

SZCZEGÓŁOWA SPECYFIKACJA TECHNICZNA

Zadania: „Dostawa sprzętu komputerowego”, realizowanego w ramach projektu: „Rozwój e-usług w mieście Ełk”

Dla zadania, w dalszej części dokumentu przedstawiono szczegółowe zakresy oraz określono min. wymagania techniczno-funkcjonalne dla każdego z systemów.

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

- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów z obszaru Unii Europejskiej,
- Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu weryfikacji działania urządzenia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem);
- Musi posiadać stosowny pakiet usług gwarancyjnych świadczonych przez producenta sprzętu (lub autoryzowany serwis) kierowanych do użytkowników z obszaru Rzeczypospolitej Polskiej;
- Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów. Wymagane jest utrzymanie świadczeń gwarancyjnych (przez producenta urządzeń lub jego autoryzowaną placówkę serwisową) także w przypadku niemożliwości ich wypełnienia przez Wykonawcę (np. w przypadku jego bankructwa);
- Wykonawca zobowiązuje się iż czas reakcji na zgłoszone awarie i usterki nie będzie dłuższy niż 12 godzin;
- Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich;
- Do każdego urządzenia musi być dostarczony komplet nośników umożliwiających odtworzenie oprogramowania zainstalowanego w urządzeniu;
- Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej, tj. dostępnym na etapie realizacji projektu, włącznie z momentem zakończenia wdrożenia urządzeń;
- Wykonawca wykona dla dostarczonych systemów informatycznych zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych) RODO:

a. zgodnie z artykułem 32 RODO proces szacowania ryzyka dla dostarczonych systemów i technicznych środków bezpieczeństwa (serwery, przełączniki infrastruktura komunikacyjna) przetwarzania danych.

b. zgodnie z art. 35 przeprowadzi oraz udokumentuje ocenę skutków dla ochrony danych OSOD (ang. DPIA - Data Protection Impact Assessment).

c. pełny audyt zgodności z RODO.

- Wykonawca wykona audyt dostarczonego systemu informatycznego z uwzględnieniem jego korelacji z istniejącą infrastrukturą zgodnie z wymaganiami ISO 27001.

- Zamawiający dopuszcza realizację poszczególnych grup funkcjonalnych przez zespoły urządzeń pod następującymi warunkami:

a) połączenie urządzeń będzie zrealizowane w sposób nie ograniczający wydajności (sumaryczna przepustowość połączeń pomiędzy dowolnymi urządzeniami wchodzącymi w skład zestawu, jak również wydajność poszczególnych urządzeń nie może być niższa niż wymagana wydajność urządzenia),

b) łączna wielkość zestawu nie będzie przekraczać wymaganej wielkości urządzenia,

c) zapewnione i dostarczone będą wszystkie elementy konieczne do połączenia zespołu urządzeń,

d) wszystkie elementy zestawu będą spełniały wymagania związane z zarządzaniem,

- Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V $\pm 10\%$, 50Hz;

- Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej.

Celem zamówienia jest dostawa, wdrożenie do działania i uruchomienie systemu złożonego z:

1. Modernizacji systemu zasilania gwarantowanego
2. Serwery sieciowe
3. Modernizacji systemu storage
4. Modernizacji systemu serwerowego, wirtualizacji i backupu
5. System bezpieczeństwa transmisji danych
6. Przełączniki rdzeniowe
7. Przełączniki sieciowe
8. Wdrożenie

Definicje i minimalne parametry urządzeń i oprogramowania obowiązujące w całym niniejszym dokumencie:

1. Modernizacji systemu zasilania gwarantowanego.

W ramach modernizacji systemu zasilania Wykonawca dostarczy, zainstaluje i uruchomi 2 szt UPS o minimalnych parametrach:

PARAMETR	WYMAGANIA MINIMALNE
Moc wyjściowa	30kVA/24kW
Topologia	VFI-SS-111

Sprawność całkowita dla Pmax (dla VFI)	<94%
Sprawność całkowita dla Pmax (dla ECO)	>98%
Chłodzenie	wymuszone, wewnętrzne wentylatory
Temperatura przechowywania	0 ÷ +40 °C
Temperatura pracy	+10 ÷ +40 °C
Stopień ochrony	IP20
PROSTOWNIK	
Zakres napięcia wejściowego	173 ÷ 485 V AC ± 2 %
Zakres częstotliwości wejściowej	45 ÷ 55 Hz ± 1 Hz
Współczynnik mocy PF (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	> 0,99
Moc bierna pojemnościowa (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	0 var
Współczynnik tg φ (bez zewnętrznych układów kompensujących, realizowane za pomocą układu prostownika)	< 0,4
Zniekształcenia prądu wejściowego THDi (bez zewnętrznych układów filtrujących, realizowane za pomocą układu prostownika)	< 2%
FALOWNIK	
Znamionowe napięcie wyjściowe	3x400 V AC
Częstotliwość napięcia wyjściowego	Synchroniczne z siecią / 50Hz ± 0,1 Hz
Regulacja statyczna napięcia	< 1 %
Zniekształcenia napięcia wyjściowego THDu	< 0,4 % dla Pmax (liniowe) < 5 % (nieliniowe wg PN EN 62040-3)
Współczynnik szczytu CF	5:1
Praca ze 100% asymetrią obciążenia wyjścia (100% obciążenia jednej fazy przy zerowym obciążeniu pozostałych)	wymagana
Przebieżalność	130% - 10min / 160% - 1min / 300% 100ms
CZAS PRACY	
Czas pracy z baterii	minimum 3 minuty dla obciążenia 24kW
akumulatory	akumulatory o pojemności nie mniejszej niż 7Ah, akumulatory szczelne bezobsługowe, zaistalowane wewnątrz UPS, o projektowanej żywotności minimum 15 lat
WYPOSAŻENIE	
Sygnalizacja	akustyczno-diodowa, wyświetlacz LCD z menu w języku polskim
Interfejs komunikacyjny	RS232, RS485, USB, bezpotencjalowe wyjścia programowalne (min. 4); SNMP/HTTP, wejścia sterujące (min. 4)
EPO	wymagane / standard NC

Parametry styków przekaźników wyjść programowalnych	1A / 250 V AC / w standardzie NO i NC dla każdego wyjścia
Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS .
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
	możliwość edycji nazw urządzeń na liście monitorowanych zasilaczy UPS
	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
Pomiar parametrów środowiskowych przez UPS	pomiar minimum temperatury i wilgotności otoczenia
Koła transportowe z minimum dwoma kołami skrętnymi umożliwiającymi swobodne przemieszczanie urządzenia	wymagane
WYPOSAŻENIE DODATKOWE	
Zewnętrzny bezprzerwowy układ obejściowy tzw BY-PASS pozwalający na naprawę, konserwację lub wymianę akumulatorów w UPSie bez przerwy w zasilaniu podłączonych urządzeń	wymagane
PARAMETRY MECHANICZNE	
Wymiary UPS (wys. X szer. X gł.)	nie większe niż 1151 x 486 x 856 mm
Masa zasilacza	nie większa niż 330 kg
GWARANCJA / SERWIS	
Gwarancja	min. 60 miesięcy na elektronikę, min. 60 miesięcy na akumulatory.
Czas naprawy	max. 14 dni roboczych
Serwis	Autoryzowany serwis producenta zlokalizowany w Polsce.
	W przypadku braku możliwości dokonania naprawy w miejscu instalacji urządzenia - oferent zagwarantuje sprzęt zastępczy o nie gorszych parametrach niż oferowany
	Serwis realizowany w systemie on-site (w miejscu zainstalowania UPSa)
Przeglądy gwarancyjne	Gwarancja powinna obejmować przeglądy.
Wymiana akumulatorów	Wymagana wymiana wszystkich akumulatorów w 4 roku użytkowania na akumulatory o pojemności nie mniejszej niż 7Ah 12V i spełniające wymagania minimalne odnośnie czasu podtrzymania tj. 3 min dla obciążenia 24kW
Pomiary	wymagane wykonania miernikiem dwóch pomiarów - bilans mocy oraz moc bierna. Wyniki pomiarów powinny być udokumentowane raportem z pomiarów.
POZOSTAŁE	

Certyfikaty / dokumenty / oświadczenia producenta sprzętu (załączyć do oferty)	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania - należy dołączyć do oferty dokument potwierdzający spełnienie wymagań
	deklaracja CE wystawiona w oparciu o obowiązujące normy (LVD, EMC)
	Wymagane dołączenie do oferty karty katalogowej oferowanego sprzętu
	Wymagane dołączenie do oferty wytycznych instalacyjnych zawierających minimum informacje o wymaganych zabezpieczeniach w rozdzielni oraz przekrojach kabli zasilających.
	do każdego zasilacza UPS wymagane dołączenie dokumentu potwierdzającego realizację gwarancji i przeglądów przez serwis producenta (zapis w karcie gwarancyjnej lub oświadczenie producenta)
	dostarczane urządzenie (UPS) będzie fabrycznie nowe, wyprodukowane nie wcześniej, niż na 1 miesiąc przed ich dostarczeniem
	sprzęt i oprogramowanie będzie pochodzić z autoryzowanego kanału sprzedaży

2. Serwery sieciowe - 4 szt o minimalnych parametrach:

LP	Parametr	Minimalne wymagania
1	Obudowa	-Typu Rack, wysokość maksimum 2U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy;
2	Płyta główna	-Dwuprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów dwudziestoośmiordzeniowych; -wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3000GB pamięci RAM DDR4 2966 Mhz; -Oferowany model serwera musi obsługiwać pamięć nieulotną instalowaną w gniazdach pamięci RAM o pojemności sumarycznej minimum 1000GB (przez pamięć nieulotną rozumie się moduły pamięci zachowujące swój stan np. w przypadku nagłej awarii zasilania) -Minimum 6 złącz PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16 i 3 złącza o prędkości x8; -Wszystkie złącza PCI Express muszą być aktywne; -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug;
3	Procesory	Zainstalowane minimum dwa procesory 16-rdzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECrate2017_int_base minimum 173 pkt. Wynik dla oferowanego serwera wraz z oferowanymi procesorami dostępny na stronie spec.org; (nie dopuszcza się procesorów o innej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowana aplikacji i systemów operacyjnych)

4	Pamięć RAM	-Zainstalowane 512 GB pamięci RAM w kościach o pojemności 32GB; -wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM;
5	Kontroler y dyskowe, I/O	-Wbudowany kontroler SATA RAID 0,1
6	Dyski twarde	- Brak dysków twardych -Minimum 8 wnęk dla dysków twardych Hotplug 2,5 cala, możliwość rozbudowy do 16 dysków twardych Hotplug 2,5 cala bez konieczności wymiany kontrolera RAID;
7	Kontroler y LAN	- 2x1Gbit/s ze wsparciem iSCSI, - 2x 10Gbit/s RJ-45
8	Kontroler y I/O FC/SAS/Inne	-Jedna dwuportowa karta FC x16;
9	Porty	-zintegrowana karta graficzna ze złączem VGA; -2x USB 3.0 dostępne na froncie obudowy -2x USB 3.0 dostępne z tyłu serwera -1x USB 3.0 wewnątrz serwera Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera;
10	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o mocy maksimum 500W, o sprawności 94% (tzw klasa Platinum) -Redundantne wentylatory hotplug;
11	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania, rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny/przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slotcie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, wbudowany na płycie głównej nośnik pamięci M.2 SSD, status karty zarządzającej serwerem, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera, Wymaga się aby system przewidywania/rozpoznawania awarii był niezależny i działał w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym) -Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: <ul style="list-style-type: none"> • Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;

		<ul style="list-style-type: none"> • Dedykowana karta LAN 1 Gb/s (dedykowane złącze RJ-45 z tyłu obudowy) do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym; • Dostęp poprzez przeglądarkę Web (także SSL, SSH) • Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii • Zarządzanie alarmami (zdarzenia poprzez SNMP) • Możliwość przejęcia konsoli tekstowej • Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM) • Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.)
12	Dokumentacja, inne	<p>-Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce - Wymagane oświadczenie producenta serwera, że oferowany do przetargu sprzęt spełnia ten wymóg;</p> <p>-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;</p> <p>-Wszystkie parametry i funkcje oferowanego serwera muszą być potwierdzone w ogólnodostępnej dokumentacji producenta.</p>

Na każdym dostarczonym serwerze należy zainstalować Serwerowy system operacyjny (SSO) o wymaganiach minimalnych:

Licencje na serwerowy system operacyjny muszą zapewnić poniżej opisane funkcjonalności dla dostarczanych serwerów w niniejszym postępowaniu, licencja musi być zgodna z ilością rdzeni dostarczanych serwerów.

Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i nieograniczonej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.

Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy.

1. Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych z możliwością kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem

wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.

5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.

6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.

7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.

8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:

- a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
- b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
- c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
- d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).

10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.

12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET

13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.

15. Graficzny interfejs użytkownika.

16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,

17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.

18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).

19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.

21. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).

22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

- a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,

- b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
- Podłączenie 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.
 - Ustanawianie praw dostępu do określonych zasobów dla użytkowników nie dołączonych do domeny
- c. Zdalna dystrybucja oprogramowania na stacje robocze.
- d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
- e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
- Dystrybucję certyfikatów poprzez http
 - Konsolidację CA dla wielu lasów domeny,
 - Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
- f. Szyfrowanie plików i folderów.
- g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
- h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
- i. Serwis udostępniania stron WWW.
- j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
- k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
- l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 300 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne 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 mają zapewnić 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
 - Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
 - Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)

23. 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.

24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

25. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

26. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

27. Sterowniki i dokumentacja od producenta sprzętu

28. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

29. Oprogramowanie musi być dostarczone w najnowszej wersji i umożliwiać instalację wersji poprzedniej (downgrade).

Instruktaż wdrożeniowy dla administratorów (3x po 2 dni (każdy dzień 6 godzin), grupy do 6 osób) obejmujący:

Wprowadzenie do zaproponowanego SSO (wersje, licencjonowanie)

Instalacja systemu na maszynie fizycznej

Omówienie podstaw wirtualizacji

Instalacja systemu

Konfiguracja zasobów dyskowych

Konfiguracja virtualizatora

Instalacja i konfiguracja środowiska katalogowego

Usługa katalogowa SSO

Instalacja kontrolera domeny

Konfiguracja domeny

Instalacja i konfiguracja usługi DHCP

Instalacja i konfiguracja serwera plików

Kopia zapasowa maszyn wirtualnych

Przygotowanie kopii zapasowej

Odtworzenie usuniętej maszyny wirtualnej

Odtworzenie usuniętych plików

Instalacja stacji roboczej

Wersje i licencjonowanie

Instalacja i konfiguracja stacji z systemem operacyjnym

Konfiguracja stacji roboczej

Aktualizacje systemu

Rozwiązywanie problemów

Odtwarzanie plików i systemu operacyjnego

Instruktaż przeprowadzi osoba posiadająca certyfikaty szkoleniowe wystawione przez producenta SSO i osoba która wykaże przeprowadzenie minimum dwóch szkoleń z powyższego zakresu w ostatnich dwóch latach kalendarzowych od dnia złożenia oferty.

Przełącznik sieci Fiber Channel 2szt. O minimalnych parametrach:

Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.

W przypadku obsadzenia portu FC za pomocą wkładki SFP 32Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 32, 16, lub 8 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.

Przełącznik FC musi być wyposażony, w co najmniej 24 aktywnych portów FC obsadzonych wkładkami SFP 16Gb/s.

Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 32Gb/s musi wynosić minimum 768 Gb/s end-to-end.

Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.

Przełącznik FC musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19".

Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.

Przełącznik FC musi mieć możliwość wymiany i aktywacji wersji firmware'u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.

Przełącznik FC musi mieć możliwość konfiguracji przez:

polecenia tekstowe w interfejsie znakowym konsoli terminala

przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.

Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.

Przełącznik FC musi umożliwiać wprowadzenie ograniczenia prędkości dla danych wchodzących dla dowolnego portu lub portów. Musi być możliwość określenia wartości limitu przepustowości danych wchodzących niższej niż wynegocjowana prędkość portu.

Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.

Przełącznik FC musi obsługiwać protokoły FCP na dowolnych portach przełącznika.

3. Modernizacji systemu storage o minimalnych parametrach:

Macierz dyskowa 1 szt. o minimalnych parametrach:

Procesor minimum 6 rdzeni 2,2GHz

Obudowa Rack z szynami do montażu w szafie rack

Pamięć RAM 8GB z możliwością rozszerzenia do 64GB

Zainstalowane dyski 12 dysków 6 TB przystosowanych do pracy w NAS

Interfejsy sieciowe 2 x Gigabit (10/100/1000) oraz 2 x 10GbE RJ-45

Porty 2 x USB 3.0

Obsługa RAID Basic, JBOD, RAID F1,0,1,5,6,10 + Hot Spare 1,5,6,10.

Funkcje RAID Możliwość zwiększania pojemności i migracja między poziomami RAID online.

Szyfrowanie Możliwość szyfrowania wybranych udziałów sieciowych, kluczem AES-256bitów

System Operacyjny Windows XP i nowsze , MAC OSX 10.5 i nowsze, Ubuntu 9.04 i nowsze

Protokoły CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP, WebDAV, CalDAV, SFTP,

praca w klastrze (HA)

Zarządzanie dyskami SMART, sprawdzanie złych sektorów, dynamiczne mapowanie uszkodzonych sektorów,

Liczba iSCSI Targetów 128

Liczba iSCSI LUN 512

Zasilanie 2 x 500W

W ramach modernizacji infrastruktury należy dostarczyć:

- dyski twarde 15 szt dysków twardych dedykowanych do rozwiązań macierzowych o pojemności 4 TB każdy.

- 2 szt dyski cache do posiadanej przez zamawiającego macierzy synology RS2416

- należy dostarczyć pamięci do posiadanych przez zamawiającego:

Primergy RX200 S8 24 16 GB 1600 MHz, IBM x3250M4 6 x 8 GB 1333 MHz, 24 szt x 16 GB DDR4-2132 (1066 MHz).

4. Modernizacji systemu serwerowego, wirtualizacji i backupu o minimalnych parametrach:

System wirtualizacji o minimalnych parametrach:

1. Licencje powinny umożliwiać uruchomienie wirtualizacji na serwerach fizycznych na czas nieoznaczony dla dostarczanej w niniejszym postępowaniu infrastruktury serwerowej (4szt. serwerów obsadzone min. dwoma procesorami każdy).

2. Wszystkie licencje powinny być dostarczone wraz z wsparciem, tryb zgłoszeń 5x9, 4h zdalna reakcja

3. Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych

4. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.

5. Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.

6. Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 576 logicznych wątków oraz do 12TB pamięci fizycznej RAM.

7. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.

8. Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB.

9. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia do 6 TB pamięci operacyjnej RAM.

10. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.

11. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 32 porty szeregowo.
12. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
13. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista, Windows 2000, Windows Server 2003/R2, Windows Server 2008/R2, Windows Server 2012/R2, Windows Server 2016, Windows 7, Windows 8, Windows 8.1, Windows 10, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, Solaris, Oracle Enterprise Linux, Debian GNU/Linux, CentOS, FreeBSD, Asianux, NeoKylin Linux, CoreOS, Ubuntu, SCO OpenServer, SCO Unixware, Mac OS X.
14. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
15. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
16. 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 do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
17. 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.
18. Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
19. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
20. Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
21. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
22. Rozwiązanie musi zapewnić wbudowany, bezpieczny mechanizm do automatycznego tworzenia kopii zapasowych, odtwarzania wskazanych maszyn wirtualnych. Mechanizm ten musi umożliwiać również odtwarzanie pojedynczych plików z kopii zapasowej oraz zapewnia stosowanie deduplikacji dla kopii zapasowych. Mechanizm zapewnia możliwość wykonywania spójnych kopii zapasowych serwerów aplikacyjnych (Microsoft SQL Server, Microsoft Exchange Server, Microsoft SharePoint Server) oraz replikację kopii zapasowych.
23. Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych.

24. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
25. Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi.
26. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA) , aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
27. Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.
28. 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.
29. 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.
30. Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).

System do wykonywania kopii zapasowej

Wymagania ogólne

Licencja na czas nieoznaczony dla dostarczanej w niniejszym postępowaniu infrastruktury serwerowej (4szt. serwerów obsadzone min. dwoma procesorami każdy).

Wsparcie producenta na okres trwania gwarancji (dostęp do aktualizacji oprogramowania do nowszych wersji, pomoc producenta w zakresie konfiguracji i rozwiązywania problemów)

Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.0, 5.1, 5.5, 6.0, 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012, 2012 R2, 2016 oraz 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 Manager, klastrami hostów oraz pojedynczymi hostami.

Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V

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 mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji

Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla co najmniej trzech pamięci masowych w 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 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 nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania

Oprogramowanie musi zapewniać backup jednorzebiegowy - nawet w przypadku wymagania granularnego odtworzenia

Oprogramowanie musi zapewniać mechanizmy informowania o wykonaniu/błędzie zadania poprzez email lub SNMP. W środowisku VMware musi mieć możliwość aktualizacji pola „notatki” na wirtualnej maszynie

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 bezpośrednią integrację z VMware vCloud Director 8.x i 9.x i archiwizować metadane vCD. Musi też umożliwiać odtwarzanie tych metadanych do vCD.

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 jakiegokolwiek funkcjonalności wymienionej w tej specyfikacji

Oprogramowanie musi oferować zarządzanie kluczami w przypadku utraty podstawowego klucza

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.

Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej

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 automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora

Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn

Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server

Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej

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 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.

Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

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 posiadać takie same funkcjonalności replikacji dla Hyper-V

Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere

Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)

Oprogramowanie musi umożliwiać 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 niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych. Dla środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania

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 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 plików z następujących systemów plików:

Linux

ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs

BSD

UFS, UFS2

Solaris

ZFS, UFS

Mac

HFS, HFS+

Windows

NTFS, FAT, FAT32, ReFS

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 dowolnych obiektów i dowolnych atrybutów Active Directory włączając hasło, obiekty Group Policy, partycja konfiguracji AD, rekordy DNS zintegrowane z AD, Microsoft System Objects, certyfikaty CA oraz elementy 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 granularne odtwarzanie Microsoft SQL 2005 i nowsze włączając bazy danych z opcją odtwarzania point-in-time, tabele, schemat

Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze. Opcja odtworzenia elementów, witryn, uprawnień.

Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzania point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.

Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.

Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.

Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows

Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.

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.

W ramach modernizacji serwerowni Wykonawca zmodernizuje system klimatyzacji. Modernizacja obejmie serwerownie Urzędu Miasta Elku położone w piwnicach budynków przy ulicy Piłsudskiego 2 i Piłsudskiego 4. W ramach zadania wykonawca zdemontuje obecne zainstalowane klimatyzatory i zamontuje nowe klimatyzatory o następującej funkcjonalności:

W każdej z dwóch serwerowni Wykonawca zamontuje po dwie redundantne klimatyzacje o parametrach:

Minimalne parametry każdego z dwóch klimatyzatorów do dostarczenia i instalacji w serwerowni Piłsudskiego 4:

Wydajność Chłodzenie kW: 9,4

Moc elektryczna Chłodzenie max 3,5

Klasa efektywności energetycznej Chłodzenie A+

Maksymalny prąd pracy Chłodzenie 19,0

Osuszanie l/h 3,5

Przepływ powietrza Wewnętrzna m³/h 1380

Minimalne parametry każdego z dwóch klimatyzatorów do dostarczenia i instalacji w serwerowni Piłsudskiego 2:

Wydajność Chłodzenie kW: 14

Moc elektryczna Chłodzenie max 4,7

Klasa efektywności energetycznej Chłodzenie A++
Maksymalny prąd pracy Chłodzenie 28.0
Osuszanie l/h 4.5
Przepływ powietrza Wewnętrzna m3/h 1800

Zamawiający wymaga dostarczenia urządzeń, które będą dobrane w systemie N+1.

Klimatyzacje muszą być dedykowane do pracy całorocznej w serwerowniach.

Urządzenie musi być wyposażone w tzw. zestaw pracy całorocznej tj. regulator obrotów wentylatora oraz grzałkę karteru sprężarki. Pozwoli to na pracę urządzenia w trybie chłodzenia przy ujemnych temperaturach powietrza na zewnątrz.

Dodatkowo urządzenia będą wyposażone w zestaw pracy naprzemiennej, rezerwowej i kaskadowej co pozwoli na równomierną pracę obu urządzeń, a w przypadku awarii któregoś z urządzeń, drugie sprawne przejmie rolę głównego urządzenia, w przypadku znacznego zapotrzebowania na moc chłodniczą włączać się mają oba urządzenia. Przez system pracy naprzemiennej zamawiający rozumie system który w sposób automatyczny zapewnia pracę naprzemienną ze zmianą pracującego klimatyzatora co określony interwał czasowy.

Urządzenia muszą być wyposażone w system zdalnego monitoringu stanu urządzeń.

Kompletna instalacja klimatyzacji oraz wszystkie użyte urządzenia, muszą być objęte serwisem gwarancyjnym.

Zakres zadania dla systemu klimatyzacji obejmuje:

- wykonanie projektów wykonawczego, budowlanego (jeżeli niezbędny) i projektu powykonawczego
- dostawę wraz z kompleksom montażem, włącznie w wszelkimi niezbędnymi pracami budowlanymi
- pełną instalację rozprowadzenia powierza w pomieszczeniu
- szkolenie eksploatacyjne

Wymagania w zakresie obsługi gwarancyjnej klimatyzacji:

- niezbędne przeglądy w ciągu całego okresu obowiązywania gwarancji
- czas reakcji na zgłoszenie awarii maks. 48h,
- w ramach gwarancji Wykonawca zapewni wszystkie niezbędne przeglądy i konserwacje dostarczonych urządzeń.

W ramach zadania Wykonawca zdemontowane klimatyzatory z serwerowni przy ulicy Piłsudskiego 4 dokona ich przeglądu serwisowego, a następnie zamontuje w kontenerze telekomunikacyjnym położonym przy kominie PEC w którym to Wykonawca będzie instalował zakończenia połączeń opisanych w ramach punktu „5. System bezpieczeństwa transmisji danych”.

5. System bezpieczeństwa transmisji danych o minimalnych parametrach:

System ma umożliwiać pracę zarówno w paśmie uwolnionym jak i licencjonowanym bez konieczności zmian sprzętu. Stacja bazowa systemu radiowego Punkt-Wielopunkt (PmP) składająca się sektorów zainstalowana zostanie na kominie żelbetowym PEC zlokalizowanym w Ełku przy ulicy Ciepłej. Komin o wysokości 120m jest własnością gminy Miasta Ełk Na kominie istnieje przygotowana infrastruktura montażowa. Anteny mają być mocowane na

wysokości ok. 80m npt. Kabel sygnałowe łączące urządzenia zewnętrzne i wewnętrzne mocowane będą do istniejącej drabiny kablowej zainstalowanej na kominie. Kable należy układać w peszlu odpornym na warunki atmosferyczne oraz mocować za pomocą opasek stalowych. Peszel należy trwale oznaczyć w celu identyfikacji właściciela. Mocowania do drabiny co ok. 0,5m, aż do podstawy komina. Pomiędzy kominem a szafą zewnętrzną, należącą do Zamawiającego, kable należy prowadzić pod ziemią w rurze arota o średnicy min 100 mm. Rura musi być zabezpieczona przed wnikaniem wody. Wejście do szafy telekomunikacyjnej za pomocą otworu w fundamencie. Rozbudowa Głównego Punktu Nadawczego (GPN) który znajduje się na kominie PEC w Elku przy ulicy Ciepłej. W ramach zadania Wykonawca wykona:

1. Na galerii komina PEC 80 m instalacja szafki teletechnicznej odpornej na warunki atmosferyczne z grzaniem i termoregulatorem.
2. Do szafki dociągnięcie i zakończenie z kontenera teletechnicznego zlokalizowanego na dole komina niezbędną infrastrukturę.

Należy dostarczyć zamontować, skonfigurować i uruchomić:

Minimalne wymagania techniczne dla stacji bazowej złożonej z 4 szt. sektorów:

1. System radiowy punkt-wielopunkt pracujący w paśmie 5.4-5.7 GHz zgodny z EN 301 893 oraz 5.7-5.8 GHz zgodny z EN 302 502;
2. Dostęp czasowy TDD (Time Division Duplex);
3. Pojemność stacji bazowej czterosektorowej co najmniej 3 Gb/s;
4. Możliwość podłączenia co najmniej 256 użytkowników;
5. Modułacja MIMO-OFDM BPSK/QPSK/16QAM/64QAM/256QAM;
6. Korekcja błędów FEC $k= 1/2, 2/3, 3/4, 5/6$;
7. Adaptacyjna modułacja i kodowanie
8. Adaptacyjna zmiana szerokości kanału co najmniej 20/40/80 MHz;
9. Asymetryczny przydział ruchu w kierunku Uplink co najmniej 85%;
10. Obsługiwana szerokość ramki co najmniej 2048 bajtów;
11. Wbudowane szyfrowanie co najmniej AES 128;
12. Synchronizacja czasowa stacji bazowej za pomocą GPS (Global Positioning System);
13. Aktywna antena sektorowa beamforming formująca wąską wiązkę dla transmisji uplink oraz downlink o zysku co najmniej 20 dBi;
14. Adaptacyjne MIMO 2x2 oraz Diversity;
15. Wbudowany analizator widma;
16. Interfejsy IDU Ethernet co najmniej 1x 1000BaseT oraz 1x SFP;
17. Możliwość lokalnej i zdalnej aktualizacji oprogramowania;
18. Zarządzanie za pomocą protokołów IPv4 oraz IPv6; HTTP, SNMP v3;
19. Obsługa QoS poziom 4 zgodnie z 802.1p i Diffserv;
20. Obsługa VLAN 802.1Q, 802.1P, QinQ oraz IGMP;
21. Zasilanie PoE (Power over Ethernet);
22. Pobór mocy <30 W;
23. Klasa szczelności co najmniej IP67;
24. Temperaturowy zakres pracy co najmniej od -35°C do 60°C;

W ramach zadania należy dostarczyć 17 szt. stacji klienckiej o minimalnych parametrach:

1. Dostęp czasowy TDD (Time Division Duplex);
2. Zwiłokrotnienie OFDM (Orthogonal Frequency Division Multiplexing);
3. Adaptacyjne MIMO 2x2 oraz Diversity;
4. Modułacja MIMO-OFDM BPSK/QPSK/16QAM/64QAM/256QAM;
5. Przepustowość co najmniej 100Mb/s z możliwością rozbudowy do 200Mb/s bez konieczności wymiany sprzętu;
6. Możliwość konfigurowania CIR (committed Information Rate);
7. Korekcja błędów FEC $k = 1/2, 2/3, 3/4, 5/6$;
8. Zintegrowana antena o zysku co najmniej 22 dBi;
9. Wbudowane szyfrowanie AES 128;
10. Obsługa QoS poziom 4 zgodnie z 802.1p i Diffserv dla Uplink i Downlink;
11. Obsługa VLAN 802.1Q, 802.1P, QinQ dla Uplink i Downlink;
12. Dostępny interfejs Ethernet co najmniej 10/100BaseT;
13. Możliwość pracy jako Hub w warstwie 2;
14. Możliwość lokalnej i zdalnej aktualizacji oprogramowania;
15. Zarządzanie za pomocą dedykowanego oprogramowania, przeglądarki internetowej oraz przy pomocy protokołów SNMP v3;
16. Zasilanie stacji bazowej poprzez PoE (Power over Ethernet);
17. Pobór mocy urządzeń radiowych <9W;
18. Klasa szczelności urządzeń radiowych IP67;
19. Temperaturowy zakres pracy co najmniej od -35°C do 60°C;

Wykonawca dostarczy dwa kompletne linki radiowe które zamontuje i uruchomi pomiędzy Kominem PEC, a masztem Zamawiającego zlokalizowanego na wieżowcu przy ulicy Wojska Polskiego 60 oraz pomiędzy Kominem PEC, a budynkiem przy ulicy Baranki 24

Wymagania techniczne dla linków radiowych

Obsługiwane pasmo częstotliwości 5.4-5.7 GHz zgodny z EN 301 893 oraz 5.7-5.8 GHz zgodny z EN 302 502;

1. Dostęp czasowy TDD (Time Division Duplex);
2. Zwiłokrotnienie OFDM (Orthogonal Frequency Division Multiplexing);
3. Wykorzystanie technik antenowych MIMO 2x2 oraz Diversity;
4. Obsługiwane modulacje BPSK/QPSK/16QAM/64QAM;
5. Obsługiwane szerokości kanałów 10, 20, 40MHz;
6. Adaptacyjna modulacja i kodowanie;
7. Przepływność co najmniej 750Mb/s;
8. Maksymalne opóźnienia End-to-End <3ms;
9. Korekcja błędów min. FEC $k = 1/2, 2/3, 3/4, 5/6$;
10. Maksymalna szerokość ramki 2048 bajtów;
11. Wydajność sprzętowa co najmniej 360.000 PPS (Packets Per Second);
12. Sprzętowe szyfrowanie AES 128;
13. Możliwość synchronizacji czasu TDD przez Ethernet;
14. Możliwość konfigurowania QoS 4-go poziomu zgodnie z 802.1p i Diffserv;
15. Możliwość konfigurowania VLAN zgodnie z 802.1Q, 802.1P, QinQ;
16. Wbudowany analizator widma dla polaryzacji V oraz H;

17. Dostępne interfejsy sieciowe Ethernet 10/100BaseT, 1000BaseT;
18. Możliwość lokalnej i zdalnej aktualizacji oprogramowania;
19. Zarządzanie radiolinia za pomocą dedykowanego oprogramowania, przeglądarki internetowej oraz protokołów SNMP (wersja 2c lub wyższa) i Telnet;
20. Pobór mocy <35W (IDU+ODU);
21. Klasa szczelności urządzeń radiowych ODU IP67;
22. ODU z zintegrowaną anteną o zysku co najmniej 23dBi
23. Temperaturowy zakres pracy od -35°C do 60°C;

6. Przełącznik rdzeniowy - 2szt o minimalnych parametrach:

Zamawiający wymaga dostarczenia przełączników rdzeniowych - brzegowych o następujących parametrach:

1. Wydajność pojedynczego switcha nie może być mniejsza niż:
 - a) 700 Gbps (full-duplex, switch fabric)
 - b) 700 Mpps (full-duplex, wydajność przełączania).
2. Wyposażonych w dwa zasilacze AC (redundancja 1+1); możliwa wymiana na zasilacze DC 48V; przepływ powietrza front-to-back.
3. Wyposażonych w minimum 24 porty 10G w standardzie SFP+ umożliwiające obsadzenie wkładkami SFP (1G) oraz SFP+ (10G).
4. Wyposażonych w minimum 24 porty 1G w standardzie SFP (1G).
5. Umożliwiających rozbudowę o dodatkowe minimum 6 portów 100G w standardzie QSFP-28 (za pomocą karty lub licencji).
6. Obsługa routingu IPv4 oraz IPv6.
7. Rozmiar tablicy RIB – co najmniej 8M wpisów.
8. Rozmiar tablicy FIB – co najmniej 1M wpisów.
9. Rozmiar tablicy MAC – co najmniej 750k adresów.
10. Musi obsługiwać minimum osiem kolejek QoS dla każdego portu liniowego.
11. Musi obsługiwać protokół umożliwiający gromadzenie i eksportowanie informacji o zbiorach pakietów IP posiadających wspólne cechy, tj. adres źródłowy, adres docelowy, port źródłowy, port docelowy, identyfikator interfejsu, BGP AS-Path itp. (np. protokół NetFlow, sFlow, jFlow, IPFIX).
12. Musi obsługiwać protokół First Hop Redundancy Protocol (np. VRRP-E) wraz z obsługą funkcji Short-Path-Forwarding tak, aby tworzyć topologię Active-Active i nie zawracać ruchu z routera Standby do routera Master.
13. Dla linków LACP musi pozwalać na utworzenie logicznego połączenia z wielu połączeń fizycznych współdzielonych pomiędzy co najmniej dwoma urządzeniami fizycznymi (protokół multi-chassis LAG – MC-LAG lub dowolny inny protokół rozszerzający protokół LACP zgodnie ze standardem IEEE 802.1AX-2008).
14. Musi obsługiwać co najmniej następujące protokoły warstwy 3 modelu OSI, realizowane zarówno dla IPv4 jak i IPv6: BGP (w tym ASN-y 32-bitowe, BFD oraz MP-BGP), OSPF v2+v3 oraz IS-IS. Wspomniane protokoły muszą również działać per VRF.
15. Musi obsługiwać protokół MPLS wraz z protokołami LDP, RSVP i VPLS.
16. Musi obsługiwać implementację EBGp-EVPN.
17. Musi obsługiwać tunelowanie ruchu – protokoły VXLAN oraz GRE.

18. Musi obsługiwać możliwość przycinania pasma (tzw. rate-limit) dla ruchu wychodzącego i przychodzącego.
19. Musi obsługiwać minimum 4000 interfejsów L3.
20. Musi wspierać minimum 250 adresów typu „secondary” na interfejsach L3.
21. Musi obsługiwać minimum 2300 jednoczesnych sesji BGP.
22. Musi obsługiwać minimum 500 VRF.
23. Musi obsługiwać minimum 90000 wpisów ARP.
24. Musi obsługiwać minimum 700000 adresów MAC.
25. Musi posiadać głębokie bufor pakietowe – minimum 6GB dla portów liniowych dla obsługi chwilowych spiętrzeń ruchu.
26. Musi wspierać protokoły zdalnej konfiguracji – NETCONF oraz REST.
27. Musi wspierać protokoły Multicast – IGMP v1/v2/v3 (RFC 1112/RFC 2236/RFC 3376), oraz PIM-SM (RFC 4601) i PIM-SSM(RFC 4607).
28. Musi wspierać VLAN Switching lub VLAN Bridge’ing oraz protokoły Spanning-Tree – IEEE 802.1s (MSTP) oraz IEEE 802.1w (Rapid STP).
29. Musi umożliwiać uruchomienie własnej maszyny VM na urządzeniu. W tym celu urządzenie musi udostępniać minimum 128 GB Flash SSD oraz wspierać architekturę x86 dla maszyny VM. Dodatkowo router musi zapewniać dedykowany interfejs analityczny o wydajności minimum 10 Gbps pomiędzy Data Plane, a VM – gdzie może zostać kopiowany (Mirror) określony ruch z portów liniowych na potrzeby np. wykrywania ataków DDoS.
30. Architektura musi zapewnić rozdzielenie funkcji przesyłania danych (Data Plane) od funkcji zarządzania urządzeniem (Control Plane).
31. Dla warstwy kontrolnej (Control Plane), musi realizować sprzętowy, konfigurowalny mechanizm ochrony przed atakami cyberwandalizmu (DoS/DDoS) – tzw. control-plane policing (CoPP) – oraz sprzętową obsługę list dostępu (ACL).
32. Musi obsługiwać protokoły IPv4 i IPv6. Przełączanie pakietów na kartach liniowych musi być realizowane bez konieczności przesyłania pakietów do modułu kontrolnego (Control-Plane), tj. Router musi realizować funkcję routingu i switchingu sprzętowo, niezależnie od kart kontrolujących.
33. Po zamontowaniu w szafie lub stojaku 19”, nie może zajmować więcej niż 1U wysokości.
34. Musi mieć dodatkowy port Ethernet, dedykowany dla zarządzania urządzeniem w trybie out-of-band.
35. Dostęp poprzez CLI (linia poleceń) realizowany protokołem telnet oraz SSH v2 oraz za pomocą konsoli szeregowej RS-232,
36. Obsługa protokołu SNMP v2 i v3,
37. Możliwość pobrania konfiguracji do zewnętrznego komputera typu PC w formie tekstowej, możliwość ponownego zaimportowania do urządzenia i uruchomienia konfiguracja po dokonaniu edycji poza urządzeniem, możliwość wyszukiwania fragmentów konfiguracji z linii poleceń,
38. Obsługa wielu poziomów dostępu do systemu operacyjnego przełącznika z różnymi poziomami uprawnień; realizacja lokalna lub przez system AAA/TACACS
39. Musi być wyposażony we wszystkie licencje oprogramowania wewnętrznego, które pozwalają na realizację wszystkich wyżej wymienionych funkcji bez konieczności dokupowania dodatkowych kluczy licencyjnych.

40. Przełącznik musi być natywnie wspierany przez posiadany przez Zamawiającego system zarządzania Extreme Networks XMC oraz kontroli dostępu do sieci EAC. Oprócz standardowej obsługi takiej jak widoczność urządzenia i jego konfiguracja musi być możliwość korzystania z funkcjonalności IGE, która jest częścią pakietu XMC.

7. Przełącznik sieciowy - 4 szt o minimalnych parametrach:

Przełącznik posiadający 48 portów 1G 10/100/1000BASE-T oraz dodatkowo minimum 2 porty 1/10 Gigabit Ethernet SFP+

Przełącznik musi być kompatybilny z posiadany przez zamawiającego systemem kontroli dostępu do sieci Extreme Networks XMC szczególności musi zapewniać:

Narzędzie do zarządzania na poziomie systemowym - umożliwiające implementację dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia

Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej aplikacji, poprzez wykonanie jednej czynności, dzięki której polityki zostaną rozesłane do wszystkich urządzeń

Pod pojęciem polityka Zamawiający rozumie wielowarstwową klasyfikację ramek która pozwala administratorowi kontrolować ruch za pomocą reguł klasyfikacji w punkcie wejścia dla systemu końcowego. Pozwala to na dynamiczną implementację dowolnej liczby akcji w dowolnej kombinacji atrybutów warstwy 2, 3 lub 4 w pakietach. Zastosowanie polityk musi umożliwić także Multi-User Authentication oraz Multi-Method Authentication czyli uwierzytelnienie wielu użytkowników na jednym porcie przy zastosowaniu różnych metod uwierzytelniania, przy zastosowaniu następujących akcji: odrzucanie ruchu, zezwalanie na ruch, wprowadzanie priorytetyzacji ruchu, przypisanie do VLAN.

Przełącznik musi być wyposażony w zasilanie PoE niezbędne do zasilania punktów dostępowych WLAN, kamer oraz innych urządzeń PoE w standardzie 802.3at oraz 802.3af

Przełącznik musi zapewniać, standard 802.3at jednocześnie na wszystkich 48 portach 1G 10/100/1000BASE-T

Przełącznik ma oferować zgodnie ze standardem 802.3af jednocześnie na wszystkich 48 portach 1G 10/100/1000BASE-T np. poprzez zastosowanie dodatkowego źródła zasilania

Przełącznik musi mieć możliwość doposażenia w system redundantnego zasilania zapewniający normalną pracę urządzenia oraz zasilanie dla wszystkich portów PoE

Przełącznik musi obsługiwać optykę 10GBase-SR, 10GBase-LR, 10GBase-ER, 10GBase-LRM

Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T

Wysokość urządzenia 1U

Przełącznik musi posiadać wbudowany zasilacz 230V AC

Nieblokującą architekturę o wydajności przełączania minimum 150 Gb/s

Szybkość przełączania minimum 100 Milionów pakietów na sekundę

Łączenie minimum 6 przełączników w stos

Realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR oraz włókien światłowodowych

Tablica MAC adresów minimum 16k

Pamięć operacyjna: minimum 1GB pamięci DRAM

Pamięć flash: minimum 2GB pamięci Flash

Pojemność bufora pakietów minimum 2MB
Obsługa sieci wirtualnych IEEE 802.1Q – minimum 4000
Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
Wsparcie dla ramek Jumbo Frames (minimum 9216 bajtów)
Obsługa Q-in-Q IEEE 802.1ad
Obsługa Quality of Service
IEEE 802.1p
DiffServ
8 kolejek priorytetów na każdym porcie wyjściowym
Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
Wbudowany DHCP serwer i klient
Instalacja minimum dwóch wersji oprogramowania - firmware
Przechowywanie minimum kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
Monitorowanie zajętości CPU
Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
Obsługa Routingu IPv4
Sprzętowa obsługa routingu IPv4 – forwarding
Pojemność tabeli routingu minimum 400 wpisów
Routing statyczny
Obsługa routingu dynamicznego IPv4
RIPv1/v2
OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania
Policy Based Routing dla IPv4
Obsługa DHCP/BootP Relay dla IPv4
Obsługa Routingu IPv6
Sprzętowa obsługa routingu IPv6 – forwarding
Pojemność tabeli routingu minimum 210 wpisów
Routing statyczny
Obsługa routingu dynamicznego dla IPv6
RIPng
OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania
Obsługa MLDv1 (Multicast Listener Discovery version 1)
Obsługa MLDv2 (Multicast Listener Discovery version 2)
Policy Based Routing dla IPv6
Obsługa DHCP/BootP Relay dla IPv6
Opcja IPv6 Router Advertisement dla DNS - RFC 6106
Obsługa Multicastów

Statyczne przyłączenie do grupy multicast
Filtrowanie IGMP
Obsługa Multicast VLAN Registration - MVR
Obsługa IGMP v1 (RFC 1112)
Obsługa IGMP v2 (RFC 2236)
Obsługa IGMP v3 (RFC 3376)
Obsługa IGMP v1/v2/v3 snooping
Bezpieczeństwo
Obsługa Network Login
IEEE 802.1x - RFC 3580
Web-based Network Login
MAC based Network Login
Obsługa wielu klientów (minimum 4) Network Login na jednym porcie (Multiple supplicants)
Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control)
Obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
Obsługa Guest VLAN dla IEEE 802.1x
Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos
Wbudowana obrona procesora urządzenia przed atakami DoS
Obsługa TACACS+ (RFC 1492)
Obsługa RADIUS Authentication (RFC 2138) (RFC 2865)
Obsługa RADIUS Accounting (RFC 2139) (RFC 2866)
RADIUS and TACACS+ per-command Authentication
Bezpieczeństwo MAC adresów
ograniczenie liczby MAC adresów na porcie
zatrzaśnięcie MAC adresu na porcie
możliwość wpisania statycznych MAC adresów na port/vlan
Funkcja wyłączenia MAC learning
Obsługa SNMPv1/v2/v3
Klient SSH2
Zabezpieczenie przełącznika przed atakami DoS
Networks Ingress Filtering RFC 2267
SYN Attack Protection
Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4
Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
Obsługa bezpiecznego transferu plików SCP/SFTP
Obsługa DHCP Option 82
Obsługa Gratuitous ARP Protection

Obsługa Trusted DHCP Server
Obsługa DHCP Snooping
Obsługa DHCP Secured ARP/ARP Validation
Obsługa powyższych funkcji IP Security na portach Network Login IEEE 802.1x
Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s
Bezpieczeństwo sieciowe

Konfiguracja portu głównego i zapasowego
Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
Obsługa STP (Spanning Tree Protocol) IEEE 802.1D
Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
Obsługa PVST+
Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
Obsługa G.8032
Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
Zarządzanie
Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)
Obsługa synchronizacji czasu NTP
Zarządzanie przez SNMP v1/v2/v3
Zarządzanie przez przeglądarkę WWW – protokół http i https
Telnet Serwer/Klient dla IPv4 / IPv6
SSH2 Serwer/Klient dla IPv4 / IPv6
Ping dla IPv4 / IPv6
Traceroute dla IPv4 / IPv6
Obsługa SYSLOG z możliwością definiowania wielu serwerów
Sprzętowa obsługa sFlow
Obsługa RMON minimum 4 grupy: Status, History, Alarms, Events (RFC 1757)
Obsługa RMON2 (RFC 2021)
Inne
Obsługa skryptów CLI
Edycja skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
Uruchamianie skryptów
Ręcznie
O określonym czasie lub co wskazany okres czasu
Na podstawie wpisów w logu systemowym

Wdrożenie

1) Instalacja:

- a) Instalacja dostarczonego sprzętu w szafie rack w siedzibie Zamawiającego
- b) Podłączenie macierzy dyskowej i serwerów z posiadaną przez Zamawiającego infrastrukturą

2) Konfiguracja:

a) Przed przystąpieniem do prac wdrożeniowych Wykonawca przedstawi do zaakceptowania Zamawiającemu koncepcję wdrożenia wszystkich elementów objętych zamówieniem.

b) Konfiguracja dostarczonych serwerów, macierzy dyskowej i oprogramowania, w celu uruchomienia protokołu Fiber Channel – wymagana jest pełna konfiguracja hypervisora oraz dostarczonych systemów operacyjnych i sprzętu. Wszystkie elementy muszą być podłączone interfejsami optycznymi do dostarczanych przełączników rdzeniowych. Zamawiający wymaga takiej konfiguracji, aby zapewnić wielościeżkowość dla serwera i macierzy dyskowej. System musi działać w klastrze wysokiej dostępności. Połączenie pomiędzy serwerami a macierzą,

c) W zakresie konfiguracji należy również dokonać zmian konfiguracji posiadanego przez Zamawiającego system zarządzania siecią oraz systemu kontroli dostępu do sieci klasy NAC. Zamawiający posiada system Extreme Networks ExtremeControl.

3) Podłączenie wszystkich elementów zgodnie z zaakceptowaną przez Zamawiającego koncepcją wdrożenia.

4) Uruchomienie kanału zdalnego zarządzania całą dostarczoną infrastrukturą na posiadanym przez Zamawiającego urządzeniu Fortigate 900D. Urządzenie UTM należy skonfigurować w taki sposób aby ruch do strefy serwerowej był skanowany wbudowanymi mechanizmami bezpieczeństwa urządzenia.

5) Konfiguracja wirtualizacji

a) Środowisko oparte o 2 serwery fizyczne oraz współdzielony zasób macierzowy.

b) Konfiguracja klastra HA dla maszyn wirtualnych na 2 maszynach fizycznych

c) Automatyczne przenoszenie i uruchomienie maszyn wirtualnych podczas awarii jednego z serwerów fizycznych na host nieuszkodzony.

d) Konfiguracja wirtualnych switchy (podział na 4 podsieci: BACKUP, DMZ, LAN, MGMT)

6) Konfiguracja routingu BGP na dostarczonych urządzeniach Konfiguracja protokołu BGP powinna składać się z 4 etapów:

a) Analiza aktualnej konfiguracji BGP.

Szczegółowa analiza aktualnej konfiguracji, przeprowadzenie testów zbieżności, testów przełączania pomiędzy ISP, analiza tablicy routingu, weryfikacja atrybutów

b) Konfiguracja protokołu BGP na routerch brzegowych

klaster routerów

konfiguracja agregacji portów

konfiguracja VLAN-ów

konfiguracja prawidłowego AS klienta

konfiguracja adresacji interfaceów w celu utworzenia relacji sąsiedztwa BGP

dodanie niezbędnych prefix-list

rozgłaszanie trasy do Internetu.

zastosowanie narzędzi kontroli ruchu (Local preference, Meric (MED), AS-PATH prepend)

Konfiguracji ma na celu wprowadzenie redundancji po stronie klienta jak i po stronie ISP.

c) Testy, optymalizacja protokołu BGP i analiza konfiguracji po przełączeniu na nowe routery.

Powinny zostać przeprowadzone testy takie same jak w etapie I , wyniki powinny zostać porównane i jeśli będzie taka potrzeba, powinna zostać przeprowadzona optymalizacja protokołu BGP.

d) Rekonfiguracja routera który obsługiwał protokół BGP

Przeznaczeniem routera rdzeniowego jest routowanie ruchu tylko sieci lokalnej. Niezbędne będzie czyszczenie pozostałej konfiguracji protokołu BGP oraz , prawidłowe przełączenie urządzenia do pracy jako główny router sieci lokalnej.

7) Po dokonaniu całości wdrożenia należy

a) przeprowadzić testy poprawności działania całej infrastruktury

b) przygotować dokumentację powykonawczą zawierającą listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów

c) Ze względu na krytyczne aplikacje które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

urządzenia dedykowane (embeded), na przykład routerów i przełączniki;

punkty styku z sieciami obcymi;

zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz.

Ponadto Oferent przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:

określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;

wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;

wskazanie potencjalnie niebezpiecznego oprogramowania znajdującego się w badanym systemie.

Badaniu będą podlegały następujące systemy:

rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);

Linux 2.4.x, 2.6.x, 3.x.x;

IBM AIX;

CISCO IOS;

Microsoft SQL;

MySQL;

Badanie zostanie zakończone raportem. Forma i zakres raportu musi być zaakceptowany przez dział informatyki Zamawiającego przed zakończeniem projektu.

8) Wykonawca w ramach zadania dostarczy wszystkie niezbędne elementy wymagane do podłączenia całej dostarczanej infrastruktury w tym w szczególności:

a) Moduły SFP+

b) Przewody optyczne

c) Przewodu zasilające

d) Kable krosowe UTP

9) Ze względu na krytyczne aplikacje i systemy które będą uruchomione i skonfigurowane na nowej infrastrukturze Zamawiający wymaga aby Wykonawca posiadał niezbędne doświadczenie oraz potencjał kadrowy:

a) Przynajmniej jednym inżynierem posiadający certyfikat producenta posiadanego przez Zamawiającego urządzenia UTM Fortigate w zakresie administrowania i konfiguracji urządzenia: NSE 4 Network Security Professional lub równoważny

b) Przynajmniej jeden inżynier posiadających aktualny certyfikat producenta posiadanych przez Zamawiającego urządzeń sieciowych Extreme Networks w zakresie administrowania i konfiguracji: Extreme Certified Expert – Networking lub równoważny

c) Przynajmniej jeden inżynier posiadających aktualny certyfikat producenta posiadanego oprogramowania Extreme Networks Extreme Control w zakresie administrowania i konfiguracji.

Extreme Certified Specialist – Extreme Control lub równoważny

d) Przynajmniej jeden inżynier posiadających aktualny certyfikat producenta dostarczonego oprogramowania do wirtualizacji w zakresie administrowania i konfiguracji.

Zamawiający dopuszcza aby jedna osoba posiadała wszystkie powyższe certyfikaty.

10) Warunki wdrożenia:

a) Wdrożenie musi być przeprowadzone w taki sposób, aby nie zakłócało bieżącej działalności Zamawiającego. Wszystkie urządzenia muszą pochodzić z legalnego źródła oraz zostać zakupione w autoryzowanym kanale sprzedaży producenta na terenie Unii Europejskiej. Sprzęt musi być fabrycznie nowy i nie może pochodzić z dostawy do realizacji projektu u innego klienta.