

**1. Serwer (do wirtualizacji) - 1szt.**

I.p.	Parametr lub warunek	Minimalne wymagania
1	Obudowa	-Typu Rack, wysokość maksimum 2U. Montaż w istniejącej szafie RACK 19" o głębokości 1000 mm i pojemności 27U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack;
2	Płyta główna	-Dwuprocessorowa, zaprojektowana i wyprodukowana przez producenta serwera, możliwość instalacji procesorów dwudziesto- ośmiordzeniowych; -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, nie dopuszcza się podtrzymania baterijnego stanu pamięci) -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; (Możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora w slotcie M.2 bez zajmowania klatek dyskowych serwera)
3	Procesory	Zainstalowane minimum dwa procesory ośmiordzeniowe w architekturze x86 osiągające w oferowanym serwerze w testach wydajności SPECrate2017_int_base minimum 81.4 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 64 GB pamięci RAM typu DDR4 Registered, 2966Mhz w kościach o pojemności 16GB; -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC lub równoważnej; -wsparcie serwera dla konfiguracji kopii lustrzanej pamięci RAM;
5	Kontrolery dyskowe, I/O	-Zainstalowany kontroler SAS 3.0 RAID 0,1,5,6,50,60 1GB pamięci podręcznej cache, -Możliwość wyposażenia w nieulotną pamięć cache (nie dopuszcza się baterii z uwagi na ograniczoną żywotność);
6	Dyski twarde	- Zainstalowane 4 dyski SAS 3.0 10K RPM o pojemności 1.2 TB każdy, dyski Hotplug; -Minimum 8 wnęk dla dysków twardych Hotplug 2,5 cala, możliwość rozbudowy do 16 dysków twardych Hotplug 2,5 cala;
8	Kontrolery LAN	-Jedna dwuportowa karta 2x1Gbit/s ze wsparciem iSCSI, niezajmująca slotu PCI Express;  -Dodatkowa osobna karta 2x 10Gbit/s SFP+, niezajmująca slotu PCI Express (dopuszcza się instalację w slotcie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilość slotów PCI Express)
9	System Operacyjny	-Serwer ma być dostarczony z serwerowym systemem operacyjnym (2 szt.) <b>opisanym w pkt. 3 specyfikacji</b>
10	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;

11	Zasilanie, chłodzenie	-Redundantne zasilacze hotplug o mocy maksimum 800W, o sprawności 94% (tzw klasa Platinum) -Redundantne wentylatory hotplug;
12	Zarządzanie	-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach: Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera; 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) Sprzętowy monitoring serwera w tym stanu dysków twardych i kontrolera RAID (bez pośrednictwa agentów systemowych) Karta zarządzająca musi sprzętowo wspierać wirtualizację warstwy sieciowej serwera, bez wykorzystania zewnętrznego hardware - wirtualizacja MAC i WWN na wybranych kartach zainstalowanych w serwerze (co najmniej wsparcie dla technologii kart 10Gbit/s Ethernet i kart FC 16Gbit/s oferowanych przez producenta serwera) Oprogramowanie zarządzające i diagnostyczne 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.).
13	Wspierane OS	- Windows 2019 Hyper-V, Windows 2016 Hyper-V, VMWare, Suse, RHEL
14	Gwarancja	-3 lata gwarancji producenta serwera w trybie onsite z gwarantowanym czasem skutecznej naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (tzw. NBD Fixtime); -Dostępność części zamiennych przez 5 lat od momentu zakupu serwera; -Wymagana jest bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera takowa licencja musi być uwzględniona w konfiguracji;
15	Dokumentacja, inne	-Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA (wymagane oświadczenie producenta serwera potwierdzające spełnienie wymagań dołączone do oferty). -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; -Oferent zobowiązany jest dostarczyć wraz z ofertą kartę produktową oferowanego serwera umożliwiającą weryfikację parametrów oferowanego sprzętu w języku polskim lub angielskim; -Ogólnopolska, telefoniczna linia techniczna producenta serwera (ogólnopolski numer stacjonarny lub o zredukowanej odpłatności 0-800/0-801, w ofercie należy podać nr telefonu) umożliwiająca w czasie obowiązywania gwarancji na sprzęt po podaniu numeru seryjnego urządzenia: zgłoszenie usterki sprzętowej urządzenia oraz weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji – obsługa w języku polskim, w trybie całodobowym również w dni świąteczne;

		<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><b>Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego urządzenia z wymaganiami niniejszej specyfikacji.</b></p>
--	--	---

## 2. Macierz dyskowa NAS

LP	Nazwa komponentu	Wymagane minimalne parametry techniczne sprzętu
1.	Pojemność dyskowa	4 kieszenie , obsługujących: - 3.5" SATA HDD - 2.5" SATA HDD - 2.5" SATA SSD Możliwość rozbudowy do 8 dysków poprzez dołożenie jednostki rozszerzającej. Kieszenie blokowane za pomocą klucza.
2.	Obudowa	Obudowa 19" 1U przygotowana do pracy w szafie rack. W zestawie szyny do montażu w szafie. Szyny powinny umożliwiać zainstalowanie urządzenia w stelażu szafy o głębokości 72 cm. Montaż w istniejącej szafie RACK 19" o głębokości 1000 mm i pojemności 27U
3.	Procesor	64-bit, 4-rdzeniowy, taktowany zegarem co najmniej 1,4 GHz
4.	Pamięć operacyjna	Nie mniej niż 2GB RAM DDR4
5.	Sieć	Karta sieciowa 2x1GbE Ethernet RJ45, zintegrowana z płytą główną, wspierająca obsługę Link Aggregation.
6.	Złącza dodatkowe	- minimum 2 szt. USB 3.0 - port konsoli RS232 - port eSATA
8.	Obsługa trybów RAID	Możliwość pracy w trybie RAID 0, 1, 5, 6, 10 z funkcją rozbudowy i funkcją migracji poziomu RAID, RAID Hot Spare
9.	Zgodność z systemami operacyjnymi	OS: Windows 7 i 10, Mac OS X Wirtualizacja: VMware VSphere, Citrix, Hyper-V
10.	Protokoły sieciowe	SMB, AFP, NFS, FTP, iSCSI, Telnet, SSH, SNMP, VPN
11.	Systemy plików	Wewnętrzny: Btrfs, ext4 Zewnętrzny: Btrfs, ext4, ext3, FAT, NTFS, HFS+, exFAT
12.	Udostępnianie plików	liczba folderów współdzielonych: 256 liczba jednoczesnych połączeń SMB/NFS/AFP/FTP: 200
13.	Usługi	- Integracja z Windows® AD, LDAP - Obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL. - Stacja monitoringu, obsługa kamer ONVIF - Serwer multimedialny
14.	Bezpieczeństwo / zarządzanie	- szyfrowanie wolumenów, - skanowanie złych sektorów, S.M.A.R.T., - szyfrowana replikacja, - automatyczne blokowanie adresów IP - powiadomienia przez e-mail - kopia zapasowa konfiguracji - kopia na nośnik zewnętrzny, - logi systemowe (użytkownicy, alarmy, błędy, połączenia do plików), - FTP przez SSL/TLS - zarządzanie przez przeglądarkę HTTPS - współpraca z zasilaczami awaryjnymi UPS - przypisanie usługi sieciowej do konkretnego portu - interfejs aplikacji www do zarządzania w języku polskim

15.	Pamięć masowa	- obsługa - liczba iSCSI Target: 128 - liczba jednostek iSCSI LUN: 256 - obsługa klonowania/migawek jednostek iSCSI LUN
16.	Zasilanie	100 – 240V, 50/60 Hz
17.	Gwarancja	3 lata. Dostawca zapewni usługę serwisową polegającą na usunięciu awarii sprzętu lub jego wymianie w ciągu 48 godzin od zgłoszenia.
18.	Pamięć masowa	4 sztuki HDD SATA 3 (6Gb/s) 3,5" o pojemności 6 TB każdy min. 256MB cache min. 7200 rpm Maksymalna średnia szybkość transmisji min. 230 MB/s
19.	Dokumentacja, inne	Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego urządzenia z wymaganiami niniejszej specyfikacji.

### 3. Serwerowy system operacyjny (SSO) – 2 szt.

Licencja na serwerowy system operacyjny musi zapewnić poniżej opisane funkcjonalności dla jednego serwera posiadającego dwa procesory przy czym każdy z procesorów posiada 8 rdzeni fizycznych.

I.p.	Parametr lub warunek	Minimalne wymagania
1.	Cechy licencji	<p>Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i <b>dwóch wirtualnych środowisk serwerowego systemu operacyjnego</b> za pomocą wbudowanych mechanizmów wirtualizacji. <b>Na fizycznym serwerze opisanym w pkt. 1 specyfikacji mają zostać uruchomione łącznie 4 (cztery) wirtualne środowiska SSO.</b></p> <p><b>Wraz z licencją SSO należy dostarczyć 50 licencji dostępowych</b> dla urządzeń, jeżeli model licencjonowania oferowanego SSO wymaga takich licencji. <b>Oprogramowanie musi być dostarczone w najnowszej wersji</b></p>
2.	Cechy SSO	<p>Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy.</p> <ol style="list-style-type: none"> <li>1. Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym</li> <li>2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny.</li> <li>3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.</li> <li>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.</li> <li>5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.</li> <li>6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.</li> <li>7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.</li> <li>8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.</li> <li>9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> <li>a. pozwalają na zmianę rozmiaru w czasie pracy systemu,</li> <li>b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,</li> <li>c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,</li> <li>d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).</li> </ol> </li> <li>10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.</li> <li>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.</li> <li>12. Możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET</li> <li>13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.</li> <li>14. Wbudowana zaporą internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.</li> <li>15. Graficzny interfejs użytkownika.</li> </ol>

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 urządzeń peryferyjnych tj. drukarek, urządzeń sieciowych itp.
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.
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:
    - i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
    - ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,,
    - iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
    - iv. 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 1000 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

		<ul style="list-style-type: none"><li>- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.</li><li>- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode)</li></ul> <p>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.</p> <p>24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).</p> <p>25. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.</p> <p>26. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.</p> <p>27. Sterowniki i dokumentacja od producenta sprzętu</p> <p>28. Materiały edukacyjne w języku polskim.</p>
3	Dokumentacja, inne	Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego oprogramowania z wymaganiami niniejszej specyfikacji.



#### 4. Oprogramowanie do backupu – 1 szt.

l.p.	Parametr lub warunek	Minimalne wymagania
1.	Wymagania ogólne	<ul style="list-style-type: none"> <li>a. Licencja dla dostarczanego środowiska składającego się z jednego serwera dwuprocesorowego (<b>opisanego w pkt. 1 specyfikacji</b>) bez ograniczeń czasowych ze wsparciem producenta na 12 miesięcy.</li> <li>b. Oprogramowanie musi współpracować conajmniej z infrastrukturą VMware w wersji 4.1, 5.0, 5.1, 5.5, 6.0 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</li> <li>c. Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.</li> <li>d. Oprogramowanie musi współpracować klastrami hostów oraz pojedynczymi hostami.</li> <li>e. Oprogramowanie musi zapewniać tworzenie kopii zapasowych i odzyskiwanie wszystkich systemów operacyjnych maszyn wirtualnych wspieranych co najmniej przez vSphere i Hyper-V</li> </ul>
2.	Całkowite koszty posiadania	<ul style="list-style-type: none"> <li>a. Oprogramowanie musi być licencjonowane w modelu "per-CPU". Wszystkie funkcjonalności zawarte w tym dokumencie powinny być zapewnione w tej licencji. Jakiegokolwiek dodatkowe licencjonowanie (per zabezpieczony TB, dodatkowo płatna deduplikacja) nie jest dozwolone</li> <li>b. Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej</li> <li>c. Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków</li> <li>d. Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakiegokolwiek funkcjonalności wymienionych w tej specyfikacji</li> <li>e. 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.</li> <li>f. Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakiegokolwiek funkcjonalności backupu lub odtwarzania</li> <li>g. Oprogramowanie musi zapewniać backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia</li> <li>h. 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</li> <li>i. Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota w środowisku VMware.</li> <li>j. Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji</li> <li>k. 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</li> <li>l. Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)</li> <li>m. Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.</li> </ul>

	Wymagania RPO	<ul style="list-style-type: none"> <li>a. Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej</li> <li>b. Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora</li> <li>c. Oprogramowanie musi wspierać kopiowanie plików na taśmy</li> <li>d. Oprogramowanie musi mieć możliwość wydzielenia osobnej roli typu tape server</li> <li>e. Oprogramowanie musi mieć możliwość kopiowania backupów do lokalizacji zdalnej</li> <li>f. Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)</li> <li>g. Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 z systemem pliku ReFS jako repozytorium backupu.</li> <li>h. 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.</li> <li>i. Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik</li> <li>j. Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)</li> <li>k. Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V</li> <li>l. Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)</li> <li>m. Oprogramowanie musi dawać możliwość tworzenia backupów ad-hoc z konsoli jak i z klienta webowego vSphere</li> <li>n. Oprogramowanie musi przetwarzać wiele wirtualnych dysków jednocześnie (parallel processing)</li> </ul>
	Wymagania RTO	<ul style="list-style-type: none"> <li>a. 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 środowiska vSphere powinien być wykorzystany wbudowany w oprogramowanie serwer NFS. Dla Hyper-V powinna być zapewniona taka sama funkcjonalność realizowana wewnętrznymi mechanizmami oprogramowania</li> <li>b. 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</li> <li>c. Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków</li> <li>d. 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</li> <li>e. 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.</li> <li>f. Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów plików: <ul style="list-style-type: none"> <li>○ <b>Linux</b> <ul style="list-style-type: none"> <li>▪ ext, ext2, ext3, ext4, ReiserFS (Reiser3), JFS, XFS, Btrfs</li> </ul> </li> <li>○ <b>BSD</b> <ul style="list-style-type: none"> <li>▪ UFS, UFS2</li> </ul> </li> </ul> </li> </ul>

		<ul style="list-style-type: none"> <li>○ <b>Solaris</b> <ul style="list-style-type: none"> <li>▪ ZFS, UFS</li> </ul> </li> <li>○ <b>Mac</b> <ul style="list-style-type: none"> <li>▪ HFS, HFS+</li> </ul> </li> <li>○ <b>Windows</b> <ul style="list-style-type: none"> <li>▪ NTFS, FAT, FAT32, ReFS</li> </ul> </li> <li>○ <b>Novell OES</b> <ul style="list-style-type: none"> <li>▪ NSS</li> </ul> </li> </ul> <p>g. Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.</p> <p>h. Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.</p> <p>i. Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, grupy oraz pozwalać na odtworzenie haseł.</p> <p>j. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects").</p> <p>k. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowsze.</p> <p>l. Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowsze.</p> <p>m. Funkcjonalność ta nie może wymagać pełnego odtworzenia wirtualnej maszyny ani jej uruchomienia.</p> <p>n. Oprogramowanie musi indeksować pliki Windows i Linux w celu szybkiego wyszukiwania plików w plikach backupowych.</p> <p>o. Oprogramowanie musi używać mechanizmów VSS wbudowanych w system operacyjny Microsoft Windows</p> <p>p. Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN</p>
	Monitoring	<p>a. System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich</p> <p>b. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 4.1, 5.x oraz 6.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie</p> <p>c. System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 oraz 2016 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.</p> <p>d. System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware</p> <p>e. System musi mieć możliwość instalacji na systemach operacyjnych w wersjach 64 bitowych:</p> <ul style="list-style-type: none"> <li>○ Microsoft Windows 2008 SP2</li> <li>○ Microsoft Windows 2008 R2 SP1</li> <li>○ Microsoft Windows 7 SP1</li> <li>○ Microsoft Windows 8</li> <li>○ Microsoft Windows 2012</li> <li>○ Microsoft Windows 2012 R2</li> </ul>

		<ul style="list-style-type: none"> <li>○ Microsoft Windows 8.1</li> <li>○ Microsoft Windows 10</li> <li>○ Microsoft Windows 2016</li> </ul> <p>f. System musi obsługiwać następujące bazy danych w wersjach 32 i 64 bitowych:</p> <ul style="list-style-type: none"> <li>○ Microsoft SQL Server 2008</li> <li>○ Microsoft SQL Server 2008 R2</li> <li>○ Microsoft SQL Server 2012 R2</li> <li>○ Microsoft SQL Server 2014</li> <li>○ Microsoft SQL Server 2016</li> </ul> <p>g. System musi umożliwiać kategoryzację obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter</p> <p>h. System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn</p> <p>i. System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel</p> <p>j. System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk</p> <p>k. Silnik raportowania powinien być oparty o SQL Server Reporting Services w celu zapewnienia bezpiecznego dostępu do raportów dla wielu użytkowników z uwzględnieniem ról, jakie pełnią w organizacji</p> <p>l. System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora</p> <p>m. System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanymi alarmami</p> <p>n. System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)</p> <p>o. System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna</p> <p>p. System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego</p> <p>q. System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych</p> <p>r. System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.</p> <p>s. System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware</p> <p>t. System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 5.5, 5.6, 8.0 oraz 8.10</p>
	Raportowanie	<p>a. System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 4.1, 5.x oraz 6.0, vCenter Server 4.1, 5.x oraz 6.0 jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2 i 2016.</p> <p>b. System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.</p>

		<p>c. System musi być certyfikowany przez VMware i posiadać status „VMware Ready”</p> <p>d. System musi instalować się na następujących systemach operacyjnych:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 SP2</li> <li>• Microsoft Windows 2008 R2 SP1</li> <li>• Microsoft Windows 7 SP1</li> <li>• Microsoft Windows 8</li> <li>• Microsoft Windows 2012</li> <li>• Microsoft Windows 2012 R2</li> <li>• Microsoft Windows 8.1</li> <li>• Microsoft Windows 10</li> <li>• Microsoft Windows 2016</li> </ul> <p>e. System musi wspierać jako silnik bazodanowy następujące bazy danych:</p> <ul style="list-style-type: none"> <li>• Microsoft SQL Server 2008</li> <li>• Microsoft SQL Server 2008 R2</li> <li>• Microsoft SQL Server 2012</li> <li>• Microsoft SQL Server 2014</li> <li>• Microsoft SQL Server 2016</li> </ul> <p>f. System do prezentacji raportów powinien używać SQL Server Reporting Services w celu jednoczesnego dostępu do raportów wielu użytkowników z określonymi przez administrator systemu uprawnieniami.</p> <p>g. System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V</p> <p>h. System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF</p> <p>i. System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc</p> <p>j. System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach</p> <p>k. Minimalny interwał czasowy dla zadań kolekcjonowania i raportowania musi wynosić min 1 godzinę</p> <p>l. System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów</p> <p>m. System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych</p> <p>n. System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych</p> <p>o. System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury</p> <p>p. System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych .</p> <p>q. System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn wirtualnych, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.</p> <p>r. System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.</p>
--	--	---

		<ul style="list-style-type: none"><li>s. System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanych użytkownikom dla platformy VMware</li><li>t. System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)</li><li>u. System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie</li></ul>
3	Dokumentacja, inne	Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego oprogramowania z wymaganiami niniejszej specyfikacji.

**5. Przełącznik sieciowy 48 portów - 1szt.**

l.p.	Parametr lub warunek	Minimalne wymagania
1.	Parametry podstawowe	<ol style="list-style-type: none"> <li>1. Przełącznik posiadający min. 48 porty 10/100/1000BASE-T</li> <li>2. Przełącznik posiadający min. 8 portów 1GBE SFP</li> <li>3. Przełącznik posiadający min. 4 porty 10 GBE SFP+</li> <li>4. Wysokość urządzenia 1U. Montaż w istniejącej szafie RACK 19" o głębokości 470 mm i posiadającej po demontażu istniejących przełączników pojemność 7U</li> <li>5. Nieblokująca architektura o wydajności przełączania min. 176 Gb/s</li> <li>6. Szybkość przełączania min. 130 Milionów pakietów na sekundę</li> <li>7. Posiada porty umożliwiające łączenie przełączników w stos. Wydajność połączenia w stos min. 40 Gb/s.</li> <li>8. Możliwość łączenia minimum 6 przełączników w stos</li> <li>9. Tablica MAC adresów min. 16k</li> <li>10. Pamięć operacyjna: min. 1 GB pamięci DRAM</li> <li>11. Pamięć flash: min. 4 GB pamięci Flash</li> <li>12. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094</li> <li>13. Obsługa sieci wirtualnych protokołowych IEEE 802.1v</li> <li>14. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci</li> <li>15. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)</li> <li>16. Obsługa Q-in-Q IEEE 802.1ad</li> <li>17. Obsługa Quality of Service <ul style="list-style-type: none"> <li>- IEEE 802.1p</li> <li>- DiffServ</li> <li>- 8 kolejek priorytetów na każdym porcie wyjściowym</li> </ul> </li> <li>18. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB</li> <li>19. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)</li> <li>20. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.</li> <li>21. Przełącznik musi posiadać możliwość dołączenia redundantnego systemu zasilania</li> <li>22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware</li> <li>23. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash</li> <li>24. Możliwość monitorowania zajętości CPU</li> <li>25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)</li> <li>26. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.</li> <li>27. Obsługa CDPv2</li> </ol>
2.	Obsługa Routingu IPv4	<ol style="list-style-type: none"> <li>1. Sprzętowa obsługa routingu IPv4 – forwarding</li> <li>2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów</li> <li>3. Routing statyczny</li> <li>4. Obsługa routingu dynamicznego IPv4 <ul style="list-style-type: none"> <li>a. RIPv1/v2</li> <li>b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania</li> </ul> </li> </ol>
3.	Obsługa Routingu IPv6	<ol style="list-style-type: none"> <li>1. Sprzętowa obsługa routingu IPv6 – forwarding</li> <li>2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów</li> <li>3. Routing statyczny</li> <li>4. Obsługa routingu dynamicznego dla IPv6 <ul style="list-style-type: none"> <li>a. RIPng</li> <li>b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania</li> </ul> </li> <li>5. Telnet Serwer/Klient dla IPv6</li> <li>6. SSH2 Serwer/Klient dla IPv6</li> </ol>

		<ul style="list-style-type: none"> <li>7. Ping dla IPv6</li> <li>8. Tracert dla IPv6</li> <li>9. Obsługa MLDv1 (Multicast Listener Discovery version 1)</li> </ul>
4.	Obsługa Multicastów	<ul style="list-style-type: none"> <li>1. Filtrowanie IGMP</li> <li>2. Obsługa Multicast VLAN Registration - MVR</li> <li>3. Obsługa IGMP v1/v2/v3 snooping</li> </ul>
5.	Bezpieczeństwo	<ul style="list-style-type: none"> <li>1. Obsługa Network Login <ul style="list-style-type: none"> <li>a. IEEE 802.1x - RFC 3580</li> <li>b. Web-based Network Login</li> <li>c. MAC based Network Login</li> </ul> </li> <li>2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)</li> <li>3. Możliwość integracji funkcjonalności Network Login z Microsoft NAP</li> <li>4. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login</li> <li>5. Obsługa Guest VLAN dla IEEE 802.1x</li> <li>6. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos</li> <li>7. Możliwość dynamicznego przypisania VLAN, QOS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication</li> <li>8. Obsługa Identity Management</li> <li>9. Wbudowana obrona procesora urządzenia przed atakami DoS</li> <li>10. Obsługa TACACS+ (RFC 1492)</li> <li>11. Obsługa RADIUS Authentication (RFC 2138)</li> <li>12. Obsługa RADIUS Accounting (RFC 2139)</li> <li>13. RADIUS and TACACS+ per-command Authentication</li> <li>14. Bezpieczeństwo MAC adresów <ul style="list-style-type: none"> <li>a. ograniczenie liczby MAC adresów na porcie</li> <li>b. zatrzaśnięcie MAC adresu na porcie</li> <li>c. możliwość wpisania statycznych MAC adresów na port/vlan</li> </ul> </li> <li>15. Możliwość wyłączenia MAC learning</li> <li>16. Obsługa SNMPv1/v2/v3</li> <li>17. Klient SSH2</li> <li>18. Zabezpieczenie przełącznika przed atakami DoS <ul style="list-style-type: none"> <li>a. Networks Ingress Filtering RFC 2267</li> <li>b. SYN Attack Protection</li> <li>c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania</li> </ul> </li> <li>19. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 <ul style="list-style-type: none"> <li>a. Adres MAC źródłowy i docelowy plus maska</li> <li>b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6</li> <li>c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.</li> <li>d. Numery portów źródłowych i docelowych TCP, UDP</li> <li>e. Zakresy portów źródłowych i docelowych TCP, UDP</li> <li>f. Identyfikator sieci VLAN - VLAN ID</li> <li>g. Flagi TCP</li> <li>h. Obsługa fragmentów</li> </ul> </li> <li>20. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika</li> <li>21. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania</li> <li>22. Obsługa bezpiecznego transferu plików SCP/SFTP</li> <li>23. Obsługa DHCP Option 82</li> </ul>



		<ul style="list-style-type: none"> <li>24. Obsługa IP Security - Gratuitous ARP Protection</li> <li>25. Obsługa IP Security - Trusted DHCP Server</li> <li>26. Obsługa IP Security - DHCP Snooping</li> <li>27. Obsługa IP Security - DHCP Secured ARP/ARP Validation</li> <li>28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 64 kb/s</li> </ul>
6.	Bezpieczeństwo sieciowe	<ul style="list-style-type: none"> <li>1. Możliwość konfiguracji portu głównego i zapasowego</li> <li>2. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania</li> <li>3. Obsługa STP (Spanning Tree Protocol) IEEE 802.1D</li> <li>4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w</li> <li>5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s</li> <li>6. Obsługa PVST+</li> <li>7. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619</li> <li>8. Obsługa G.8032 v1/v2</li> <li>9. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.</li> <li>10. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.</li> </ul>
7.	Zarządzanie	<ul style="list-style-type: none"> <li>1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)</li> <li>2. Obsługa synchronizacji czasu NTP</li> <li>3. Zarządzanie przez SNMP v1/v2/v3</li> <li>4. Zarządzanie przez przeglądarkę WWW – protokół http i https</li> <li>5. Możliwość zarządzania poprzez protokół XML</li> <li>6. Telnet Serwer/Klient dla IPv4 / IPv6</li> <li>7. SSH2 Serwer/Klient dla IPv4 / IPv6</li> <li>8. Ping dla IPv4 / IPv6</li> <li>9. Traceroute dla IPv4 / IPv6</li> <li>10. Obsługa SYSLOG z możliwością definiowania wielu serwerów</li> <li>11. Sprzętowa obsługa sFlow</li> <li>12. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)</li> <li>13. Obsługa RMON2 (RFC 2021)</li> </ul>
8.	Inne	<ul style="list-style-type: none"> <li>1. Zakres temperatury pracy 0-50 °C</li> <li>2. Obsługa skryptów CLI</li> <li>3. Obsługa funkcji TCL/Tk w skryptach CLI</li> <li>4. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)</li> <li>5. Obsługa OpenFlow – możliwość rozszerzenia przez licencje</li> <li>6. Obsługa AVB (Audio Video Bridging) - możliwość rozszerzenia przez licencje</li> <li>7. Możliwość uruchamiania skryptów <ul style="list-style-type: none"> <li>a. Ręcznie</li> <li>b. O określonym czasie lub co wskazany okres czasu</li> <li>c. Na podstawie wpisów w logu systemowym</li> </ul> </li> <li>8. Przełącznik zostanie dostarczony z przewodem typu DAC o długości 1m do połączenia przełącznika w stos oraz dwoma wkładkami SFP+ MM.</li> </ul>
9.	Gwarancja, dokumentacja	<p>Przełącznik sieciowy musi być objęty gwarancją producenta min 36 miesięcy.</p> <p>Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego urządzenia z wymaganiami niniejszej specyfikacji.</p>

**6. Przełącznik sieciowy 24 porty - 1szt.**

l.p.	Parametr lub warunek	Minimalne wymagania
1	Parametry podstawowe	<ol style="list-style-type: none"> <li>1. Przełącznik posiadający min. 24 porty 10/100/1000BASE-T</li> <li>2. Przełącznik posiadający min. 8 portów 1GBE SFP</li> <li>3. Możliwość rozbudowy o min. 4 porty 10 GBE SFP+ (min. 2 porty aktywne)</li> <li>4. Wysokość urządzenia 1U Montaż w istniejącej szafie RACK 19" o głębokości 470 mm i posiadającej po demontażu istniejących przełączników pojemność 7U</li> <li>5. Nieblokująca architektura o wydajności przełączania min. 128 Gb/s</li> <li>6. Szybkość przełączania min. 95 Milionów pakietów na sekundę</li> <li>7. Posiada porty umożliwiające łącznie przełączników w stos. Wydajność połączenia w stos min. 40 Gb/s.</li> <li>8. Możliwość łączenia minimum 6 przełączników w stos</li> <li>9. Tablica MAC adresów min. 16k</li> <li>10. Pamięć operacyjna: min. 1 GB pamięci DRAM</li> <li>11. Pamięć flash: min. 4 GB pamięci Flash</li> <li>12. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094</li> <li>13. Obsługa sieci wirtualnych protokołowych IEEE 802.1v</li> <li>14. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci</li> <li>15. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)</li> <li>16. Obsługa Q-in-Q IEEE 802.1ad</li> <li>17. Obsługa Quality of Service <ol style="list-style-type: none"> <li>a. IEEE 802.1p</li> <li>b. DiffServ</li> <li>c. 8 kolejek priorytetów na każdym porcie wyjściowym</li> </ol> </li> <li>18. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB</li> <li>19. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)</li> <li>20. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.</li> <li>21. Przełącznik musi posiadać możliwość dołączenia redundantnego systemu zasilania</li> <li>22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware</li> <li>23. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash</li> <li>24. Możliwość monitorowania zajętości CPU</li> <li>25. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)</li> <li>26. Wbudowany dodatkowy port Fast Ethernet do zarządzania poza pasmem - out of band management.</li> <li>27. Obsługa CDPv2</li> </ol>
2	Obsługa Routingu IPv4	<ol style="list-style-type: none"> <li>1. Sprzętowa obsługa routingu IPv4 – forwarding</li> <li>2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów</li> <li>3. Routing statyczny</li> <li>4. Obsługa routingu dynamicznego IPv4 <ol style="list-style-type: none"> <li>a. RIPv1/v2</li> <li>b. OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania</li> </ol> </li> </ol>
3	Obsługa Routingu IPv6	<ol style="list-style-type: none"> <li>1. Sprzętowa obsługa routingu IPv6 – forwarding</li> <li>2. Pojemność tabeli routingu typowa dla przełącznika brzegowego min. 16 wpisów</li> <li>3. Routing statyczny</li> <li>4. Obsługa routingu dynamicznego dla IPv6 <ol style="list-style-type: none"> <li>a. RIPv6</li> <li>b. OSPF v3 – możliwość rozszerzenia przez licencję oprogramowania</li> </ol> </li> <li>5. Telnet Serwer/Klient dla IPv6</li> </ol>

		<ol style="list-style-type: none"> <li>6. SSH2 Serwer/Klient dla IPv6</li> <li>7. Ping dla IPv6</li> <li>8. Tracert dla IPv6</li> <li>9. Obsługa MLDv1 (Multicast Listener Discovery version 1)</li> </ol>
4	Obsługa Multicastów	<ol style="list-style-type: none"> <li>1. Filtrowanie IGMP</li> <li>2. Obsługa Multicast VLAN Registration - MVR</li> <li>3. Obsługa IGMP v1/v2/v3 snooping</li> </ol>
5	Bezpieczeństwo	<ol style="list-style-type: none"> <li>1. Obsługa Network Login <ol style="list-style-type: none"> <li>a. IEEE 802.1x - RFC 3580</li> <li>b. Web-based Network Login</li> <li>c. MAC based Network Login</li> </ol> </li> <li>2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)</li> <li>3. Możliwość integracji funkcjonalności Network Login z Microsoft NAP</li> <li>4. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login</li> <li>5. Obsługa Guest VLAN dla IEEE 802.1x</li> <li>6. Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos</li> <li>7. Możliwość dynamicznego przypisania VLAN, QoS, rate limiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication</li> <li>8. Obsługa Identity Management</li> <li>9. Wbudowana obrona procesora urządzenia przed atakami DoS</li> <li>10. Obsługa TACACS+ (RFC 1492)</li> <li>11. Obsługa RADIUS Authentication (RFC 2138)</li> <li>12. Obsługa RADIUS Accounting (RFC 2139)</li> <li>13. RADIUS and TACACS+ per-command Authentication</li> <li>14. Bezpieczeństwo MAC adresów <ol style="list-style-type: none"> <li>a. ograniczenie liczby MAC adresów na porcie</li> <li>b. zatrzaśnięcie MAC adresu na porcie</li> <li>c. możliwość wpisania statycznych MAC adresów na port/vlan</li> </ol> </li> <li>15. Możliwość wyłączenia MAC learning</li> <li>16. Obsługa SNMPv1/v2/v3</li> <li>17. Klient SSH2</li> <li>18. Zabezpieczenie przełącznika przed atakami DoS <ol style="list-style-type: none"> <li>a. Networks Ingress Filtering RFC 2267</li> <li>b. SYN Attack Protection</li> <li>c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania</li> </ol> </li> <li>19. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 <ol style="list-style-type: none"> <li>a. Adres MAC źródłowy i docelowy plus maska</li> <li>b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6</li> <li>c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.</li> <li>d. Numery portów źródłowych i docelowych TCP, UDP</li> <li>e. Zakresy portów źródłowych i docelowych TCP, UDP</li> <li>f. Identyfikator sieci VLAN - VLAN ID</li> <li>g. Flagi TCP</li> <li>h. Obsługa fragmentów</li> </ol> </li> <li>20. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika</li> <li>21. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI. – możliwość rozszerzenia przez licencję oprogramowania</li> </ol>

		<ul style="list-style-type: none"> <li>22. Obsługa bezpiecznego transferu plików SCP/SFTP</li> <li>23. Obsługa DHCP Option 82</li> <li>24. Obsługa IP Security - Gratuitous ARP Protection</li> <li>25. Obsługa IP Security - Trusted DHCP Server</li> <li>26. Obsługa IP Security - DHCP Snooping</li> <li>27. Obsługa IP Security - DHCP Secured ARP/ARP Validation</li> <li>28. Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 64 kb/s</li> </ul>
6	Bezpieczeństwo sieciowe	<ul style="list-style-type: none"> <li>1. Możliwość konfiguracji portu głównego i zapasowego</li> <li>2. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania</li> <li>3. Obsługa STP (Spanning Tree Protocol) IEEE 802.1D</li> <li>4. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w</li> <li>5. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s</li> <li>6. Obsługa PVST+</li> <li>7. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619</li> <li>8. Obsługa G.8032 v1/v2</li> <li>9. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów. Możliwość konfiguracji połączenia Link Aggregation z różnych przełączników w stosie.</li> <li>10. Obsługa MLAG - połączenie link aggregation do dwóch niezależnych przełączników.</li> </ul>
7	Zarządzanie	<ul style="list-style-type: none"> <li>1. Obsługa synchronizacji czasu SNTP v4 (Simple Network Time Protocol)</li> <li>2. Obsługa synchronizacji czasu NTP</li> <li>3. Zarządzanie przez SNMP v1/v2/v3</li> <li>4. Zarządzanie przez przeglądarkę WWW – protokół http i https</li> <li>5. Możliwość zarządzania poprzez protokół XML</li> <li>6. Telnet Serwer/Klient dla IPv4 / IPv6</li> <li>7. SSH2 Serwer/Klient dla IPv4 / IPv6</li> <li>8. Ping dla IPv4 / IPv6</li> <li>9. Traceroute dla IPv4 / IPv6</li> <li>10. Obsługa SYSLOG z możliwością definiowania wielu serwerów</li> <li>11. Sprzętowa obsługa sFlow</li> <li>12. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)</li> <li>13. Obsługa RMON2 (RFC 2021)</li> </ul>
8	Inne	<ul style="list-style-type: none"> <li>1. Zakres temperatury pracy 0-50 °C</li> <li>2. Obsługa skryptów CLI</li> <li>3. Obsługa funkcji TCL/Tk w skryptach CLI</li> <li>4. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)</li> <li>5. Obsługa OpenFlow – możliwość rozszerzenia przez licencje</li> <li>6. Obsługa AVB (Audio Video Bridging) - możliwość rozszerzenia przez licencje</li> <li>7. Możliwość uruchamiania skryptów <ul style="list-style-type: none"> <li>a. Ręcznie</li> <li>b. O określonym czasie lub co wskazany okres czasu</li> <li>c. Na podstawie wpisów w logu systemowym</li> </ul> </li> <li>8. Przełącznik zostanie dostarczony z przewodem typu DAC o długości 1m do połączenia przełącznika w stos oraz dwoma wkładkami SFP+ MM.</li> </ul>
9.	Gwarancja	<p>Przełącznik sieciowy musi być objęty gwarancją producenta min 36 miesięcy.</p> <p>Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego urządzenia z wymaganiami niniejszej specyfikacji.</p>

## 7. Urządzenie UTM - 1szt.

W celu zabezpieczenia dostępu sieci zamawiający wymaga dostarczenia urządzenia typu UTM o poniższych parametrach

I.p.	Parametr lub warunek	Minimalne wymagania
1	Typ urządzenia	1. Urządzenie typu UTM, zapewniające funkcjonalności: Firewall, Koncentrator IPSec VPN, ochrona przed wirusami, spyware, sonda IPS, filtrowanie poczty, filtrowanie stron www po kategoriach i według reguł tworzonych przez administratora
2	Specyfikacja fizyczna urządzenia	1. Dedykowane rozwiązanie sprzętowe 2. Obudowa 1U przeznaczona do montażu w szafie RACK 3. Pamięć RAM: minimum 1 GB 4. Procesor wielordzeniowy: minimum 4x 1 GHz 5. Ilość interfejsów <ol style="list-style-type: none"> <li>Nie mniej niż 8 interfejsów GigabitEthernet</li> <li>Nie mniej niż 2 interfejsy USB</li> <li>Min. 1 interfejs konsoli</li> </ol>
3	Wydajność urządzenia	1. Obsługa nielimitowanej ilości hostów w sieci chronionej 2. Przepustowość zapory sieciowej przy pracy w trybie Statefull Packet Inspection lub równoważnym, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 1,4 Gbps 3. Przepustowość zapory sieciowej pracującej jako sonda IPS, mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 1000 Mbps 4. Przepustowość zapory sieciowej przy pracy w trybie Deep Packet Inspection lub równoważnym, przy włączonych wszystkich usługach filtrowania i skanowania: nie mniejsza niż 400 Mbps 5. Przepustowość zintegrowanego z zaporą sieciową koncentratora połączeń IPSec VPN AES/3DES mierzona zgodnie z zaleceniami RFC 2544: nie mniejsza niż 1000 Mbps 6. Maksymalna ilość jednocześnie obsługiwanych sesji: nie mniej niż 125 000 7. Obsługa nie mniej niż 8000 nowych sesji na sekundę 8. Ochrona przed atakami DoS i DDoS
4	Funkcjonalności urządzenia w zakresie konfiguracji połączeń IPSec VPN	1. Minimalna ilość jednocześnie obsługiwanych połączeń IPSec VPN: 25 2. Minimalna ilość klientów IPSec VPN w cenie urządzenia: 5 szt. 3. Wspierane mechanizmy uwierzytelniania i szyfrowania: DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1 4. Wspierane mechanizmy wymiany kluczy: IKE, IKEv2, Manual Key, PKI (X.509) 5. Wsparcie certyfikatów: Verisign, Thawte, Cybertrust, RSA Keon, Entrust, Microsoft CA dla połączeń site-to-site pomiędzy urządzeniami UTM 6. Obsługa funkcjonalności: L2TP IPSec, DHCP over VPN, redundantna brama zdalna w przypadku połączeń site-site VPN
5	Sieciowe funkcjonalności urządzenia	1. Możliwość pracy jako Router, Bridge L2 lub w trybie transparentnym 2. Obsługa nie mniej niż 50 sieci VLAN działających zgodnie ze standardem 802.1Q 3. Wbudowany serwer DHCP umożliwiający przydzielanie adresów statycznie, dynamicznie, przekierowanie zgłoszeń do zewnętrznego serwera DHCP 4. Możliwość przesyłania komunikatów DHCP pomiędzy różnymi strefami 5. Wsparcie mechanizmów NAT: 1:1, 1:many, many:1, many:many, PAT 6. Możliwość scentralizowanego zarządzania nie mniej niż 32 punktami dostępowymi, wsparcie dla standardów 802.11 b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, 7. EAP-TTLS, IPSec over WLAN 8. Możliwość kreowania reguł routingu statycznego

		9. Wsparcie dynamicznych protokołów routingu: BGP, RIP v1/v2, OSPF i wsparcie dla routowania transmisji multicast 10. Wsparcie funkcjonalności QoS: tagowanie/mapowanie 802.1p, DSCP, możliwość ustawienia przynajmniej 100 reguł określających maksymalne i gwarantowane pasmo 11. Możliwość skonfigurowania przynajmniej 2 łączy WAN, działających w trybie redundantnym lub umożliwiających równoważenie obciążeń dla ruchu wychodzącego. 12. Możliwość konfiguracji monitorowania pracy łączy WAN w oparciu o połączenia TCP i ICMP i reguł przełączenia ruchu z łączy podstawowego na łączy redundantne 13. Możliwość konfiguracji reguł równoważenia obciążeń dla ruchu przychodzącego do hostów znajdujących się w sieci chronionej 14. Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, pełna kompatybilność z większością urządzeń i serwerów VoIP
6	Funkcjonalności urządzenia w zakresie uwierzytelniania użytkowników	1. Lokalna baza użytkowników 2. Uwierzytelnianie użytkowników w oparciu o: XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Terminal Services, Citrix
7	Funkcjonalności urządzenia w zakresie zarządzania i wysokiej dostępności	1. Możliwość zarządzania urządzeniem poprzez: HTTP, HTTPS, CLI (SSH, konsola), SNMP 2. Możliwość dokupienia dedykowanego oprogramowania do scentralizowanego zarządzania większą ilością urządzeń 3. Możliwość podłączenia drugiego urządzenia do pracy w klastrze wysokiej dostępności w trybie Active – Standby
8	Funkcjonalności urządzenia w zakresie mechanizmów filtrowania Deep Packet Inspection i Statefull Packet Inspection lub równoważnych	1. Możliwość kreowania stref bezpieczeństwa przydzielanych do danych interfejsów zarówno fizycznych, jak i wirtualnych (możliwość przypisania więcej niż jednego interfejsu do pojedynczej strefy bezpieczeństwa) 2. Możliwość indywidualnej konfiguracji usług bezpieczeństwa dla każdej ze stref 3. Możliwość kreowania reguł Firewall dla ruchu przychodzącego/wychodzącego z/do zadanej strefy, w określonych przedziałach czasu, z uwzględnieniem użytkowników, dla których reguła ma być aktywna 4. Możliwość włączania i wyłączania reguł Firewall i NAT bez konieczności ich usuwania 5. Wymagane jest, aby na urządzeniu uruchomione były następujące usługi w subskrypcji na okres <b>nie mniej niż 24 miesięcy</b> : <ul style="list-style-type: none"> <li>a. Sieciowa ochrona antywirusowa zapewniająca skanowanie ruchu na protokołach HTTP, FTP, POP3, SMTP, IMAP, ruch TCP oraz NetBios.</li> <li>b. Filtr antywirusowy powinien zapewniać skanowanie załączników poczty elektronicznej, plików skompresowanych ZIP i GZIP. Wymagane jest, aby możliwe było włączenie lub wyłączenie usługi antywirus w poszczególnych strefach bezpieczeństwa, oraz możliwość włączenia lub wyłączenia reagowania na określone sygnatury.</li> <li>c. Sonda IDP (detekcja i blokowanie wtargnięć do sieci) zapewniająca skanowanie ruchu w oparciu o sygnatury dostarczone przez producenta. Sygnatury powinny umożliwiać wykrywanie i blokowanie zdarzeń takich jak: korzystanie z programów do wymiany plików P2P (np. Limewire, BitTorrent, eMule, etc.), korzystanie z komunikatorów internetowych (np. Yahoo Messenger, Gadu-Gadu, Skype, etc.), ataki typu backdoor, exploit, SQL-Injection, etc. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.</li> <li>d. Sieciowa ochrona antyspyware, zapewniająca skanowanie ruchu HTTP, FTP, SMTP, POP3, IMAP. Wymagane jest, aby poza możliwością włączenia lub wyłączenia usługi IDP w poszczególnych strefach bezpieczeństwa możliwa była indywidualna konfiguracja każdej z sygnatur w celu uruchomienia bądź wyłączenia jej dla zadanych adresów IP, użytkowników lub przedziałów czasowych.</li> </ul>

		<ul style="list-style-type: none"> <li>e. Usługa filtrowania treści stron WWW, zapewniająca blokowanie apletów Java, aplikacji Active-X, plików cookie, definiowanie białych i czarnych list stron www, definiowanie słów kluczowych umożliwiających zablokowanie strony w przypadku ich wystąpienia. Dodatkowo wymagane jest tworzenie reguł filtrowania treści dla poszczególnych grup użytkowników umożliwiających filtrowanie treści w oparciu o informacje z zewnętrznych serwerów zawierających bazę stron. Wymagane jest, aby mechanizm filtrowania treści uwzględniał także filtrowanie stron HTTPS oraz możliwość włączenia lub wyłączenia mechanizmu filtrowania treści w poszczególnych strefach bezpieczeństwa i zdefiniowanie domyślnej reguły dla każdej ze stref działającej niezależnie od uprawnień poszczególnych użytkowników.</li> <li>f. Usługa Firewall aplikacji umożliwiająca definiowanie własnych sygnatur oraz reakcji urządzenia w przypadku wykrycia ruchu zgodnego z wprowadzonymi sygnaturami.</li> <li>g. Ochrona poczty elektronicznej w oparciu o białe/czarne listy nadawców oraz serwery RBL.</li> </ul> <ol style="list-style-type: none"> <li>6. Wymagana jest taka możliwość skonfigurowania połączeń IPSec VPN client-site, aby cały ruch z połączonych do urządzenia klientów był przesyłany poprzez urządzenie i możliwe było jego skanowanie przez mechanizmy antywirus, antyspyware, IDP, filtrowania treści.</li> <li>7. Wymaga się, aby na urządzeniu możliwe było włączenie blokowania ruchu przesyłanego pomiędzy strefami w przypadku, kiedy na stacjach roboczych lub serwerach nie ma zainstalowanego odpowiedniego oprogramowania antywirusowego, lub oprogramowanie to będzie miało nieaktualne sygnatury.</li> <li>8. Wymaga się, aby mechanizmy antywirus, antyspyware i sonda IDP nie posiadały ograniczeń co do wielkości skanowanych plików</li> </ol>
9	Wsparcie techniczne i gwarancja	<ol style="list-style-type: none"> <li>1. Wymagane jest aby dostarczane urządzenie objęte było okresem gwarancji przez <b>okres co najmniej 24 miesięcy</b>, z możliwością przedłużenia na dłuższy okres czasu. Wymagane jest, aby w ramach gwarancji uszkodzone urządzenie zostało wymienione w ciągu jednego dnia roboczego.</li> <li>2. Wymagane jest, aby urządzenie objęte było wsparciem technicznym 8x5, realizowanym przez producenta przez okres 24 miesięcy z możliwością przedłużenia na dłuższy okres czasu</li> </ol>
10	Dokumentacja, inne	Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego urządzenia z wymaganiami niniejszej specyfikacji.

**8. Zasilacz UPS - 1szt.**

Wymagania minimalne		
1	Moc wyjściowa (pozorna / czynna)	minimum 3000 VA
		minimum 3000 W
2	Topologia	VI (line interactive)
3	Typ obudowy	Rack 19"
4	Chłodzenie	Wymuszone, wewnętrzne wentylatory
WEJŚCIE		
5	Napięcie znamionowe (wartość skuteczna)	230 V AC
6	Zakres napięcia wejściowego (wartości skuteczne) i tolerancja	178 ÷ 281 V AC ± 2 %
7	Częstotliwość znamionowa napięcia wejściowego	50 Hz
8	Zakres częstotliwości i tolerancja	45 ÷ 55 Hz ± 1 Hz
9	Progi przełączania: sieć – UPS	178 ÷ 281 V AC ± 2 %
WYJŚCIE		
10	Napięcie znamionowe (wartość skuteczna)	230 V AC
11	Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa	195 ÷ 253 V AC ± 2 %
12	Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa	230 V AC ± 5 %
13	Automatyczna regulacja napięcia (AVR)	± 10 %
14	Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej)	Sinusoidalny / Tak jak na wejściu
15	Częstotliwość znamionowa napięcia wyjściowego	50 Hz
16	Filtracja napięcia wyjściowego	Filtr przeciwzakłóceńowy RFI/EMI, tłumik warystorowy
17	Progi przełączania: UPS – sieć	183 ÷ 276 V AC ± 2 %
18	Czas przełączenia na pracę rezerwową	< 3 ms
19	Czas powrotu na pracę sieciową	0 ms
20	Przeciążalność	> 105% - 15 s (wyłączenie UPS)
AKUMULATORY I CZASY PODTRZYMANIA		
21	Akumulatory wewnętrzne	minimum 8x 12 V / 7 Ah VRLA
22	Możliwość podpięcia modułów bateryjnych	wymagane minimum 1szt
23	Czas podtrzymania z baterii wewnętrznych ( 100 % / 80 % / 50 % Pmax)	minimum 3 / 4 / 7 min
24	Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza).	do 4 h
PARAMETRY MECHANICZNE		
25	Wymiary, montaż	Montaż w szafie RACK 19" o głębokości 1000 mm i pojemności 27U. Maksymalna wysokość 3U
ZABEZPIECZENIA		
26	Zabezpieczenie wejściowe	Przeciwzwarciove – Bezpiecznik automatyczny 16 A / 250 V AC Przeciwprzepięciowe
27	Zabezpieczenie wyjściowe	Elektroniczne – przeciwzwarciove i przeciążeniowe
28	Zabezpieczenia wejścia DC (akumulatory wewnętrzne)	Zabezpieczenie nadprądowe
29	Zabezpieczenia DC (zewnętrzny moduł bateryjny)	Zabezpieczenie nadprądowe
WYPOSAŻENIE I FUNKCJE DODATKOWE		
30	Przyłącze zasilania UPS	1 x IEC 320 C20 (16 A)



31	Przyłącza wyjściowe (liczba i typ gniazd)	minimum 3 x IEC320 C13 (10 A) - sterowalne
		minimum 3 x IEC320 C13 (10 A)
		minimum 1 x IEC320 C19 (16 A)
		minimum 2 x PL (z bolcem uziemiającym)
32	Sygnalizacja	Akustyczno – optyczna; graficzny wyświetlacz LCD, dioda LED
33	Interfejsy komunikacyjne	USB HID, SNMP/HTTP
34	Gniazdo na dodatkowe karty rozszerzeń	wymagane minimum 1 wolne gniazdo
35	Filtr teleinformatyczny (linii danych) – RJ45	LAN 1 Gbit/s
36	Wsporniki do montażu w szafie RACK	wymagane
37	Oprogramowanie monitorująco-zarządzające	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS .
		wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
		wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
ZASTOSOWANE STANDARDY		
38	Deklaracje	CE
39	Normy	PN-EN 62040-1:2009, PN-EN 62040-2:2008
GWARANCJA / SERWIS		
40	Gwarancja	min 36 miesięcy na elektronikę i 24 miesiące na akumulatory;
41	Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
		serwis realizowany w systemie door to door
DKUMENTACJA, INNE		
42	Wykonawca dostarczy wraz z ofertą oświadczenie o zgodności proponowanego urządzenia z wymaganiami niniejszej specyfikacji.	

## 9. Rozbudowa posiadanego przez Zamawiającego serwera- 1szt.

W ramach zadania wykonawca rozbuduje posiadany przez Zamawiającego serwer Actina Solar 100 S5 (system operacyjny Windows Server 2008 R2) o następujące elementy:

- 4szt. dysków 4TB 3.5", Fizyczna wielkość sektora: 512 E, Cache 256 MB. 7.2K RPM
- Sprzętowy kontroler RAID z pamięcią cache min 1GB, oraz niezbędnym okablowaniem do podłączenia dostarczanych dysków

## 10. Usługa wdrożenia.

Opis wdrożenia:

- a) Instalacja:
  - Demontaż istniejącego sprzętu z szaf RACK zlokalizowanych w siedzibie Zamawiającego
  - Instalacja dostarczonego sprzętu w szafach RACK.
  - Podłączenie urządzeń do sieci LAN zgodnie z wymaganiami Zamawiającego.
- b) Serwery
  - Podłączenie serwerów do sieci LAN: 2x porty SFP+ 10GB i 2x porty RJ-45 1GB.
  - Instalacja systemów operacyjnych opisanych w pkt 3 na serwerze.
  - Aktualizacja systemów operacyjnych do najnowszej wersji z wszystkimi poprawkami.
  - Aktualizacja oprogramowania firmware wszystkich komponentów serwera.
  - Stworzenie grup RAID dla serwerów:
    - Nowy serwer RAID 1+0: 4x dyski 1.2TB SAS 10K
    - Posiadany serwer Actina RAID 1+0 : 4x dyski 4TB NL-SAS 7.2K
- c) Przełączniki sieciowe
  - Wymiana posiadanych przełączników sieciowych na dostarczane z zachowaniem konfiguracji.
  - Uruchomienie segmentacji sieci na sieci wirtualne VLAN (BACKUP, DMZ, LAN, MGMT).
  - Podłączenie serwerów z wykorzystaniem portów SFP+ 10GB oraz reszty urządzeń RJ-45 1GB.
  - Konfiguracja protokołów STP, MSTP, ARP inspection i DHCP snooping.
- d) Macierz NAS
  - Stworzenie grupy RAID 5 z dysków twardych.
  - Udostępnienie zasobów na potrzeby wykonywania kopii zapasowej oraz udziałów sieciowych dla użytkowników.
  - Integracja z kontrolerem domeny.
- e) UPS
  - Podłączenie wszystkich urządzeń do dostarczonego UPS.
  - Uruchomienie funkcji automatycznego wyłączenia serwerów w przypadku zaniku zasilania oraz automatycznego włączania serwerów w przypadku powrotu zasilania wraz z instalacją i konfiguracją niezbędnego oprogramowania sterującego oraz przeprowadzeniem testów.
- f) Backup
  - Instalacja i konfiguracja dostarczonego oprogramowania do tworzenia kopii zapasowej, konfiguracja oprogramowania musi być zgodna z dobrymi praktykami producenta oprogramowania i zaakceptowana przez Zamawiającego.
  - Stworzenie harmonogramu wykonywania kopii zapasowej (kopia pełna, przyrostowa)
  - Konfiguracja posiadanego serwera Actina Solar 100 S5: instalacja dostarczanych komponentów oraz konfiguracja serwera (instalacja i konfiguracja systemu operacyjnego serwera wraz z dołączeniem do domeny) w celu stworzenia z przestrzeni dyskowej repozytorium danych dla systemu backup.
- g) Konfiguracja virtualizacji
  - Środowisko oparte o 1 serwer fizyczny
  - Konfiguracja wirtualnych switchy (podział na 4 podsieci: BACKUP, DMZ, LAN, MGMT)
- h) Konfiguracja urządzenia UTM
  - Konfiguracja routingu.
  - Zestawienie połączenia VPN z dwoma oddziałami zdalnymi (leśniczówki) oraz jednego połączenia dla administratora.

- Uruchomienie kanału zdalnego zarządzania całą dostarczoną infrastrukturą na dostarczonym urządzeniu UTM.
  - Konfiguracja polityk bezpieczeństwa w oparciu o kontrolę aplikacji, filtrowanie witryn, wykrywanie zagrożeń i włamań do sieci LAN.
  - Integracja z kontrolerem domeny.
- i) Migracja systemów
- Migracja i wirtualizacja oprogramowania i systemów operacyjnych znajdującego się na posiadanych przez Zamawiającego serwerach fizycznych na dostarczone środowisko. Testowanie poprawności działania przeniesionego oprogramowania (baz danych), oraz wykonywania połączeń z zasobami sieciowymi, logowaniem i autoryzacją użytkowników, zasadami użytkowników, dostępem do sieci Internet, poprawności działania kluczy sprzętowych z posiadanymi przez Zamawiającego licencjami oprogramowania sieciowego (system ERP Optima oraz ESRI ArcGIS ver.9.3), działaniem baz danych obsługiwanych przez serwery, przeniesienie zasobów plikowych przechowywanych na dotychczasowych serwerach, migracja domeny Windows (wraz z przeniesieniem wszystkich ustawień, kont użytkowników i urządzeń przyłączonych do domeny itd.). Po migracji serwer obsługujący domenę (kontroler domeny), serwer baz danych oraz serwer danych GIS zachowają dotychczasowe adresy IP. Wraz z migracją domeny zostaną zachowane dotychczasowe pule adresów IP w sieci wraz z istniejącymi zakresami adresów IP wyłączonych z rozpowszechniania.
  - Migracja będzie dotyczyć 3 serwerów fizycznych:
    - Serwer 1 – podstawowy kontroler domeny (działający obecnie pod kontrolą systemu Windows Server 2008 R2)
    - Serwer 2 – zapasowy kontroler domeny (działający obecnie pod kontrolą systemu Windows Server 2008 R2) pełniący rolę serwera baz danych (1 baza danych w wersji MS SQL 2008 R2 i jedna baza danych w wersji MS SQL 2014), serwer klucza licencyjnego dla systemu Optima
    - Serwer 3 – serwer danych GIS (działający obecnie pod kontrolą systemu Windows 2008) – serwer danych plikowych, serwer klucza licencyjnego dla oprogramowania ESRI ArcGIS
- j) Dokumentacja powykonawcza
- Dokumentacja powykonawcza zawierająca, schematy, opisy urządzeń, numery seryjne oraz instrukcje i dokumenty dostarczane przez producentów sprzętu zarówno w postaci papierowej jak i w postaci nośników elektronicznych.

**Prace związane z modernizacją urządzeń serwerowni, a w szczególności migracją domeny oraz konfiguracją połączenia internetowego i dostępu VPN prowadzone powinny być w sposób nie zakłócający normalnej pracy w Dyrekcji PNGS (w szczególności działu księgowości oraz działu ochrony zasobów przyrodniczych).**

**Szczegółowy harmonogram prac (w tym czas wyłączenia serwerów oraz prace montażowe) zostanie uzgodniony z przedstawicielem Zamawiającego.**

Jeżeli producent dostarcza oprogramowanie będące przedmiotem zamówienia na nośnikach elektronicznych, Wykonawca zobowiązany jest dostarczyć Zamawiającemu wraz z dokumentami licencyjnymi oryginały nośników zawierających to oprogramowanie. W przypadku, gdy oprogramowanie jest udostępniane wyłącznie w postaci plików na serwerach producenta, Wykonawca wskaże w odrębnym dokumencie adresy serwerów, z których możliwe jest pobranie najnowszych, legalnych wersji dostarczonego oprogramowania.

**Dostawca zapewni zdalne wsparcie powdrożeniowe inżyniera w wymiarze 10 godzin.**

Instalacja i konfiguracja będzie wykonywana przez inżynierów posiadających:

- co najmniej 1 certyfikat producenta potwierdzający umiejętności konfiguracji i obsługi oferowanego urządzenia UTM
- co najmniej 1 certyfikat producenta potwierdzający umiejętności konfiguracji i obsługi oferowanych przełączników sieciowych

Wszystkie urządzenia dostarczone przez Wykonawcę pochodzić będą z legalnego źródła, zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i świadczonych przez sieć serwisów producenta na terenie Polski. Sprzęt będzie fabrycznie nowy i nie będzie pochodził z dostawy do realizacji projektu u innego klienta.