SPECYFIKACJA TECHNICZNA

Serwer – 2 sztuki:

Lp.	Parametr	Wymagania minimalne
1	Budowa	Obudowa Rack o wysokości max 1U z możliwością instalacji do 8 dysków 2.5" Hot-Plug wraz z kompletem wysuwanych szyn i organizerem kabli, umożliwiająca montaż w szafie rack i wysuwanie serwera do celów serwisowych.
2	Procesor	Zainstalowany minimum jeden procesor szesnastordzeniowy, trzydziestodwuwątkowy, klasy x86, dedykowany do pracy z zaoferowanym serwerem, umożliwiający osiągnięcie wyniku min. 71 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org (wynik dla oferowanego modelu serwera, dla jednego procesora).
3	RAM	128GB DDR4 RDIMM 2666MT/s w modułach 32GB. Płyta główna wyposażona w minimum 16 slotów przeznaczonych do instalacji pamięci.
4	Gniazda rozszerzeń	Serwer wyposażony w dwa złącza PCIe x16, Gen3
5	Interfejsy sieciowe	Minimum 6 interfejsów 1Gb Ethernet w standardzie BaseT. Interfejsy sieciowe muszą być umieszczone na co najmniej dwóch fizycznych kartach sieciowych umieszczonych w osobnych slotach. Minimum 2 porty Fibre Channel 16Gbit/s umożliwiające bezpośrednie podpięcie macierzy lub przełączników SAN.
6	Kontroler dysków	Sprzętowy RAID, zgodny z oferowanym serwerem, z możliwością obsługi 2GB cache, poziomów RAID 0, RAID 1, RAID 5, RAID 10, RAID 50, standardu SAS 12Gb/s i posiadający minimum 8 kanałów .
7	Dyski twarde	Zainstalowane 2 dyski 120GB SSD SATA o poziomie wytrzymałości minimum 1 DWPD
8	Zasilacze	Min 2 redundantne zasilacze Hot Plug o mocy minimum 450W każdy
9	Karta zarządzająca	Zainstalowana w dedykowanym slocie karta zarządzająca niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane złącze RJ-45 i umożliwiająca: - zdalny dostęp do graficznego interfejsu Web karty zarządzającej - zdalne monitorowanie i informowanie o statusie serwera - szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika - możliwość podmontowania zdalnych wirtualnych napędów - wirtualną konsolę z dostępem do myszy, klawiatury - wsparcie dla WSMAN (Web Service for Managament); SNMP; IPMI2.0, VLAN tagging, Telnet, SSH - możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer - możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer - integracja z Active Directory - wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej
10	Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001. Serwer musi posiadać deklarację CE. Serwer musi być

		wyszczególniony na liście kompatybilności HCL oferowanego wraz z serwerem wirtualizatora (dla najnowszej wersji). Serwer musi być zgodny z systemami Windows Server 2012 R2, 2016 oraz RedHat (potwierdzone przez producentów)
11	Gwarancja	Gwarancja świadczona przez producenta serwera, obejmująca min. 3 lata, realizowana w miejscu instalacji sprzętu, z czasem reakcji maksymalnie w następnym dniu roboczym. Możliwość rozszerzenia gwarancji świadczonej przez producenta serwera o kolejne lata. Możliwość rozszerzenia gwarancji świadczonej przez producenta serwera o wyższy wariant (np. 24x7x365).

Macierz – 1 sztuka:

Lp.	Parametr	Wymagania minimalne
	Budowa	Obudowa Rack o wysokości max 2U z możliwością instalacji do 24 dysków 2.5" Hot-Plug wraz z kompletem szyn, umożliwiająca montaż w szafie rack.
	Kontrolery	Macierz wyposażona w dwa redundantne kontrolery, działające w trybie active/active z lustrzanymi kopiami pamięci podręcznej. Każdy kontroler musi być wyposażony w co najmniej 4GB pamięci cache z podtrzymywaniem bateryjnym, chronionej przez układ flash zapewniający trwałość danych. Dostępna możliwość dwukrotnego zwiększenia pojemności pamięci cache bez użycia dysków SSD.
	RAID	RAID 0, 1, 10, 5 i 6. Możliwość zarządzania dyskami ulokowanymi w grupach RAID oraz w dynamicznych pulach dyskowych.
	Dyski	Obsługa dysków: Dyski SAS 2,5" o prędkości 15 tys. obr./min i pojemności 300 GB, 600 GB Dyski NL-SAS 2,5" o prędkości 10 tys. obr./min i pojemności 600 GB, 900 GB, 1,2 TB oraz 1,8 TB Dyski NL-SAS 2,5" o prędkości 7,2 tys. obr./min i pojemności 1 TB oraz 2 TB Dyski SSD 2,5" o pojemności 200 GB, 400 GB, 800 GB, 1,6 TB Macierz musi mieć możliwość obsługi minimum do 192 dysków.
	Zainstalowane dyski	Zainstalowane minimum 13 dysków 1,2 TB 10 tys. obr./min.
	Hot-Spare	Możliwość definiowania dysków Hot-Spare lub użycia dystrybuowanej przestrzeni, zarezerwowanej dla odtwarzania danych, ulokowanej na każdym z dysków.
	Porty	Obsługa standardu FC 16Gbit i zainstalowane porty SAS do obsługi dodatkowych półek dyskowych. Co najmniej 4 porty FC 16Gbit per kontroler. Co najmniej 4 porty macierzy obsadzone wkładkami FC 16Gbit.
	Zasilanie	2 redundantne zasilacze
	Zgodność	Zgodność z technologiami VASA, VAAI oraz ODX, VASA. Dostępny plugin dla vCenter do integracji z macierzą. Obsługa replikacji synchronicznej i asynchronicznej, do 512 snapshotów, obsługa dysków SED (niektóre opcje mogą wymagać zakupu dodatkowych licencji)

	Gwarancja	Gwarancja świadczona przez tego samego producenta co serwer, obejmująca min. 3 lata, realizowana w miejscu instalacji sprzętu, z czasem reakcji maksymalnie w następnym dniu roboczym. Możliwość rozszerzenia gwarancji świadczonej przez producenta macierzy o kolejne lata. Możliwość rozszerzenia gwarancji świadczonej przez producenta macierzy o wyższy wariant (np. 24x7x365).

System wirtualizacji – 1 komplet:

- Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych
- Licencje powinny obejmować min. trzy co najmniej dwuprocesorowe serwery i oraz serwer zarządzający oraz posiadać okres wsparcia producenta minimum rok. Wsparcie serwisowe musi dawać możliwość korzystania z pomocy technicznej oraz dawać możliwość pobierania i instalacji nowych wersji zakupionego oprogramowania.
- Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-128 procesorowych.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych
  z możliwością przydzielenia do 1 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 co najmniej 4 porty szeregowe i 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 powinno być w możliwie największym stopniu niezależne od producenta platformy sprzętowej.
- Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Licencjonowanie nie może odbywać się w trybie OEM.
- 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 dyskach lokalnych serwera lub na macierzy.
- 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, nie wymagająca dodatkowej licencji na system operacyjny.

- 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.
- Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
- Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- Oprogramowanie do wirtualizacji oraz oprogramowanie zarządzające muszą posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
- Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (np. wgrywania krytycznych poprawek) bez potrzeby wyłączania wirtualnych maszyn.
- Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.
- Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 4 lub więcej takich procesów przenoszenia jednocześnie.
- Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
- 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)

System backupu – 1 komplet:

Wymagania ogólne

- Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0, 6.5 oraz Microsoft Hyper-V 2012, 2012 R2 i 2016. 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 wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V

Całkowite koszty posiadania

- Oprogramowanie musi być licencjonowanie w modelu "per-CPU". Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiekolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone
- 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 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 jednoprzebiegowy - 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 akutalizacji 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 zapewniać bezpośrednią integrację z VMware vCloud Director 5.5, 5.6, 8.0, 8.10, 8.20, 9.0 i archiwizować również 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 jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
- 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 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 plików na taśmy
- 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 wspierać BlockClone API w przypadku użycia Windows Server 2016 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)

Wymagania RTO

- Oprogramowanie musi umożliwić 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 srodowiska 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.
- 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 obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
- 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.
- Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze.
- 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
- Licencje na oprogramowanie muszą objąć wszystkie systemy uruchomione na dostarczonym sprzęcie oraz posiadać okres wsparcia producenta minimum rok. Wsparcie serwisowe musi dawać możliwość korzystania z pomocy technicznej oraz dawać możliwość pobierania i instalacji nowych wersji zakupionego oprogramowania.

Oprogramowanie systemowe – 1 komplet:

Rozbudowa posiadanych licencji Microsoft Windows o:

8 licencji Windows 2016 Standard
50 CAL Windows Server 2016
Wszystkie licencje w wariancie licencjonowania Open GOV.

Przełącznik sieciowy typ 1 – 2 sztuki:

L.p	Warunek	Opis
1	Ilość portów	min. 48 portów 10/100/1000, 4 porty SFP
2	Obudowa	wieżowa 1U umożliwiająca instalację w szafie 19"
3	Rozmiar tablicy adresów MAC	min. 16 000 pozycji
4	Rozmiar tablicy routingu IPv4	Min. 1000

5	Protokół zdalnego zarządzania	SNMP, RMON, Telnet, SNMP v3, SNMP v2c, HTTP, HTTPS, SSH, CLI
6	Warstwa przełączania	2,3
7	Funkcje warstwy 3	Routing statyczny
8	Prędkość magistrali	min. 100 Gbps
9	Przepustowość	min. 77 Mpps
10	Ilość obsługiwanych VLAN-ów	min. 4090
11	Funkcje wysokiej dostępności	Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Muliple Spanning Tree (802.1s)
12	Cechy	Przełączanie warstwy 3, przełączanie warstwy 2, obsługa DHCP, obsługa BOOTP, obsługa VLAN, nasłuchiwanie IGMP, obsługa Syslog, zapobieganie atakom typu DoS, dublowanie portów, obsługa DiffServ, ważone cykliczne kolejkowanie (WRR), Broadcast Storm Control, obsługa IPv6, kontrola nad szturmem pakietów multicast, kontrola nad szturmem pakietów unicast, możliwość aktualizacji firmwaru, obsługa protokołu Spanning Tree (STP), obsługa protokołu Rapid Spanning Tree (RSTP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa protokołu Trivial File Transfer Protocol (TFTP), obsługa list dostępu (ACL), Quality of Service (QoS), obsługa Jumbo Frames, MLD snooping, dynamiczne przydzielanie sieci VLAN przez serwer RADIUS z wykorzystaniem autentykacji 802.1x
13	QoS	prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, Diff Serv, rate-limiting
14	Monitorowanie	RMON 4 grupy (statistics, history, alarm, events)
15	OS	aktualizacje OS dostępne na stronie producenta przez co najmniej 12 miesięcy
16	Obsługa i wsparcie	Ograniczona gwarancja dożywotnia (do 5 lat od wycofania z produkcji/sprzedaży przez producenta). Gwarancja realizowana w trybie 8x5xNBD przez 12 miesięcy
17	Zasilanie	zasilacz 230 VAC, maksymalny pobór mocy 60W, wparcie dla IEEE 802.3az

Przełącznik sieciowy – typ 2 –5 sztuk:

L.p	Warunek	Opis

1	Ilość portów	min. 16 portów 10/100/1000, 4 porty SFP
2	Obudowa	wieżowa 1U umożliwiająca instalację w szafie 19"
3	Rozmiar tablicy adresów MAC	min. 16 000 pozycji
4	Rozmiar tablicy routingu IPv4	Min. 1000
5	Protokół zdalnego zarządzania	SNMP, RMON, Telnet, SNMP v3, SNMP v2c, HTTP, HTTPS, SSH, CLI
6	Warstwa przełączania	2,3
7	Funkcje warstwy 3	Routing statyczny
8	Prędkość magistrali	min. 40 Gbps
9	Przepustowość	min. 29 Mpps
10	Ilość obsługiwanych VLAN-ów	min. 4090
11	Funkcje wysokiej dostępności	Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), Muliple Spanning Tree (802.1s)
12	Cechy	Przełączanie warstwy 3, przełączanie warstwy 2, obsługa DHCP, obsługa BOOTP, obsługa VLAN, nasłuchiwanie IGMP, obsługa Syslog, zapobieganie atakom typu DoS, dublowanie portów, obsługa DiffServ, ważone cykliczne kolejkowanie (WRR), Broadcast Storm Control, obsługa IPv6, kontrola nad szturmem pakietów multicast, kontrola nad szturmem pakietów unicast, możliwość aktualizacji firmwaru, obsługa protokołu Spanning Tree (STP), obsługa protokołu Rapid Spanning Tree (RSTP), obsługa protokołu Multiple Spanning Tree Protocol (MSTP), obsługa protokołu Trivial File Transfer Protocol (TFTP), obsługa list dostępu (ACL), Quality of Service (QoS), obsługa Jumbo Frames, MLD snooping, dynamiczne przydzielanie sieci VLAN przez serwer RADIUS z wykorzystaniem autentykacji 802.1x
13	QoS	prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, Diff Serv, rate-limiting
14	Monitorowanie	RMON 4 grupy (statistics, history, alarm, events)
15	OS	aktualizacje OS dostępne na stronie producenta przez co najmniej 12 miesięcy
16	Obsługa i wsparcie	Ograniczona gwarancja dożywotnia (do 5 lat od wycofania z produkcji/sprzedaży przez producenta). Gwarancja

		realizowana w trybie 8x5xNBD przez 12 miesięcy
17	Zasilanie	zasilacz 230 VAC, maksymalny pobór mocy 20W, wparcie dla IEEE 802.3az

Firewall – 2 sztuki ze wsparciem i licencjami:

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. Powinna istnieć możliwość dedykowania co najmniej 9 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.

Interfejsy, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 9 portami Gigabit Ethernet RJ-45.
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 1.25 mln jednoczesnych połączeń oraz 29 500 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 2,8 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 2,8 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 600 Mbps.
5. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 1,95 Gbps.
6. 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 395 Mbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 183 Mbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 165 Mbps.

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, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych dla administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL.

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.

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.
- 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.

Routing i obsługa łącz 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.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

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.

Kontrola Antywirusowa

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).

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Ochrana przed atakami na aplikacje pracujące na niestandardowych portach.

3. Baza sygnatur ataków powinna zawierać minimum 4500 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. 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 avoidance.
2. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
3. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
4. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
5. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

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 dwuskładnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

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 dwuskładnikowego 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, jflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie

1. System musi mieć możliwość logowania 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 przypadku, kiedy usługa logowania i raportowania realizowana jest w chmurze, wykonawca musi dostarczyć stosowne licencje upoważniające do składowania logów przez okres co najmniej jednego roku
3. 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.
4. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
5. Musi istnieć możliwość logowania do serwera SYSLOG.

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 12 miesięcy.

d) Logowanie do usługi realizowanej w chmurze na okres 12 miesięcy.

Gwarancja oraz wsparcie

1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 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 8x5.

Oprogramowanie do wizualizacji środowiska:

Proponuje się system monitorowania i infrastrukturą obiektową oparty na dedykowanym oprogramowaniu dla tego typu obiektów. Wybrane rozwiązanie powinno pozwalać na integrację, monitorowanie zastosowanych systemów infrastruktury obiektu w ramach jednego systemu. System powinien posiadać elastyczności oprogramowania i modułową budowę w celu zebrania informacji z pozostałych systemów, wprowadzenie zależności programowych oraz stworzenie funkcji monitorowania, sterowania, kontroli i informowania użytkownika o aktualnym funkcjonowaniu obiektu.

Podstawowymi wymaganiami określającymi funkcjonalność oprogramowania do monitorowania i kontroli infrastruktury obiektu, jest zapewnienie użytkownikowi możliwości ciągłej obserwacji funkcjonowania wszystkich systemów infrastruktury, mających, chociaż w niewielkim stopniu wpływ na dostępność i funkcjonowanie serwerowni.

Zakres systemu obejmuje:

- Wizualizację szaf rack
    - Możliwość wizualizacji różnych typów szaf rack, z uwzględnieniem dowolnej wysokości, określonej przez klienta
    - Wizualizacja wszystkich urządzeń wewnątrz tych szaf z uwzględnieniem tzw. „komponentów" czyli urządzeń montowanych w innych urządzeniach, oraz uwzględnieniem portów w tych urządzeniach. Porty zajęte i wolne reprezentować będą inne kolory
    - Możliwość wizualizacji połączeń konkretnego portu w urządzeniu bez konieczności przenoszenie się do innego/kolejnego widoku modułu wizualizacji
    - Możliwość wizualizacji połączeń portów zasilających wraz z aktualnymi odczytami parametrów z bez konieczności przenoszenia się do innego/kolejnego widoku modułu wizualizacji
    - Możliwość eksportu elementów składowych/zawartości szafy rack do pliku PDF
- Obsługa eksportowania szablonów do pliku
- Obsługa importowania szablonów z pliku

Całość oprogramowania powinna charakteryzować się:

- działaniem poprzez przeglądarki internetowe takie jak Chrome, Firefox
- możliwością informowania o zgłoszeniach, nawet jeśli okno przeglądarki jest zminimalizowane
- posiadaniem własnego serwera aplikacji instalowanego na serwerze użytkownika
- posiadaniem własnego wbudowanego serwera HTTP/HTTPS, co zabezpieczy go przed standardowymi atakami zewnętrznymi i zapewni wysoki poziom bezpieczeństwa,
- szyfrowaniem połączeń kluczem SSL
- działaniem serwera aplikacji na systemach Windows, Linux oraz Mac
- posiadaniem zewnętrznego API, służącego do komunikacji z innymi programami
- interfejsem w języku polskim
- możliwością pracy na urządzeniach mobilnych typu tablet
- licencja na oprogramowanie powinna być bezterminowa
- brakiem ograniczeń co do liczby wprowadzonych oraz monitorowanych urządzeń

- możliwością raportowania do pliku i wizualizacji historycznych danych w systemie.