Serwer – sztuk 2 – wymagania minimalne		
LP	**Parametr lub warunek**	**Minimalne wymagania**
1	Obudowa	-Typu Rack, wysokość maksimum 2U; -Dostarczona wraz z szynami umożliwiającymi pełne wysunięcie serwera z szafy rack; -Szyny montażowe muszą zostać dostarczone wraz z ramieniem porządkującym przewody za serwerem;
2	Płyta główna	-Wieloprocesorowa (2 lub 4 procesorowa), wyprodukowana i zaprojektowana przez producenta serwera, możliwość instalacji procesorów 28-rdzeniowych; -Wyposażona w minimum 24 gniazda pamięci RAM DDR4, obsługa minimum 3000GB pamięci RAM DDR4 2933 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 bateryjnego stanu pamięci) – minimum 12 gniazd pamięci RAM musi umożliwiać wymienną instalację tego typu modułów; -Sumarycznie minimum 6 złącz PCI Express generacji 3, w tym minimum 3 złącza o prędkości x16; -Aktywne wszystkie sloty PCIe; -Minimum 2 sloty dla dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express) nie zajmujące klatek dla dysków hot-plug; -Zainstalowany moduł TPM 2.0;
3	Procesory	-Zainstalowany minimum jedne procesor 20-rdzeniowy w architekturze x86 o standardowej częstotliwości taktowania min. 2,1 GHz osiągające wynik w testach wydajności SPECrate2017_int_base min. 91,5 pkt. dla oferowanego modelu serwera. Wymagamy aby był załączony PDF ze strony spec.org i poświadczony przez producenta serwera oferowanego w postępowaniu. Nie dopuszcza się procesorów o większej ilości rdzeni fizycznych z uwagi na optymalizację kosztową licencjonowania aplikacji i systemów operacyjnych;
4	Pamięć RAM	-Zainstalowane 256 GB pamięci RAM typu DDR4 Registered, 2933Mhz w kościach o pojemności 32 GB; -Wsparcie dla technologii zabezpieczania pamięci Advanced ECC, Memory Scrubbing, SDDC; -Wsparcie dla konfiguracji pamięci w trybie „Rank Sparing”
5	Kontrolery dyskowe, I/O	-Zainstalowany sprzętowy kontroler SAS 3.0 obsługujący poziomy RAID 0,1,5,10,50;
6	Dyski twarde	-Zainstalowane min. 2 dyski SSD o pojemności min. 960 GB każdy, parametr DWPD min. 1,5 ; -Minimum 8 wnęk dla dysków twardych Hotplug 2,5”. Możliwość rozbudowy do 16 zatok na dyski 2,5”.
7	Inne napędy zintegrowane	-Możliwość instalacji wewnętrznego napędu LTO-7 SAS lub LTO-8 SAS. Alternatywnie dopuszcza się zaoferowanie dodatkowej obudowy rack max 1U dla napędu LTO7/8 wyposażonej w nadmiarowe zasilacze hotplug i okablowanie oraz dostarczenie oferowanego serwera wraz z zainstalowanym kontrolerem SAS HBA umożliwiającym podłączenie i

		poprawną pracę oferowanej obudowy wyposażonej w napęd LTO-7 lub LTO-8 z oferowanym serwerem; Obudowa musi być objęta jednolitym serwisem takim jak oferowany serwer; -Zainstalowany fabrycznie, wewnętrzny napęd optyczny DVD-RW;
8	Kontrolery LAN	-Jedna dwuportowa karta 2x1 Gbit/s RJ-45 ze wsparciem iSCSI, niezajmująca slotu PCI Express; -Zainstalowana dodatkowa osobna karta sieciowa wyposażona w porty - 2 x 10Gbit/s SFP+(wraz z wkładkami SFP+ MM), niezajmująca slotu PCI Express (dopuszcza się instalację w slocie PCI Express pod warunkiem dostarczenia serwera z większą niż wymagana ilości slotów PCI Express); -Dodatkowa osobna dwuportowa karta sieciowa, wyposażona w porty 1Gbit/s RJ-45;
9	Kontrolery I/O FC/SAS/Inne	-Zainstalowana karta SAS HBA, karta wyposażona w min. 2 zewnętrzne porty SAS 12 Gb/s (MiniSASHD-8644);
10	Porty	-Zintegrowana karta graficzna ze złączem VGA wyprowadzonym na tył obudowy serwera; -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 minimum 800W każdy, o sprawności 94%, dostarczone wraz z kablami C13-C14 o długości 2,5m każdy; -Redundantne wentylatory hotplug;
12	Zarządzanie	-Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera (system przewidywania/rozpoznawania awarii) – co najmniej informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów: karty rozszerzeń zainstalowane w dowolnym slocie PCI Express, procesory CPU, pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM, zainstalowany na płycie głównej nośnik pamięci M.2 SSD, status karty zarządzającej serwera, wentylatory, bateria podtrzymująca ustawienia BIOS/Płyty głównej, zasilacze - poprawność napięć elektrycznych płyty głównej w trybie włączonym (on) i oczekiwania (standby) serwera; -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 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 32Gbit/s oferowanych przez producenta serwera) Możliwość pobrania darmowego oprogramowania zarządzającego i diagnostycznego, wyprodukowanego przez producenta serwera. Oprogramowanie 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.). Zainstalowana, dedykowana dla potrzeb karty zarządzającej pamięć flash o pojemności minimum 16 GB; Rozwiązanie musi umożliwiać instalację obrazów systemów, własnych narzędzi diagnostycznych w obrębie dostarczonej dedykowanej pamięci (pojemność dostępna dla obrazów własnych – minimum 8,5GB); Możliwość zdalnej naprawy systemu operacyjnego uszkodzonego przez użytkownika, działanie wirusów i szkodliwego oprogramowania; Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN; Możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej (w szczególności bez pendrive, dysków twardych wewn. i zewn., itp.) – możliwość manualnego wykonania aktualizacji jak również możliwość automatyzacji; Rozwiązanie musi umożliwiać konfigurację i uruchomienie automatycznego powiadomienia serwisu o zbliżającej się lub istniejącej usterce serwera (co najmniej dyski twarde, zasilacze, pamięć RAM, procesory, wentylatory, kontrolery RAID, karty rozszerzeń); Możliwość zapisu i przechowywania informacji i logów o pełnym stanie maszyny, w tym usterki i sytuacje krytyczne w obrębie wbudowanej pamięci karty zarządzającej - dostęp do tych informacji musi być niezależny od stanu włączenia serwera oraz stanu sprzętowego w tym np. usterki elementów poza kartą zarządzającą;

		Karta zarządzająca musi umożliwiać konfigurację i uruchomienie automatycznego informowania autoryzowanego serwisu producenta serwera o zaistniałej lub zbliżającej się usterce (wymagana jest możliwość automatycznego otworzenia zgłoszenia serwisowego bezpośrednio w systemie producenta serwera, nie dopuszcza się komunikacji SNMP czy email). Jeżeli są wymagane jakiekolwiek dodatkowe licencje lub pakiety serwisowe potrzebne do uruchomienia automatycznego powiadamiania autoryzowanego serwisu o usterce należy takie elementy wliczyć do oferty – czas trwania minimum równy dla wymaganego okresu gwarancji producenta serwera;
13	Wspierane OS	- Windows Server 2019, Windows Server 2016, VMware 6.7 U3, 7.0 U1, 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); -Uszkodzone dyski pozostają u Zamawiającego; -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 Unii Europejskiej - 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; -Wymagane jest oświadczenie Producenta oferowanego serwera, iż wymagany w postepowaniu poziom gwarancji i wsparcia na sprzęt i oferowane wraz z nim oprogramowanie został zaaferowany przez Producenta serwera na potrzeby oferty w niniejszym postępowaniu;

		-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera; -Wszystkie parametry i funkcje oferowanego serwera muszą być wspierane przez producenta i zaimplementowane fabrycznie oraz dostępne w seryjnej produkcji danego modelu urządzenia. Zamawiający nie dopuszcza dostosowywania funkcji na potrzeby niniejszego postępowania. -Wszystkie parametry i funkcje oferowanego serwera muszą być potwierdzone w ogólnodostępnej dokumentacji producenta.

Macierz dyskowa – sztuk 1 – wymagania minimalne		
Lp.	**Nazwa podzespołu**	**Minimalne wymagane parametry**
1.	Obudowa	1) Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych HDD i/lub dysków SSD kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych, kontrolujących wszystkie zasoby dyskowe macierzy z poziomu pojedynczej konsoli WebGUI/CLI administratora; 2) Macierz musi posiadać architekturę modułową w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez kontrolery i dyski dla zapisów danych Użytkownika; 3) System musi być dostarczony ze wszystkimi komponentami do instalacji w standardowej szafie rack 19” z zajętością maks. 2U w tej szafie; 4) Każdy skonfigurowany moduł/obudowa musi posiadać układ nadmiarowy zasilania i chłodzenia, zapewniający bezprzerwową pracę macierzy bez ograniczeń czasowych w przypadku utraty redundancji w danym układzie (zasilania lub chłodzenia); 5)Każdy moduł/obudowa macierzy powinna posiadać widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii; 6) Rozbudowa o dodatkowe moduły dla obsługiwanych dysków powinna odbywać się wyłącznie poprzez zakup takich modułów, bez konieczności zakupu dodatkowych licencji lub specjalnego oprogramowania aktywującego proces rozbudowy; 7) Moduły dla dalszej rozbudowy o dodatkowe dyski i przestrzeń dyskową muszą zapewniać gęstości upakowania co najmniej 24 dysków 2,5” lub co najmniej 12 dysków 3,5” na każde 2U przestrzeni instalacyjnej w szafie przemysłowej rack standardu 19”; 8) Dostarczona konfiguracja macierzy musi pozwalać na połączenie kaskadowe lub w układzie pętli pomiędzy modułami rozwiązania (moduł kontrolerów, moduły/półki dyskowe), z wykorzystaniem minimum 2-torów kablowych w tych połączeniach – okablowanie to musi być zgodne ze standardem SAS 12Gb/s. W przypadku braku obsługi połączeń w układzie pętli dopuszcza się jako alternatywne rozwiązanie macierz z zainstalowanymi 4 kontrolerami RAID;

2.	Pojemność	1) Oferowana macierz musi obsługiwać min. 12 dysków wykonanych w technologii hot-plug – jeżeli dla obsługi tej funkcjonalności konieczny jest zakup dodatkowych licencji to należy ją dostarczyć wraz z macierzą; SSD SAS 960GB 2.5 x4 sztuki, SAS 1.2TB 10krpm 2.5inch x 8sztuk 2) Model oferowanej macierzy musi obsługiwać przestrzeń dyskową w trybie tzw. surowym (RAW) minimum 100TB, bez konieczności wymiany zainstalowanych kontrolerów – wymagana zgodność z zapisami aktualnej na moment składania oferty specyfikacji technicznej macierzy, udostępnionej publicznie na stronie internetowej producenta lub jego przedstawiciela w Polsce; 3) Model oferowanej macierzy musi umożliwiać rozbudowę do wyższego modelu z tej samej rodziny urządzeń w trybie w „data-in-place" tj. z wykorzystaniem wszystkich modułów półek rozszerzeń dyskowych wykorzystywanych przed rozbudową i z dostępem do wcześniej zapisanych danych; 4) Wszystkie zainstalowane dyski hot-plug, z wyłączeniem dysków SSD stosowanych jako rozszerzenie pamięci Cache kontrolerów, muszą być dostępne dla zapisu danych Użytkownika;
3.	Kontrolery	1) Kontrolery macierzy muszą obsługiwać tryb pracy w układzie active-active lub mesh-active, macierz musi być dostarczona z zainstalowanymi minimum 2 kontrolerami; 2) Każdy z kontrolerów macierzy musi posiadać po minimum 16 GB pamięci podręcznej Cache – kontrolery muszą obsługiwać między sobą mechanizm lustrzanej kopii danych (cache mirror) przeznaczonych do zapisu; 3) Macierz musi obsługiwać rozbudowę pamięci podręcznej cache dla operacji odczytu o minimum 1,6 TB poprzez instalację dodatkowych modułów pamięci w kontrolerach lub wykorzystanie dysków SSD. Obecnie nie jest wymagana rozbudowa pamięci cache przeznaczonej do odczytu; 4) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik; 5) Kontrolery muszą posiadać możliwość ich wymiany (w przypadku awarii lub planowych zadań utrzymaniowych) bez konieczności wyłączania zasilania całego urządzenia – wymaganie w przypadku konfiguracji z min. 2 kontrolerami; 6) Macierz musi obsługiwać wymianę kontrolera RAID bez utraty danych zapisanych na dyskach; 7) Każdy z kontrolerów RAID powinien posiadać dedykowane minimum 2 interfejsy RJ-45 Ethernet obsługujące połączenia z prędkością minimum 1Gb/s - dla zdalnej komunikacji z oprogramowaniem zarządzającym i konfiguracyjnym macierzy; 8) Kontrolery macierzy muszą być oparte o procesor wykonany w technologii wielordzeniowej; 9) Każdy kontroler macierzy musi pozwalać na konfigurację interfejsów niezbędnych dla współpracy w sieci IP/FC/SAS SAN oraz NAS; 10) Dla obsługi operacji blokowych I/O w sieci IP/FC/SAS SAN, kontrolery macierzy muszą wspierać protokoły transmisji (komunikacja z serwerami): FC 32/16Gb/s , iSCSI 10/1Gb/s, SAS 12Gb/s; 11) Dla obsługi operacji plikowych I/O w sieci NAS kontrolery macierzy muszą wspierać minimum protokoły dostępu: CIFS, NFS. Obecnie nie jest wymagana obsługa protokołów CIFS, NFS, ale musi

		istnieć możliwość rozbudowy o tą funkcjonalność. Rozbudowa o tę funkcjonalność nie może wymagać montażu żadnych zewnętrznych elementów/modułów po za obudową macierzy. W przypadku rozbudowy macierzy o dostęp plikowy dopuszcza się wymianę części z obecnie wymaganych portów; 12) Uruchomienie obsługi protokołów CIFS i NFS nie może powodować zmniejszenia rozmiaru pamięci podręcznej cache wykorzystywanej przez macierz do obsługi protokołów blokowych – jako równoważność dla tego wymagania dopuszczone jest skonfigurowanie dodatkowo minimum po 16GB pamięci podręcznej Cache dla każdego kontrolera lub 2 grup dyskowych RAID 1 z dyskami SAS SSD minimum 200GB – nie jest wymagane dostarczenie tej funkcjonalności w postepowaniu, możliwość rozbudowy w przyszłości; 13) Kontrolery macierzy muszą obsługiwać do 72 grup dyskowych w całym rozwiązaniu, bez konieczności wymiany dostarczonych kontrolerów;
4.	Interfejsy	1) Każdy kontroler macierzy musi mieć minimum 4 porty SAS 12Gb/s przeznaczone do dołączenia serwerów. Wraz z macierzą należy dostarczyć 4 kable MiniSASHD(8644-8644) o dł. min. 1,1 m każdy; 2) Macierz musi umożliwiać wymianę portów do transmisji danych(z serwerami) na porty obsługujące protokoły: FC 32 Gb/s, FC 16 Gb/s, iSCSI 10Gb/s, iSCSI 1Gb/s; 3) Wymiana portów jw. nie może powodować wymiany samych kontrolerów RAID w oferowanym rozwiązaniu, a w przypadku konieczność licencjonowania tej funkcjonalności macierz ma być dostarczona z aktywną licencją na instalację i obsługę każdego z wymienionych protokołów transmisji danych;
5.	Poziomy RAID	1) Macierz musi zapewniać poziom zabezpieczenia danych na dyskach, definiowany poziomami RAID: 0, 1, 10, 5 , 50, 6;
6.	Wspierane dyski	1) Wszystkie dyski wspierane przez oferowany model macierzy muszą być wykonane w technologii hot-plug i posiadać podwójne porty SAS obsługujące tryb pracy full-duplex; 2) Oferowana macierz musi wspierać dyski hot-plug: - dyski elektroniczne SSD i mechaniczne HDD iż interfejsami SAS12Gb/s; - dyski mechaniczne HDD o prędkości obrotowej 7,2 krpm, 10 krpm oraz 15k rpm; 3) Macierz musi obsługiwać mieszaną konfigurację dysków hot-plug SSD i HDD zainstalowanych w pojedynczej obudowie o wysokości 2U; 4) Model macierzy musi pozwalać na instalację dysków hot-plug w formacie 2,5” i 3,5”; 5) Macierz musi obsługiwać min. 72 dyski SAS SSD w całym rozwiązaniu; 6) Wymagane jest dostarczenie macierzy zawierającej min. 18 dysków HDD-SAS o pojemności min. 1,8 TB każdy, o prędkości obrotowej 10000 obr/min; 7) Macierz musi umożliwiać skonfigurowanie każdego zainstalowanego dysku hot-plug jako dysk hot-spare (dysk zapasowy) w trybach: - hot-spare dedykowany dla zabezpieczenia tylko wybranej grupy dyskowej RAID - hot-spare dla zabezpieczenia dowolnej grupy dyskowej RAID; 8) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku

		na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk (tzw. CopyBackLess); 9) Dostarczona macierz w oferowanej konfiguracji umożliwia szyfrowanie danych na zainstalowanych dyskach dowolnego typu – funkcjonalność realizowana bezpośrednio przez kontrolery macierzy dla danych blokowych – minimum AES 256. Jeżeli funkcjonalność ta wymaga dodatkowych elementów sprzętowych bądź aktywacji dodatkowej licencji to należy dostarczyć je wraz z rozwiązaniem dla maksymalnej pojemności macierzy.
7.	Opcje software'owe	1) Macierz musi być wyposażona w system kopii migawkowych umożliwiających wykonanie minimum 1024 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanej macierzy; 2) Macierz musi umożliwiać zdefiniowanie min. 4096 woluminów (LUN); 3) Macierz musi umożliwiać aktualizację oprogramowania wewnętrznego kontrolerów RAID i dysków bez konieczności wyłączania macierzy; 4) Macierz musi umożliwiać dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacje: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, migrowanie woluminu na inną grupę dyskową; 5) Macierz musi posiadać wsparcie dla systemów operacyjnych : MS Windows Server 2012R2/2016/2019, SuSE Linux, Oracle Linux, Oracle VM, RedHat Linux, AIX, Solaris, VMWare , Citrix XEN Server. 6) Macierz musi być dostarczona z licencją na oprogramowanie wspierające technologię typu multipath (obsługa nadmiarowości dla ścieżek transmisji danych pomiędzy macierzą i serwerem); 7) Macierz musi posiadać możliwość uruchamiania mechanizmów zdalnej replikacji danych, w trybie synchronicznym i asynchronicznym, po protokołach FC oraz iSCSI (w zależności od zastosowanych portów), bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 8) Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy, jako tzw. storage-based data replication; 9) Replikacja danych jak w pkt.7 musi być obsługiwana w połączeniu z każdą macierzą z tej samej rodziny urządzeń wspierającą obsługę zdalnej replikacji danych; 10) Macierz musi posiadać możliwość tworzenia lokalnych tj. w obrębie zasobów macierzy, pełnych kopii danych (tzw. klony danych), kopii przyrostowych oraz kopii lustrzanych (mirror) – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 11) W przypadku obsługi protokołów CIFS i NFS wymagana jest funkcjonalność agregacji przepustowości dla interfejsów dedykowanych do obsługi tych protokołów; 12) Macierz musi obsługiwać dla interfejsów iSCSI i interfejsów obsługujących protokoły CIFS i NFS adresacje IP v.4 i IP v.6; 13) W przypadku korzystania z protokołów dostępu plikowego obsługa CIFS i NFS musi odbywać się jednocześnie;

		14) Macierz musi obsługiwać mechanizmy Thin Provisioning, czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w macierzy; 15) Model oferowanej macierzy musi wspierać rozwiązania klasy 'klastra macierzowego' tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform software'owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych pomiędzy minimum 2 macierzami ; 16) Mechanizm klastra macierzowego musi być obsługiwany dla protokołów FC oraz iSCSI (w zależności od zastosowanych portów), zarówno w zakresie replikacji danych jak i w zakresie sposobu podłączenia serwerów do zasobów macierzy – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 17) Pod użytym w pkt. 15 pojęciem 'wysoka dostępność zasobów dyskowych' należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/ system operacyjny/ serwer) podłączonego do macierzy (macierz podstawowa) w przypadku wystąpienia awarii logicznego połączenia z tą macierzy bądź awarii samej macierzą, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej; 18) Dla uruchomienia funkcjonalności 'klastra macierzowego' musi być możliwość wykorzystania istniejącej infrastruktury FC/IP SAN Użytkownika w zakresie przełączników FC/Ethernet i kart HBA FC/Ethernet zainstalowanych w serwerach Użytkownika; 19) Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie 'klastra macierzowego', musi wspierać poziomy RAID1, RAID10, RAID5, RAID6 bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną; 20) Funkcjonalność 'klastra macierzowego' musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover); 21) Funkcjonalność 'klastra macierzowego' musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover); 22) Funkcjonalność 'klastra macierzowego' musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback); 23) Macierz musi obsługiwać mechanizmy typu AST (Automated Storage Tiering) tj. automatycznego migrowania i realokacji bloków danych pomiędzy różnymi technologiami dyskowymi na podstawie analizy częstotliwości operacji I/O dla tych bloków oraz wg potrzeb wydajnościowych serwerów, środowisk i aplikacji korzystających z zasobów macierzy – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 24) Mechanizm AST musi być obsługiwany przy korzystaniu zarówno z trzech jak z dwóch dostarczonych technologii dyskowych: SSD, SAS, NLSAS; 25) Macierz musi pozwalać na definiowanie minimum 32 różnych polityk i zasad migrowania danych w obrębie tej samej macierzy;

		26) Maksymalna wielkość pojedynczego bloku danych podczas migracji i realokacji mechanizmami AST nie może przekraczać 256MB; 27) Mechanizm AST musi być wyposażony w funkcję Quality-of-Services pozwalająca na zagwarantowaniu wydajności dla wybranych zasobów macierzy (woluminów) mierzonej jako maksymalny czas opóźnień operacji I/O wykonywanych przez serwer/środowisko/aplikację – Licencja na wymienioną funkcjonalność nie jest przedmiotem niniejszego postępowania. Musi istnieć możliwość rozbudowy macierzy o wymienioną funkcjonalność. 28) Mechanizm AST musi pozwalać na definiowanie okna czasowego dla zbierania pomiarów wydajności operacji I/O oraz okna czasowego dla migrowania danych wg ustalonych zasad i polityk – minimalny definiowany czas trwania w/w operacji (długość okna czasowego) nie może być dłuższy niż 4 godziny; 29) Mechanizm AST musi pozwalać na wykluczanie wybranych godzin i dni z pomiarów wydajności operacji I/O; 30) Macierz musi obsługiwać mechanizmy migracji danych w trybie online z innej macierzy tej klasy, z zachowaniem obsługi operacji I/O dla serwerów podłączonych do migrowanej macierzy tj. do migrowanych zasobów LUN;
8.	Konfiguracja, zarządzanie	1) Oprogramowanie do zarządzania musi być zintegrowane z systemem operacyjnym systemu pamięci masowej zarówno przy obsłudze transmisji danych protokołami blokowymi (FC, iSCSI, SAS) jak i do obsługi transmisji protokołami CIFS/NFS; 2) Oprogramowanie zarządzające musi być dostarczone w wariancie dla maksymalnej obsługiwanej pojemności dyskowej macierzy oraz dla maksymalnej liczby dysków wspieranej przez oferowaną macierz; 3) Komunikacja z wbudowanym oprogramowaniem zarządzającym macierzą musi być możliwa w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. 4) Musi być możliwe zdalne zarządzanie macierzą z wykorzystaniem standardowej przeglądarki internetowej (np. Internet Explorer, Google Chrome, Mozilla Firefox) bez konieczności instalacji żadnych dodatkowych aplikacji na stacji administratora; 5) Wbudowane oprogramowanie macierzy musi obsługiwać połączenia z modułem zarządzania macierzy poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI ;
9.	Gwarancja i serwis	1) Macierz dyskowa musi zostać objęta minimum 3 letnim okresem gwarancji producenta w trybie onsite, z czasem reakcji w miejscu instalacji macierzy, najpóźniej w następnym dniu roboczym od zgłoszenia usterki. Producent macierzy musi umożliwiać skuteczne zgłaszanie usterek w trybie całodobowym, 7 dni w tygodniu, również w dni świąteczne; 2) Macierz musi być zaoferowana z serwisem producenta macierzy, który w przypadku wymiany dysków twardych HDD/SSD, umożliwia pozostawienie wszystkich uszkodzonych nośników u Zamawiającego; 3) Serwis gwarancyjny musi obejmować dostęp do poprawek i nowych wersji oprogramowania wbudowanego, które są elementem zamówienia, w ciągu 60 miesięcy od daty zakupu; 4) Po zakończeniu okresu gwarancji musi być zapewniony przez producenta rozwiązania bezpłatny dostęp do aktualizacji oprogramowania wewnętrznego oferowanej macierzy; 5) Macierz musi umożliwiać konfigurację i uruchomienie dedykowanej funkcji automatycznego powiadomienia serwisu o usterce przez samo urządzenie (poprzez dedykowany system

			wbudowany w macierz - bez pośrednictwa administratora, nie dopuszcza się użycia ogólnodostępnych mechanizmów - poczty email w tym m.in. protokołu SNMP i SMTP, nie dopuszcza się SMS – Zamawiający nie dopuszcza możliwości komunikacji z/do macierzy poprzez pocztę email/SNMP/SMTP itp. z powodów bezpieczeństwa). Funkcjonalność musi pozwalać na automatyczne otwarcie zgłoszenia serwisowego w bazie serwisowej producenta macierzy zgodnie z wymaganym w specyfikacji poziomem SLA; Opcja ta musi być dostępna bezpłatnie w trakcie całego okresu gwarancji producenta macierzy. Oferowana funkcjonalność musi również umożliwiać konfigurację i uruchomienie zdalnego dostępu do macierzy bezpośrednio przez Producenta – musi być do tego wykorzystany dedykowany system serwisowy macierzy. 6) Macierz musi pochodzić z legalnego kanału sprzedaży producenta w Polsce i musi reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się użycia macierzy odnawianych, demonstracyjnych lub powystawowych; 7) Urządzenie musi być wykonane zgodnie z europejskimi dyrektywami RoHS i WEEE stanowiącymi o unikaniu i ograniczaniu stosowania substancji szkodliwych dla zdrowia; 8) Producent oferowanej macierzy musi posiadać dedykowaną, ogólnie dostępną stronę internetową, gdzie po wpisaniu numeru seryjnego macierzy można zweryfikować co najmniej: czas i poziom oferowanego serwisu gwarancyjnego producenta zarówno dla macierzy jak i dowolnej z półek dyskowych, datę zakończenia wsparcia gwarancyjnego, datę zakończenia wsparcia producenta dla oferowanego urządzenia – w formularzu ofertowym należy podać pełen adres internetowy strony producenta macierzy, gdzie można zweryfikować wymagane informacje;

Firewall– sztuk 1 - wymagania minimalne
Wymagania ogólne Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. System musi wspierać IPv4 oraz IPv6 w zakresie: • Firewall. • Ochrony w warstwie aplikacji. • Protokołów routingu dynamicznego. . **Redundancja, monitoring i wykrywanie awarii** 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. W ramach postępowania system musi zostać dostarczony w postaci redundantnej.

3. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
4. Monitoring stanu realizowanych połączeń VPN.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:

- 5 portami interfejsami miedzianymi Gigabit Ethernet RJ-45 (10/100/1000 Base-TX).

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Firewall'a: nie mniej niż 20 Mbps
3. Wydajność szyfrowania 3DES: nie mniej niż 20 Mbps
4. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B.
5. Wydajność systemu Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 900 Mbps.
6. Wydajność szyfrowania IPSec VPN nie mniej niż 4 Gbps.
7. 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 Gbps.
8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps.
9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 300 Mbps.

Funkcje Systemu Bezpieczeństwa:

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

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

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu.
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.

- Amazon Web Services (AWS).
- Microsoft Azure
- Google Cloud Platform (GCP).
- OpenStack.
- VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
- Obsługa protokołu Diffie-Hellman grup 19 i 20.
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
- Mechanizm „Split tunneling" dla połączeń Client-to-Site.

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
- Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego.
- Policy Based Routingu.
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

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

Ochrona przed malware

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

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

Ochrona przed atakami

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

Kontrola aplikacji

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

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.

- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. 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 powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

- ICSA lub EAL4 dla funkcji Firewall.

Serwisy i licencje

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

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

Gwarancja oraz wsparcie

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

Opisy do wymagań ogólnych

1. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca 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 (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) 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. Opis przedmiotu zamówienia (nie techniczny, tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Przełącznik (switch) zarządzalny: – ilość 1 sztuka - wymagania minimalne

Typ przełącznika	Zarządzany
Przełącznik wielowarstwowy	L2/L3
Obsługa jakość serwisu (QoS)	Tak
Zarządzanie przez stronę www	Tak
Zarządzany w chmurze	Tak
Inspekcja ARP	Tak
Konfigurowanie ustawień lokalizacji (CLI)	Tak
Obsługa MIB	Tak
Łączność	
Podstawowe przełączanie RJ-45 Liczba portów Ethernet	24
Podstawowe przełączania Ethernet RJ-45 porty typ	Gigabit Ethernet (10/100/1000)
Liczba zainstalowanych modułów SFP	4
Liczba portów USB 2.0	1
Sieć komputerowa	
Standardy komunikacyjne	IEEE 802.1D, IEEE 802.1w, IEEE 802.1s, IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3ad
Obsługa 10G	Tak
Dublowanie portów	Tak
Podpora kontroli przepływu	Tak
Agregator połączenia	Tak
Kontrola wzrostu natężenia ruchu	Tak
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
Automatyczne MDI/MDI-X	Tak
Protokół drzewa rozpinającego	Tak
Blokowanie head-of-line (HOL)	Tak
Obsługa sieci VLAN	Tak
Liczba VLANs	4094

Serwer NAS do tworzenia kopi – 1 szt **wymagania minimalne**

Procesor	Model CPU	AMD Ryzen R1600
	Liczba procesorów	1
	Architektura procesora	64-bit
	Częstotliwość procesora	2-core 2.6 (podstawowy) / 3.1 (turbo) GHz
	Mechanizm szyfrowania sprzętowego (AES-NI)	
Pamięć	Pamięć systemowa	4 GB DDR4 ECC
	Fabrycznie zainstalowany moduł pamięci	4 GB (4 GB x 1)
	Całkowita liczba gniazd pamięci	2
	Maksymalna pojemność pamięci	32 GB (16 GB x 2)

Przechowywanie Kieszeń/kieszenie na dyski 4
Liczba zaistalowanych Dysków 4 sztuki
Minimalna pojemność każdej sztuki 4TB 3,5', 5400RPM, 256MB
Przeznaczenie HDD NAS/Serwer
Kieszenie dysków M.2 2 (NVMe)
3.5" SATA HDD
2.5" SATA SSD
M.2 2280 NVMe SSD

Porty zewnętrzne Port LAN RJ-45 1GbE* 2 (z obsługą funkcji Link Aggregation / przełączania awaryjnego)
Port USB 3.2 1. generacji* 2
Port eSATA 1
Uwagi
Porty sieci LAN 1GbE tego urządzenia mają maksymalny rozmiar jednostki transmitującej (MTU) 1 500 bajtów.
Nazwa standardu USB 3.0 została zmieniona na USB 3.2 1. generacji przez USB Implementers Forum (USB-IF) w 2019 roku.

PCIe Rozszerzenie karty PCIe 1 x Gen3 x2 network upgrade slot
System plików Wewnętrzne dyski twarde

Btrfs
EXT4
Zewnętrzne dyski twarde
Btrfs
EXT4
EXT3
FAT
NTFS
HFS+
exFAT

Inne Wentylator obudowy 92 mm x 92 mm x 2 pcs
Tryb prędkości wentylatora
Tryb pełnej prędkości
Tryb chłodzenia
Tryb cichy

Kontrolki LED z regulacją jasności
Przywracanie zasilania
Natężenie dźwięku* 22.9 dB(A)
Zaplanowane włączanie/wyłączanie
Funkcja Wake on LAN / WAN
Zasilacz / Adapter 100 W
Napięcie wejściowe zasilania prądem zmiennym 100V to 240V AC
Częstotliwość zasilania 50/60 Hz, Jednofazowy
Zużycie energii 35.51 W (dostęp)
11.52 W (hibernacja dysków twardych)
British thermal unit 121.09 BTU/hr (dostęp)
39.28 BTU/hr (hibernacja dysków twardych)
Uwagi
Temperatura Temperatura pracy 0°C do 40°C (32°F do 104°F)
Temperatura przechowywania -20°C do 60°C (-5°F do 140°F)
Wilgotność względna 5% do 95% RH
Certyfikaty

FCC
CE
BSMI
VCCI
RCM
UKCA
EAC
CCC
KC

Gwarancja 3-letnia gwarancja na sprzęt, z możliwością rozszerzenia do 5 lat dzięki EW201 lub Przedłużonej Gwarancji Plus

Środowisko Zgodność z dyrektywą RoHS

Zawartość opakowania
Jednostka główna X 1
Pakiet akcesoriów X 1
Zasilacz X 1
Kabel zasilania X 1
Kabel LAN RJ-45 X 2
Przewodnik szybkiej instalacji X 1

UPS serwerowy – 1szt **wymagania minimalne**

- Moc: **2500VA / 2000W**
- Napięcie: **230V AC**
- Gniazda wyjściowe: **2x gniazdo 230V z uziemieniem typu schuko lub listwa zaciskowa**
- Zabezpieczenie wyjścia: **Bezpiecznik C20**
- Częstotliwość: **50Hz**
- Typ transformatora: **Toroidalny**
- Stabilizacja napięcia: **TAK**
- Przebieg napięcia: **Czysta sinusoida**
- Zniekształcenie fali: **≤3%**
- Obsługiwane typy akumulatorów: **24V - AGM VRLA i GEL**
- Napięcie ładowania: **27,2V**
- Maksymalny prąd ładowania: **24A**
- Zabezpieczenie akumulatora: **na poziomie 20,5V**
- Czas przełączania: **<10 ms**
- Czas pracy UPS: **Zależny od zastosowanej instalacji akumulatorowej minimum 50 minut przy maksymalnym obciążeniu**
- Sygnalizacja dźwiękowa: **TAK**

W zestawie z zasilaczem UPS 2 sztuki akumulatorów AGM lub GEL 100Ah 12 V wraz z przewodami 2x16mm^2 + Balanser do akumulatorów Akumulatora PROTECT 24V