiami Zamawiającego

DEDUPLIKATOR:

Lp.	Parametr wymagany
1.	Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli.
2.	Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji, wymagana skalowalność do min. 32TB netto.
3.	Oferowane urządzenie musi posiadać minimum • 4 porty Ethernet 10 Gb/s BaseT, • 2 porty 10Gb/s Eth OP wymagana możliwość obsługi każdym portem Ethernet protokołów CIFS, NFS, deduplikacja na źródle • wymagana możliwość wymiany portów Eth 10Gb/s OP na 2-a porty FC 16Gb/s
4.	Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami: • CIFS, NFS, deduplikacja na źródle – alternatywnie BOOST/OST/CATALYST • VTL – po instalacji portów FC
5.	Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, BOOST/OST/CATALYST (alternatywnie) dla maksymalnej pojemności urządzenia (określonej w wymaganiach dot. skalowalności).
6.	Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami CIFS, NFS: co najmniej 1,9 TB/h (dane podawane przez producenta) oraz co najmniej 2,4 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta).
7.	Urządzenie musi pozwalać na jednoczesną obsługę minimum 30 strumieni jednocześnie (w tym 20 dedykowanych do zapisu oraz 10 dedykowanych do odczytu), wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji.
8.	Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy. Na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do urządzenia.
9.	Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku. Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu.
10.	Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości
11.	Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, BOOST/OST/CATALYST) przechowywanych w obrębie całego urządzenia (niezależnie od ilości wykorzystywanych udziałów) co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany.

12.	Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych protokołów dostępowych.
13.	Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych.
14.	Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line)
15.	Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: oferowana aplikacja, VERITAS NetBackup, EMC NetWorker, EMC Avamar, Oracle RMAN, Microsoft SQL Server Management Studio, Veeam.
16.	W przypadku współpracy z każdą z poniższych aplikacji: • oferowana aplikacja • RMAN (dla ORACLE) • Microsoft SQL Server Management Studio (dla Microsoft SQL) • VERITAS NetBackup • EMC NetWorker • EMC Avamar • Veeam urządzenie musi umożliwiać deduplikację na źródle i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN. Deduplikacja danych odbywa się na dowolnym serwerze posiadającym funkcjonalność Media Servera NetBackup'a / klienta Avamar / serwera RMAN / serwera SQL / klienta systemu NetWorker nie posiadającego licencji Storage Node. Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby z serwerów do urządzenia były transmitowane poprzez sieć LAN tylko fragmenty danych nie znajdujące się dotychczas na urządzeniu.
17.	W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów.
18.	Dla aplikacji VERITAS NetBackup, EMC NetWorker, urządzenie musi pozwalać na łączenie backupów pełnych i inkrementalnych bez odczytu danych z urządzenia. Zarządzanie łączeniem backupów pełnych i inkrementalnych musi być wykonywane co najmniej z poziomu aplikacji VERITAS NetBackup, EMC NetWorker
19.	Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.
20.	Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu w tym deduplikatora wirtualnego będącego przedmiotem Zapytania. Konfiguracja replikacji musi być możliwa w każdym z trybów: * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).

	Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację musi być dostarczona w ramach postępowania.
21.	Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji.
22.	W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
23.	W przypadku replikacji danych między dwoma urządzeniami kontrolowanej przez systemy VERITAS NetBackup / EMC Avamar / EMC NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności: • replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących • replikacji podlegają tylko te fragmenty danych, które nie znajdują się na docelowym urządzeniu • replikacja zarządzana jest z poziomu aplikacji backupowej • aplikacja backupowa posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji
24.	Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
25.	Urządzenie musi pozwalać na przechowywanie minimum 200 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia - umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności.
26.	Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą d-duplikowane (globalna deduplikacja między logicznymi częściami urządzenia).
27.	Urządzenie musi mieć możliwość podziału na minimum 4 logiczne części pracujące równolegle.
28.	Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia.
29.	Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem: • CIFS • NFS • BOOST/OST/CATALYST
30.	Oferowane urządzenie powinno być objęte wsparciem producenta w okresie 36 miesięcy, realizowanym w trybie 5x9 NBD.

Akcesoria

Szafa Rack

Parametr	Charakterystyka	Spełnia wymagania (TAK/NIE)
Wysokość	42U	
Maksymalna waga	135 KG	
Minimalna głębokość	104 cm	
Maksymalna wysokość	200 cm	
Standardy i certyfikaty	UL 2416 UL 60950-1 EIA-310E	
Gwarancja	3 lata	

Zasilacz awaryjny UPS

Parametr	Charakterystyka (wymagania minimalne)	Spełnia wymagania (TAK/NIE)
Moc skuteczna	4500W	
Moc pozorna	5000VA	
Topologia	Podwójna konwersja online	
Współczynnik szczytu obciążenia	03:01	
Wyjścia	(6) IEC 320 C13 (4) IEC 320 C19 (2) IEC Jumpers	
Częstotliwość	40 - 70 Hz	
Czas ładowania	1.5 godziny	
Interfejsy	RJ-45 10/100 Base-T , RJ-45 Serial , Smart-Slot , USB	
Temperatura pracy	0 – 40 ^{0}C	
Głośność pracy	55.0dBA	
Gwarancja	3 lata, 2 lata gwarancji na baterie	

Przełącznik KVM

Parametr	Charakterystyka	Spełnia wymagania (TAK/NIE)
Maksymalna wysokość	1U	
Maksymalna waga	3 kg	
Interfejsy	Minimum 4 porty USB 2.0, dedykowany port USB do podłączenia myszy i klawiatury, 2 porty gigabit Ethernet, port ACI,	
Zasilacz	Maksymalnie 20 W, połączenie IEC C14	
Wyposażenie dodatkowe	3 szt. modułów interfejsu ze złączami VGA, USB, z obsługą nośników wirtualnych i kart CAC	
Oprogramowanie zarządzające	Interfejs przeglądarkowy do zdalnego zarządzania	
Gwarancja	3 lata	

Monitor do przełącznika KVM

Parametr	Charakterystyka	Spełnia wymagania (TAK/NIE)
Maksymalna wysokość	1U	
Maksymalna waga	1.5 kg	
Interfejsy	Minimum 2 porty USB 3.0	
Matryca	Maksymalnie 20 cali z podświetleniem LED, minimalna rozdzielczość 1355x768	
Wyposażenie dodatkowe	Szyny do montażu w szafie rack	
Oprogramowanie zarządzające	Interfejs przeglądarkowy do zdalnego zarządzania	
Gwarancja	3 lata	

Urządzenie bezpieczeństwa brzegu sieci

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

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

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.
3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.
5. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

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

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.
12. Analiza ruchu szyfrowanego protokołem SSH.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
   - Translację jeden do jeden oraz jeden do wielu.
   - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
   - Amazon Web Services (AWS).
   - Microsoft Azure

- Cisco ACI.
- Google Cloud Platform (GCP).
- OpenStack.
- VMware vCenter (ESXi).

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - Wsparcie dla IKE v1 oraz v2.
   - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
   - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:
   - Routingu statycznego.
   - Policy Based Routingu.
   - Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.

3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
7. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Rozwiązanie musi obsługiwać autentykatory sprzętowe tego samego producenta wyposażone w bezpieczną obudowę uniemożliwiającą jej otwarcie i dostęp do elementów wewnętrznych bez ich uszkodzenia oraz w przynajmniej 6 znakowy wyświetlacz LCD i przycisk „budzenia" tokena. Dla systemu musi również istnieć możliwość obsługi tokenów softwareowych tego samego producenta. Wraz z systemem należy dostarczyć 20 wspomnianych wyżej fizycznych tokenów zbudowanych w formie breloka do kluczy.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Access Point

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:
    a. Temperatura -20–50°C,
    b. Wilgotność 5–90%.
2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.
3. Urządzenie musi być wyposażone w dwa niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:
    a. 2.4 GHz 802.11b/g/n,
    b. 5 GHz 802.11a/n/ac,
4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 16 SSID.
5. Liczba interfejsów:
    a. Ethernet – 1 w standardzie 10/100/1000 Base-TX,
    b. USB – 1 Typ A.
6. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz.
7. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:
    a. Tunnel,
    b. Bridge,
    c. Mesh.
8. Wsparcie dla QoS: 802.11e, WME/WMM Multimedia Extensions, konfigurowalne polityki QoS per użytkownik/aplikacja.
9. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA-PSK, WPA-TKIP, WPA2-AES, Web Captive Portal, MAC blacklist & whitelist, 802.11i, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, PEAP, EAP-FAST, EAP-SIM, EAP-AKA).
10. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:
    a. MIMO – 2x2,
    b. Transmit Beam Forming (TxBF),
    c. Maksymalna przepustowość dla poszczególnych modułów radiowych:
        i. 400 Mbps;
        ii. 867 Mbps;
    d. Wymagana moc nadawania:
        i. min. 25 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;
        ii. min. 23 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;
    e. Wsparcie dla 802.11n 20/40Mhz HT,
    f. Wsparcie dla kanału 80 MHz dla 802.11ac,
    g. Anteny – 4 wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 5dBi dla pasma 5GHz.
    h. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,
    i. Maksymalna deklarowana liczba klientów per moduł radiowy – 512.
11. Funkcje interfejsu radiowego:
    a. Skaner częstotliwości 2.4 oraz 5 GHz,

b. Skanowanie w tle podczas obsługi klientów na pasmach 2.4 oraz 5 GHz,
c. Skaner częstotliwości 2.4 oraz 5GHz w trybie dedykowanego monitora,

12. Funkcje dodatkowe:
    a. Low-Density Parity Check (LDPC) Encoding,
    b. Maximum Likelihood Demodulation (MLD),
    c. Maximum Ratio Combining (MRC),
    d. A-MPDU and A-MSDU Packet Aggregation,
    e. MIMO Power Save,
    f. Short Guard Interval,
    g. WME Multimedia Extensions.
13. Punkt dostępowy musi być certyfikowanym urządzeniem WiFi Alliance: WiFi certified IEEE Std 802.11a/b/g/n (ac) oraz posiadać certyfikację DFS.

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Przełącznik typ 1	
	Minimalne wymagania
Porty	Przełącznik 1U wyposażony w porty: - 12 x 25 Gigabit Ethernet SFP28 - 3 x 100 Gigabit Ethernet QSFP28 - 1 port konsolowy RJ45 - 1 port zarządzający typu out-of-band management - 1 port typu USB
System operacyjny	Modularny system operacyjny, Musi być zgodny ze standardem ONIE i umożliwiać instalacje systemów operacyjnych innych producentów, w celu uzyskania dodatkowych funkcjonalności.
Zasilanie	2 redundantne zasilacze AC
Dodatkowe wyposażenie	2 wkładki SFP+ 10GbE, 6 kabli DAC 10GbE, 1 kabel QSFP+
RACK	Musi zapewniać instalację w szafach 19". Dostarczony wraz ze wszystkimi elementami umożliwiającymi instalację w szafie RACK.
Pamięć	Pamięć CPU: 8GB Pojemność bufora pakietów: 32MB
Wydajność	Musi posiadać matrycę przełączającą o wydajności min. 2.10 Tbps (full-duplex), min. 890Mpps
Chłodzenie	Musi posiadać możliwość chłodzenia urządzenia w trybie przód-do-tyłu lub tył-do-przodu (ustawienia fabryczne). Musi być wyposażony w redundantne moduły wentylatorów Temperatura pracy w przedziale 0-45 stopni Celsjusza
Funkcjonalności warstwy II	Musi obsługiwać ramki „Jumbo" o długości min. 9000B. Musi obsługiwać, co najmniej 4000 VLANów. Pamięć, dla co najmniej 150 000 adresów MAC. Musi obsługiwać, co najmniej protokoły: STP, RSTP, PVST+, MSTP Musi wspierać funkcjonalność wirtualnej agregacji portów umożliwiającą: - terminowanie pojedynczej wiązki EtherChannel/LACP wyprowadzonej z urządzenia zewnętrznego (serwera, przełącznika) na 2 niezależnych opisywanych urządzeniach - budowę topologii sieci bez pętli z pełnym wykorzystaniem agregowanych łączy - umożliwiać wysokodostępny mechanizm kontroli dla 2 niezależnych opisywanych urządzeń Urządzenie musi posiadać możliwość definiowana łączy w grupy LAG (802.3ad). Obsługa min. 16 łączy w grupie LAG
Funkcjonalności warstwy III	Musi obsługiwać protokoły dynamicznego routingu dla IPv4 i dla IPv6: OSPF, BGP Musi obsługiwać protokół BFD, przynajmniej dla protokołu OSPF i OSFP v3 i tras statycznych Musi przechowywać sprzętowo minimum 32000 wpisów routingu IPv4 i 16000 wpisów routingu IPv6 Musi wspierać mechanizm L3 ECMP Load Balancing Musi wspierać protokół redundancji VRRP Wsparcie dla DHCP server i DHCP Relay oraz DHCPv6 Relay Obsługa Policy Based Routing Obsługa Muticastów, IGMP Snooping oraz Multicast Snooping, protokołu PIM oraz filtrów dla PIM Musi obsługiwać funkcjonalność VxLAN, Static VxLan Musi obsługiwać funkcjonalność VXLAN BGP EVPN (Ethernet VPN) z MP-BGP Obsługa routingu między VxLAN-ami (VxLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway Obsługa Multi-AS dla EVPN oraz trybów Asymmetric IRB (Integrated routing and bridging) oraz Symmetric IRB Obsługa mechanizmu BGP unnumbered dla EVPN

Mechanizmy bezpieczeństwa i QoS	Klasyfikacja ruchu dla klas różnej, jakości obsługi QoS poprzez wykorzystanie, co najmniej następujących paramentów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, vlan, wartość DSCP Implementacja, co najmniej 8 kolejek sprzętowych na każdym porcie wyjściowym dla obsługi ruchu o różnej klasie obsługi. Możliwość obsługi jednej z powyższych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority). Implementacja mechanizmu Weighted Random Early Detection (WRED) Obsługa IP Precedence i DSCP Obsługa Control-Plane-Policing (ochrona systemu operacyjnego przed atakami DoS) Musi obsługiwać DCB (Data Center Bridging), 802.1Qbb Priority-Based Flow Control oraz Priority Flow Control oraz Enhanced Transmission Selection i iSCSI TLV Co najmniej 3 poziomy dostępu administracyjnego przez konsole: Autoryzacja użytkowników/portów w oparciu o 802.1x Obsługa List dostępu ACL dla adresów MAC i adresów IPv4 i IPv6 Wsparcie dla Ipv6 RA Guard
Mechanizmy zarządzania	Musi wspierać następujące mechanizmy zarządzania Możliwość uzyskania dostępu do urządzenia przez SNMPv1/2/3 i SSHv2 Obsługa monitorowania ruchu na porcie (Port Monitoring), ACL-Based Monitoring oraz RSPAN Urządzenie musi posiadać dedykowany port konsolowy do zarządzania typu RJ45 (konsola) oraz drugi wydzielony typu Ethernet 100/1000BaseT Plik konfiguracyjny urządzenia musi być możliwy do edycji 'off-line'. Tzn. konieczna jest możliwość przeglądania zmian konfiguracji w pliku tekstowym na dowolnym PC. Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne bez częściowych restartów urządzania po dokonaniu zmian. Wsparcie dla mechanizmu Beacon LED control – włączenie diody danego interfejsu celem identyfikacji Urządzenie musi posiadać funkcjonalność automatycznej instalacji oprogramowania poprzez ściągnięcie z serwera TFTP pliku z oprogramowaniem (firmware), w trakcie pierwszego podłączenia do sieci Ethernet Urządzenie musi mieć możliwość utworzenia skryptów systemu linux oraz uruchomienia skryptów utworzonych w języku Python oraz umożliwiać jego konfigurację przez narzędzia Ansible, Chef i Puppet Możliwość użycia Restconf API, autoryzacja w oparciu o tokeny dla REST API oraz wsparcie dla mechanizmu tłumaczenia dowolnej komendy CLI na wywołanie Restconf
Warunki gwarancji	Trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające do okazania na życzenie Zamawiającego. Na życzenie Zamawiającego przedstawienie oświadczenia Producenta potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Przełącznik typ 2

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Wbudowany redundantny zasilacz.
- Budżet mocy dla portów PoE min.: 770 W.

· Maksymalny pobór mocy bez budżetu dla PoE: 160 W.

- Minimalny zakres temperatury pracy: 0-50°C.

Interfejsy sieciowe - wymagania minimalne

1. Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 48 porty GE RJ-45.

- W tym porty PoE w ilości co najmniej: 48, zgodne ze standardem: 802.3af oraz 802.3at.

e) 4 porty 10 GE SFP+.

Zarządzanie

- Dedykowany 1 interfejs Ethernet RJ-45 do zarządzania.
- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów przydzielających tryb dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 176 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 260 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32 k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 1 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLANów, zgodna ze standardem 802.1Q.
- Wsparcie dla Private VLAN.
- Obsługa routingu statycznego.
- Obsługa Quality of Service, w tym zakresie: 802.1p oraz DSCP.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLANu dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Centralne zarządzanie sieciami VLAN.
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci.
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
   - W przypadku gdy do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC wymagane są licencje, producent zobowiązany jest je dostarczyć .
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- Stateful firewall, umożliwiający kontrolę pomiędzy sieciami VLAN.
- Routing statyczny i dynamiczny (co najmniej OSPF).
- Policy Based Routing.

Gwarancja oraz wsparcie

1. System musi być objęty serwisem gwarancyjnym producenta przez okres 36 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Wymagania ogólne
Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,
Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.
Całkowite koszty posiadania
Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli.
Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu
Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API

Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.
Wymagania RPO
Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
Oprogramowanie musi oferować ten mechanizm z dokładnością do pojedynczego datastoru
Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware i być dostępna dla następujących macierzy: HPE, Dell EMC, NetApp, Cisco, IBM, Lenovo, Fujitsu, Huawei, INFINIDAT, Pure Storage.
Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
Oprogramowanie musi posiadać wsparcie dla NDMP
Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN.

Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwosc zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO.
Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)
Wymagania RTO
Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.
Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
o Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
o BSD: UFS, UFS2
o Solaris: ZFS, UFS
o Mac: HFS, HFS+
o Windows: NTFS, FAT, FAT32, ReFS
o Novell OES: NSS
Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.

Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN
Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA
Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN
Ograniczenie ryzyka
Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
Dla VMware'a oprogramowanie musi pozwalać na uruchomienie takiego środowiska bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach.
Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.