ZESTAWIENIE PARAMETRÓW TECHNICZNO UŻYTKOWYCH OFEROWANEGO SPRZĘTU		
Cecha/Funkcjonalność	**Minimalne parametry wymagane przez Zamawiającego**	**Parametry oferowane przez Wykonawcę (wypełnia Wykonawca).**
Serwery – 2 szt. (dostawa z wdrożeniem, konfiguracją i przeszkoleniem)		Producent* ……...…… Model * …….
Obudowa	Do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych. Możliwość zamontowania ramienia do prowadzenia kabli.	
Procesor	Architektura x86, maksymalny TDP dla procesora – 135W. Wymagana ilość rdzeni dla procesora – min 16. Minimalna częstotliwość pracy procesora 2.4GHz. Minimalna ilość kanałów procesora – 8 . Wynik wydajności procesora zainstalowanego w oferowanym serwerze nie powinien być niższy niż 233 punktów base w teście SPECrate 2017 Integer, opublikowanym przez SPEC.org (www.spec.org) dla konfiguracji dwuprocesorowej. Test przeprowadzony przez producenta serwera musi być zamieszczony na stronie spec.org. Obsługa minimum dwóch procesorów..	Producent procesora…… Typ…….. Model ……. Ilość punktów w teście SPECrate 2017 Integer ……
Liczba procesorów	2	
Płyta główna	Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje	
Pamięć operacyjna	Zainstalowane minimum 128GB pamięci RAM o częstotliwości 3200MHz w modułach 32GB. Zainstalowana pamięć powinna być sygnowana i zoptymalizowana do użycia przez producenta serwera. Minimum 32 sloty na pamięć. Możliwość rozbudowy do 8TB RAM przy użyciu pamięci RDIMM Łączna ilość zainstalowanej pamięci RDIMM oraz pamięci persistent memory powinna wynosić minimum 12TB	
Zabezpieczenie pamięci	memory mirroring, ECC, SDDC, ADDDC	
Procesor Graficzny	Zintegrowana karta graficzna z minimum 16MB pamięci osiągająca rozdzielczość 1920x1200 przy 60 Hz. 1 port VGA na tylnym panelu serwera.	
Rozbudowa dysków	W chwili dostawy serwer musi posiadać 8 zatok na dyski 2,5” w tym	

	musi posiadać zainstalowane: 2 dyski 2,5" SSD o pojemności min 960GB każdy.
Kontroler dyskowy	Zainstalowany sprzętowy kontroler SAS 12Gb do obsługi dysków wewnętrznych. Kontroler musi posiadać 2GB pamięci Flash. Kontroler musi obsługiwać poziomy RAID - 0/1/10/5/50/6/60.
Zasilacz	Minimum dwa redundantne zasilacze o mocy minimum 750W z certyfikatem minimum Titanium. Moc pojedynczego zasilacza musi być wystarczająca do zasilenia serwera w oferowanej konfiguracji.
Interfejsy sieciowe	Zainstalowane: • Karta posiadająca 4 porty 1Gb. Karta nie może zajmować żadnego ze slotów wyszczególnionych w sekcji Dodatkowe sloty I/O • Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej.
Dodatkowe karty	Zainstalowane Dwie karty dwuportowe FC 16Gb
Dodatkowe sloty I/O	W chwili dostawy serwer powinien posiadać 3 sloty PCIe Gen4 x16
Dodatkowe porty	• z przodu obudowy: 1x USB 3.1, 1x USB 2.0 • z tyłu obudowy: 3x USB 3.1, 1x VGA . Możliwość instalacji portu DB9 • wewnątrz obudowy: 1x USB3.1
Chłodzenie	Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1
Zarządzanie	Zintegrowany z płytą główną serwera, niezależny od systemu operacyjnego, sprzętowy kontroler zdalnego zarzadzania umożliwiający: • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: cpu, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, utylizacja cpu, utylizacja pamięci oraz komponentów I/O • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH

	• Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS • Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. Wymagany wbudowany sprzętowy kontroler zdalnego zarządzania, który musi być umieszczony na osobnej dedykowanej płytce I/O (wspomnianej w sekcji Dodatkowe Porty). Płytka I/O musi posiadać swój własny min. 2 rdzeniowy procesor o taktowaniu min. 1.2GHz. • Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna • Pozyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzajacej, utylizacja cpu, utylizacja pamięci oraz komponentow I/O, lokalizacja • Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów. • Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń. • Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3 • Update systemowego firmware • Monitoring i możliwość ograniczenia poboru prądu • Zdalne włączanie/wyłączanie/restart • Zapis video zdalnych sesji • Podmontowanie lokalnych mediów z wykorzystaniem Java client • Przekierowanie kosnoli szeregowej przez IPMI • Zrzut ekranu w momencie zawieszenia systemu • Możliwość przejęcia zdalnego ekranu • Możliwość zdalnej instalacji systemu operacyjnego • Alerty Syslog • Przekierowanie konsoli szeregowej przez SSH • Wyświetlanie danych aktualnych I historycznych dla użycia energii oraz temperatury serwera • Możliwość mapowania obrazów ISO z lokalnego dysku operatora • Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS

	• Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę • wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API • Wymaga się możliwości wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z karta zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego. • Kontroler zarządzania musi posiadać 4Gb wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware. • Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u. • Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami. Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200. Wraz z serwerem powinno zostać dostarczone dodatkowe oprogramowanie zarządzające umożliwiające: - zarzadzanie infrastruktura serwerów i storage bez udziału dedykowanego agenta - przedstawianie graficznej reprezentacji zarządzanych urządzeń - możliwość skalowania do minimum 1000 urządzeń - obsługę szyfrowanej komunikacji z zarządzanymi urządzeniami, wsparcie dla NIST 800-131A oraz FIPS 140-2 - wsparcie dla certyfikatów SSL tzw self-signed oraz zewnętrznych - udostępnianie szybkiego podgląd stanu środowiska - udostępnianie podsumowania stanu dla każdego urządzenia - tworzenie alertów przy zmianie stanu urządzenia - monitorowanie oraz tracking zużycia energii przez monitorowane urządzenie, możliwość ustalania granicy zużycia energii, - konsola zarzadzania oparta o HTML 5 - dostępność konsoli monitorującej na urządzeniach przenośnych ze wsparciem dla systemu Android oraz iOS, aplikacja musi umożliwiać włączenie wyłączenie oraz restart urządzenia, musi również mieć możliwość aktywowania diody lokacyjnej na urządzeniu, - automatyczne wykrywanie dołączanych systemów oraz szczegółowa inwentaryzacja - możliwość podnoszenia wersji oprogramowania dla komponentów zarządzanych serwerów w oparciu o repozytorium lokalne jak i zdalne dostępne na stronie producenta oferowanego rozwiązania - definiowanie polityk zgodności wersji firmware komponentów zarządzanych urządzań - definiowanie roli użytkowników oprogramowania

	- obsługa REST API oraz Windows PowerShell - obsługa SNMP, SYSLOG, Email Forwarding - autentykacja użytkowników: centralna (możliwość definiowania wymaganego poziomu skomplikowania danych autentykacyjnych) oraz integracja z MS AD oraz obsługa single sign on oraz SAML - obsługa tzw Forward Secrecy w komunikacji z zarządzanymi urządzeniami - przedstawianie historycznych aktywności użytkowników -blokowanie możliwości podłączenia innego systemu zarzadzania do urządzeń zarządzanych - tworzenie dziennika zdarzeń ukończonych sukcesem lub bledem, oraz zdarzeń będących w trakcie. Możliwość definiowania filtrów wyświetlanych zdarzeń z dziennika. Możliwość eksportu dziennika zdarzeń do pliku csv - Obsługa NTP - przesyłanie alertów do konsoli firm trzecich - tworzenie wzorców konfiguracji zarządzanych urządzeń (definiowanie przez konsole albo kopiowanie konfiguracji z już zaimplementowanych urządzeń) - instalowanie systemów operacyjnych oraz wirtalizatorów Vmware i Hyper-V. Wymagana jest integracja konsoli zarządzania z konsolą wirtualizatora tak, aby zarządzanie środowiskiem sprzętowym mogło odbywać się z konsoli wirtualizatora. Wymaga się możliwości instalacji systemu na przynajmniej 20 nodach jednocześnie - możliwość automatycznego tworzenia zgłoszeń w centrum serwisowym producenta dla określonych zdarzeń wraz z przesylem plików diagnostycznych, Producent serwera ponadto powinien mieć w swojej ofercie narzędzia integrujące zarządzanie infrastrukturą z następującymi produktami: VMware vCenter, Microsoft AdminCenter, Microsoft SystemCenter, RedHat CloudForms, Splunk. Wyżej wymienione oprogramowanie musi mieć również możliwość zarządzania pozostałym sprzętem oferowanym w ramach tego postępowania tj. Switchem SAN
Funkcje zabezpieczeń	Możliwość instalacji czujnika otwarcia obudowy zintegrowanego z modułem zarządzania serwerem, hasło włączania, hasło administratora, moduł TPM. Możliwość zainstalowana przedniego panelu zabezpieczającego zamykanego na klucz.
Urządzenia hot-swap	Dyski twarde, zasilacze, wentylatory.
Obsługa	Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ów PCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych.
Diagnostyka	Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID Możliwość użycia aplikacji mobilnej na telefonie, do przeglądania awarii, konfiguracji i włączenia/wyłączenia serwera.
Systemy operacyjne	Microsoft Windows Server 2016, 2019, 2022, Red Hat Enterprise Linux 7, 8, 9 SUSE Linux Enterprise Server 12 oraz 15, VMware vSphere (ESXi) 6, 7, 8, Ubuntu 18, 20, 22
Gwarancja	Serwer powinien posiadać min. 24 miesięczną gwarancję producenta on-site z czasem reakcji NBD. Uszkodzone nośniki danych pozostają własnością

	zamawiającego. Możliwość wykupienia dodatkowego serwisu zapewniającego gwarantowany czas naprawy serwera w ciągu 6 godzin. W przypadku braku funkcjonalności przewidywania awarii dla wszystkich komponentów wymienionych w punkcie Diagnostyka wymagane jest dostarczenie serwera nadmiarowego, mogącego zastąpić funkcjonalni jak i wydajnościowo wymagane powyżej maszyny. Wszystkie komponenty serwera powinny być sygnowane i zoptymalizowane do użycia przez producenta serwera. - Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać Autoryzacje producenta urządzeń – dokumenty potwierdzające - należy załączyć do oferty. Dokument musi być oznaczony nazwą i numerem postępowania. - Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Dokument musi być oznaczony nazwą i numerem postępowania - Wymagane dołączenie do oferty oświadczenia Producenta, z którego będzie wynikało, iż w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 – dokumenty należy dołączyć do oferty. Serwer musi posiadać deklaracja CE – dokument należy dołączyć do oferty.
Switche typu 1 (2 sztuki) (dostawa z wdrożeniem, konfiguracją i przeszkoleniem)	Producent* ……...…… Model * ……
Obudowa	Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U wraz z kompletem odpowiednich szyn mocujących dedykowanych przez producenta przełącznika.
Technologia	Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8, 4Gbs, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji. Przełącznik FC musi mieć możliwość instalacji wkładek SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km z prędkością 16Gb/s. Jeśli powyższa funkcjonalność wymaga licencji, nie wymaga się jej w momencie dostawy przełącznika.
Porty	Przełącznik FC musi być wyposażony, w co najmniej 8 aktywnych portów FC obsadzone wkładkami SFP 16Gb/s krótkiego zasięgu. Rodzaj obsługiwanych portów: E, D, M oraz F.
Przepustowość	Architektura non-blocking pozwalająca na pracę wszystkich portów przełącznika równocześnie z pełną prędkością 32Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC. Całkowita przepustowość przełącznika FC musi wynosić minimum 768Gb/s. Opóźnienie przy

	przesyłaniu ramek FC między dowolnymi portami przełącznika nie większe niż 1µs.
Funkcjonalność	Przełącznik FC musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami z przynajmniej ośmiu linków. Połączenie zagregowane musi być zrealizowane na poziomie ramek FC. Jeśli do aktywacji tej funkcjonalności wymagana jest dedykowana licencja, nie wymaga się jej w momencie dostawy. Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa: • szyfrowanie połączenia z konsolą administracyjną, wsparcie dla SSH, • definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control), • definiowane kont administratorów w środowisku RADIUS, Active Directory, LDAP, TACACS+, • szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS, • obsługa SNMP • obsługa protokołów SCP oraz SFTP,
Zarządzanie i konfiguracja	Możliwość zarządzania poprzez konsole graficzną oraz tryb tekstowy CLI. Interfejsy: zintegrowany port Ethernet, RS232 oraz port USB na potrzeby przenoszenia plików firmware, plików konfiguracji, plików log. Switch musi posiadać możliwość zarządzania z poziomu oprogramowania do zarządzania opisanego przy serwerze w tym postępowaniu.
Gwarancja i wsparcie	Min. 24 miesięcy gwarancji producenta on-site z czasem reakcji NBD. Możliwość zgłaszania awarii poprzez linię telefoniczną producenta lub firmy serwisującej. Gwarancja realizowana przez Producenta lub Autoryzowany Serwis Producenta. - Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać Autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Dokument musi być oznaczony nazwą i numerem postępowania. - Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Dokument musi być oznaczony nazwą i numerem postępowania Switch musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001 – dokumenty należy dołączyć do oferty. Switch musi posiadać deklarację CE – dokument należy dołączyć do oferty.
Switche typu 2 - 4 sztuki (dostawa z wdrożeniem, konfiguracją i przeszkoleniem)	Producent* ……..…… Model * ……
Ilość portów	48 porty 1GBaseT, 2 x SFP+ oraz 2 x 10GBaseT niezależne

Chłodzenie od przodu do tyłu obudowy	Tak	
Możliwość instalacji redundantnego zasilacza	Tak	
Tablica MAC	min. 16K	
Bufor	16Mb	
MTBF	min. 578472 godzin	
Wydajność	min. 130,9 Mp/s	
Przepustowość	min. 176 Gb/s	
Porty	• Port USB • Port miniUSB • Port zarządzania Out-of-band;	
Protokoły oraz funkcje	• Web GUI • HTTPs • CLI • Telnet • SSH • SNMP • MIB RSPAN • Radius • TACACS+ • DiffServ • Możliwość łączenia w stos za pomocą interfejsów 10Gb/s • Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh • Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram • IPv4/IPv6 Multicast filtering • IGMPv3 MLDv2 Snooping • ASM & SSM • IGMPv1,v2 Querier • Auto-VoIP • Auto-iSCSI • Policy-based routing (PBR) • LLDP-MED • Spanning Tree • Green Ethernet • STP • MTP • RSTP • PV(R)STP • BPDU/STRG Root Guard • EEE (802.3az) • GVRP/GMRP • Q in Q,	

	• Private VLAN • DOT1X • MAB • Captive Portal • DHCP Snooping • Dynamic ARP • Inspection • IP Source Guard • CPU min 800 Mhz • Min 1GB RAM • Min 256MB Flash • Min ilość obsługiwanych VLAN 4K • DHCP Server min 2K rezerwacji • OSPFv3 min. sąsiadów 400 • OSPFv3 min. sąsiadów na interfejs 100 • UDLD • LLPF • DHCPv6 Snooping • wysyłanie alertów na email • MMRP • Ilość ACL min. 100 • Ilość reguł na listę min. 1023 na wejściu • Zasilacz z certyfikatem 80+ • CE: EN 55032:2012+AC:2013/CISPR 32:2012, EN 61000-3-2:2014, • Class A, EN 61000-3-3:2013, EN 55024:2010 • VCCI : VCCI-CISPR 32:2016, Class A • RCM: AS/NZS CISPR 32:2013 Class A • FCC: 47 CFR FCC Part 15, Class A, ANSI C63.4:2014 • ISED: ICES-003:2016 Issue 6, Class A, ANSI C63.4:2014 • BSMI: CNS 13438 Class A
Gwarancja	Min 24 miesiące. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające że urządzenie jest objęte gwarancją producenta realizowaną w systemie door-to-door przez serwis producenta. Urządzenie będzie objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii w okresie gwarancji.
Urządzenie typu UTM (dostawa z wdrożeniem, konfiguracją i przeszkoleniem)	
Wymagania Ogólne	System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne

	platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System wspiera protokoły 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 – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji. 2.Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 3.Monitoring stanu realizowanych połączeń VPN. 4.System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych
Interfejsy, Dysk, Zasilanie:	1.System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów: •8 portami Gigabit Ethernet RJ-45. •2 gniazdami SFP 1 Gbps. 2.System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 3.System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q. 4.System jest wyposażony w zasilanie AC.
Parametry wydajnościowe:	1.W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę. 2.Przepustowość Stateful Firewall: nie mniej niż 6,5 Gbps dla pakietów 512 B. 3.Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. 4.Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. 5.Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. 6.Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps. 7.Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.
Funkcje Systemu Bezpieczeństwa:	W ramach systemu ochrony są 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. 5.Ochrona przed atakami - Intrusion Prevention System. 6.Kontrola stron WWW. 7.Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8.Zarządzanie pasmem (QoS, Traffic shaping). 9.Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 10.Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site. 11.Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. 12.Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. 13.Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).
Polityki, Firewall	1.Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2.System realizuje 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 istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4.Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP. 5.Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe. 6.Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna. 7.Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu. •Amazon Web Services (AWS). •Microsoft Azure. •Cisco ACI. •Google Cloud Platform (GCP). •OpenStack. •VMware NSX. •Kubernetes.
Połączenia VPN	1.System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:

	•Wsparcie dla IKE v1 oraz v2. •Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM). •Obsługa protokołu Diffie-Hellman grup 19, 20. •Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh. •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. •Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat. •Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu. •Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu. •Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth. •Mechanizm „Split tunneling" dla połączeń Client-to-Site. 2.System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia: •Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0. •Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. •Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
Routing i obsługa łączy WAN	W zakresie routingu rozwiązanie zapewnia obsługę: 1.Routingu statycznego. 2.Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). 3.Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. 4.Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. 5.ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. 6.BFD (Bidirectional Forwarding Detection). 7.Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
Funkcje SD-WAN	1.System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. 2.SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
Zarządzanie pasmem	1.System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

	2.System daje możliwość określania pasma dla poszczególnych aplikacji. 3.System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. 4.System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.
Ochrona przed malware	1.Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2.Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. 3.System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości. 4.System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. 5.System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 6.Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 7.System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze. 8.System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. 9.Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. 10.Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
Ochrona przed atakami	1.Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2.System chroni przed atakami na aplikacje pracujące na niestandardowych portach. 3.Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 4.Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. 5.System zapewnia 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). 7.Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. 8.Wykrywanie i blokowanie komunikacji C&C do sieci botnet. 9.Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji	1.Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2.Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 3.Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 4.Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 5.Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. 6.Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). 7.System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).
Kontrola WWW	1.Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2.W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3.Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. 4.Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 5.Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). 6.Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. 7.Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. 8.Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. 9.System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
Uwierzytelnianie użytkowników w ramach sesji	1.System Firewall umożliwia 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.System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.

	3.System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie. 4.Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.
Zarządzanie	1.Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania. 2.Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. 3.Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4.System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. 5.System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 6.Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 7.Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. 8.Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). 9.Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.
Logowanie	1.Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2.W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania. 3.Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. 4.Możliwość włączenia logowania per reguła w polityce firewall. 5.System zapewnia możliwość logowania do serwera SYSLOG. 6.Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
Certyfikaty	Poszczególne elementy systemu bezpieczeństwa posiadają następujące certyfikacje: •ICSA lub EAL4 dla funkcji Firewall.
Serwisy i licencje	Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: a) Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego

	Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy.
Gwarancja oraz wsparcie	Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.
Rozszerzone wsparcie serwisowe	System jest objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy. Dla zapewnienia wysokiego poziomu usług podmiot serwisujący posiada certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe są przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim 24x7. Wymagania powinny być potwierdzone dokumentami.
Oprogramowanie Managera logów - 1 sztuka (dostawa z wdrożeniem, konfiguracją i przeszkoleniem)	Producent* ……...…… Model * ……
Wymagania Ogólne	W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy sprzętowej lub programowej. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
Interfejsy, Dysk, Zasilanie	1.System musi dysponować co najmniej: •2 portami Gigabit Ethernet RJ-45. 2.Rozwiązanie musi dysponować powierzchnią dyskową min. 4 TB. 3.System musi być wyposażony w zasilanie AC.
Parametry wydajnościowe	1.System musi być w stanie przyjmować minimum 25 GB logów na dzień. 2.System musi być w stanie przeanalizować minimum 500 logów na sekundę. 3.Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 50 systemów. W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje
Logowanie	1.Podgląd logowanych zdarzeń w czasie rzeczywistym. 2.Możliwość przeglądania logów historycznych z funkcją filtrowania. 3.System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej: a. Listę najczęściej wykrywanych ataków. b. Listę najbardziej aktywnych użytkowników.

	c. Listę najczęściej wykorzystywanych aplikacji. d. Listę najczęściej odwiedzanych stron www. e. Listę krajów , do których nawiązywane są połączenia. f. Listę najczęściej wykorzystywanych polityk Firewall. g. Informacje o realizowanych połączeniach IPSec. 4.Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów. 5.Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514. 6.System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
Raportowanie	W zakresie raportowania system musi zapewniać: 1.Generowanie raportów co najmniej w formatach: PDF, CSV. 2.Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników. 3.Funkcję definiowania własnych raportów. 4.Możliwość spolszczenia raportów. 5.Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.
Korelacja logów	W zakresie korelacji zdarzeń system musi zapewniać: 1.Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany. 2.Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa. 3.Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń: •Malware. •Aplikacje sieciowe. •Email. •IPS. •Traffic. •Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.
Zarządzanie	1.System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI. 2.System musi umożliwiać definiowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
Serwisy i licencje	Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Wsparcie serwisowe	•Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). •Certyfikat ISO 9001 podmiotu serwisującego.
Rozszerzone wsparcie serwisowe	1. System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres 24 miesięcy. 2. Zgłoszenia serwisowe będą przyjmowane w języku polskim przez dedykowany serwisowy moduł internetowy oraz infolinię w języku polskim.
Opisy do wymagań ogólnych	1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (t.j. Dz.U. 2023.0.1582) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania. 2. Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż Wykonawca posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.
Urządzenie UPS - 2 sztuki	Producent* ……...…… Model * ……
Ogólne	Zasilacz UPS o mocy 3000VA/2700W musi zapewnić czas podtrzymania minimum 3 minuty dla obciążenia 2700 W. Zasilacz UPS wykonany w technologii podwójnej konwersji on-line z automatycznym bypassem oraz czystym sinusoidalnym przebiegiem napięcia. Uniwersalna obudowa Tower/Rack maksymalna wysokość 2U. Zasilacz UPS dostarczany wraz z kompletem przewodów oraz zestawem szyn do montażu w szafie Rack. UPS wyposażony w funkcję zimnego startu
Parametry wejściowe	•Napięcie znamionowe: 208/220/230/240 V

	• Tolerancja napięcia: 180– 280V dla 100% obciążenia oraz 120-300V dla 50% obciążenia •Częstotliwość : 50 / 60 Hz z automatycznym wyborem • Gniazdo wejściowe IEC 320-C20 (16A)
Parametry wyjściowe	• Napięcie (czysty przebieg sinusoidalny): 208/220/230/240 V • Częstotliwość: 50 /60 Hz ± 8% (± 0,1% w trybie akumulatorowym) • Współczynnik mocy 0,9 • Przeciążalność: < 105% w sposób ciągły; < 130% przez 30s < 150% przez 3 s; > 150% natychmiastowe wyłączenie • Gniazda wyjściowe: 6 x IEC 320-C13 (10A), 1x IEC 320 (16A)
Bateria	• Hermetyczne, bezobsługowe akumulatory o żywotności 3-5 lat wg klasyfikacji EUROBAT. • UPS posiada wewnątrz 1 łańcuch bateryjny zbudowany z 6 szt. akumulatorów 12V/9Ah. • Czas ładowania baterii < 4 godz. do pojemności użytkowej 80 % wydajności po całkowitym rozładowaniu • Możliwość sprawdzenia stanu baterii – Zamawiający zastrzega możliwość przeprowadzenia testu baterii przy odbiorze.
Urządzenie musi posiadać wyświetlacz LCD - Panel sterowania z funkcjami	• Poziom naładowania/stan baterii • Informacje o czasie podtrzymania • Alarm ogólny • Poziom/ stan obciążenia • Informacje o napięciu wejściowym • Informacje o napięciu wyjściowym • Tryb UPS normalny/praca z użyciem baterii • Informacje o usterce • Wyciszenie alarmu akustycznego
Zasilacz UPS musi posiadać alarmy dźwiękowe sygnalizujące	• tryb bateryjny, • przeciążenie, • konieczność wymiany baterii
Zasilacz UPS musi być zgodny z Normami	• Bezpieczeństwo: EN 62040-1 • Kompatybilność elektromagnetyczna EMC: EN 62040-2 • Sprawność: EN 62040-3 • Certyfikaty: RoHS, CE • Stopień ochrony IP: min. IP20
Zasilacz UPS musi spełniać parametry środowiskowe co najmniej takie jak	• Temperatura pracy od 0 °C do +40 °C (optymalne warunki żywotności baterii w zakresie temperatur od 15 °C do 25 °C) • Wilgotność: 20-90 % bez kondensacji • Poziom hałasu w odległości 1 m < 50 dB
Wymiary szer. x głęb. x wys. (mm)	max. 440 x 630 x 90; 2U
Waga	Max. 30 kg
Komunikacja	1. Zasilacz musi być wyposażony w kartę komunikacyjną posiadającą poniższe funkcje oraz parametry: o połączenie z siecią Ethernet (złącze RJ 45), o zarządzanie zasilaczem UPS za pomocą protokołu SNMP o monitorowanie zasilacza UPS przez przeglądarkę internetową 2. Możliwość dodania ręcznego bypassu serwisowego z gniazdami IEC 4 x IEC 10A + 1 x IEC 16A o wysokości 1 U. Bypass musi być tego samego producenta co zasilacz UPS.
Gwarancja	24 miesiące

Oprogramowanie do wirtualizacji – 1 sztuka (dostawa z wdrożeniem, konfiguracją i przeszkoleniem)	Producent* ……...…… Model * ……
System wirtualizacji	▪Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych, ▪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 zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne wyposażone w 320 logicznych wątków oraz do 4TB pamięci fizycznej RAM, ▪Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych, ▪Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości do 62 TB, ▪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 w możliwie największym stopniu być 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 wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows NT 4.0, Windows 2000, Windows Server 2003,

	Windows Server 2008, Windows Server 2012, Windows 7, Windows 8, SLES 11, SLES 10, SLES 9, SLES 8, RHEL 6, RHEL 5, RHEL 4, RHEL 3, Solaris 11 ,Solaris 10, Solaris 9, Solaris 8, OS/2 Warp 4.0, NetWare 6.5, NetWare 6, NetWare 5, OEL 4, OEL 5, Debian, CentOS, FreeBSD, Asianux, Mandriva, Ubuntu 12.04, SCO OpenServer, SCO Unixware, Mac OS X, ▪Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji, ▪Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na 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, ▪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 musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory, ▪Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn, ▪Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych w obrębie klastra serwerów fizycznych, ▪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 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). ▪Dostarczona wraz z oprogramowaniem licencja musi zapewniać możliwość instalacji na minimum 2 serwerach fizycznych (o parametrach jak serwer niniejszego zamówienia), zapewniając jednocześnie możliwość utworzenia jednego klastra, w ramach którego będzie możliwa migracja maszyn pomiędzy hostami w locie (bez przerwy w działaniu).

Podpisany elektronicznie przez
LESZCZYŃSKI Marek Paweł
16.10.2024
15:24:37 +02'00'