Załącznik nr.6 do SWZ

Fundusze Europejskie na Rozwój Cyfrowy

Opis przedmiotu zamówienia

Część 1 zamówienia

1. Serwer produkcyjny - dostawa , instalacja i konfiguracja – 2 kpl

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	• Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Obudowa wyposażona w panel LCD wbudowany na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze. • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	• Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. • Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset	• Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	• Dwa procesory 8-rdzeniowe, min. 2.9GHz, umożliwiające osiągnięcie wyniku min. 176 w teście SPECrate2017_int_base, dla oferowanego serwera, dostępnym na stronie www.spec.org w konfiguracji dwuprocesorowej
RAM	• Minimum 64GB DDR5 RDIMM 4800MT/s,
Funkcjonalność	• Demand Scrubing, • Patrol Scrubing,

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego : Cyberbezpieczny Samorząd , Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).

pamięci RAM	• Permanent Fault Detection
Gniazda PCI	• minimum trzy sloty PCIe
Interfejsy sieciowe/FC/SAS	• Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe)
Dyski twarde	• Zainstalowane dwa dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug skonfigurowane w RAID 1.
Kontroler SAS	○ Zainstalowany sprzętowy kontroler SAS do podłączenia macierzy dyskowej
Wbudowane porty	• 4 x USB z czego nie mniej niż 1x USB 3.0, • 2x VGA
Video	• Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	• Redundantne, Hot-Plug min. 1100W klasy Titanium.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. • Możliwość wyłączenia w BIOS funkcji przycisku zasilania. • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. • Moduł TPM 2.0 • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem
System operacyjny	• Windows Server 2022 Standard + 15 device CAL
Karta Zarządzania	• Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: ○ zdalny dostęp do graficznego interfejsu Web karty zarządzającej; ○ zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); ○ szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; ○ możliwość podmontowania zdalnych wirtualnych napędów; ○ wirtualną konsolę z dostępem do myszy, klawiatury; ○ wsparcie dla IPv6; ○ wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; ○ możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; ○ możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; ○ integracja z Active Directory; ○ możliwość obsługi przez dwóch administratorów jednocześnie; ○ wsparcie dla dynamic DNS; ○ wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. ○ możliwość bezpośredniego zarządzania poprzez dedykowany port USB na

	przednim panelu serwera ○ możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: ○ Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej ○ Przesyłanie danych telemetrycznych w czasie rzeczywistym ○ Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze ○ Automatyczna rejestracja certyfikatów (ACE)
Oprogramowanie do zarządzania	• Możliwość zainstalowania oprogramowania producenta do zarządzania, spełniającego poniższe wymagania: ○ Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych ○ integracja z Active Directory ○ Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta ○ Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish ○ Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram ○ Szczegółowy opis wykrytych systemów oraz ich komponentów ○ Możliwość eksportu raportu do CSV, HTML, XLS, PDF ○ Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu. ○ Grupowanie urządzeń w oparciu o kryteria użytkownika ○ Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji ○ Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach ○ Szybki podgląd stanu środowiska ○ Podsumowanie stanu dla każdego urządzenia ○ Szczegółowy status urządzenia/elementu/komponentu ○ Generowanie alertów przy zmianie stanu urządzenia. ○ Filtry raportów umożliwiające podgląd najważniejszych zdarzeń ○ Integracja z service desk producenta dostarczonej platformy sprzętowej ○ Możliwość przejęcia zdalnego pulpitu ○ Możliwość podmontowania wirtualnego napędu ○ Kreator umożliwiający dostosowanie akcji dla wybranych alertów ○ Możliwość importu plików MIB ○ Przesyłanie alertów „as-is” do innych konsol firm trzecich ○ Możliwość definiowania ról administratorów ○ Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów ○ Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania) ○ Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta ○ Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów ○ Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. ○ Wbudowany w serwer mechanizm pozwalający na weryfikację niezmienności

	konfiguracji sprzętowej serwera od momentu produkcji do dostawy do docelowej lokalizacji. Mechanizm ma również pozwalać na kontrolę otwarcia urządzenia w trakcie transportu, niezależnie od stanu zasilania wymagane dołączenie do oferty potwierdzenia przez producenta ○ Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności. ○ Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile ○ Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. ○ Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. ○ Zdalne uruchamianie diagnostyki serwera. ○ Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym. ○ Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	• Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001:2018 oraz ISO-14001:2015 • Serwer musi posiadać deklaracja CE. • Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Silver według normy wprowadzonej w 2019 roku dla Polski lub kraju członkowskiego UE- **Wykonawca złoży dokument potwierdzający spełnianie wymogu.** • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika	• Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji	• Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres co najmniej 36 miesięcy. • Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. • Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy (dla krytycznych zgłoszeń serwisowych) • Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania.

	• Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. • Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. • Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. • Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii, automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych, wskazówki dotyczące bezpieczeństwa produktów, samodzielne wysyłanie części, a także ocena bezpieczeństwa cybernetycznego • Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. • Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. • Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

2. Serwer do backupu - dostawa , konfiguracja i wdrożenie – 1 kpl

L.p.	**Charakterystyka (wymagania minimalne)**
1.	Przedmiotem zapytania jest kompletne rozwiązanie backupowe dostarczone w postaci gotowego do pracy appliance'u (HW+SW) łączącego funkcje: - serwera backupu realizującego backup poprzez wykorzystanie deduplikacji na źródle - medium backupowego dedykowanego do przechowywania zabezpieczanych danych, gwarantującego globalną deduplikację danych - systemu umożliwiającego indeksowanie oraz pełnotekstowe przeszukiwanie danych backupowych - systemu raportującego Appliance będący przedmiotem zapytania musi być gotowym produktem pochodzącym od jednego producenta, musi być oznaczony nazwą i typem dostępnym w katalogu produktów

	określonego producenta, oferowanym na moment ukazania się niniejszego zapytania.
2.	Dostarczone rozwiązanie musi być gotowe do pracy, co oznacza: - wyeliminowanie konieczności instalacji serwera backupowego - wyeliminowanie konieczności instalacji media serwerów - dostarczona platforma musi być optymalna pod kątem pracy ciągłej co oznacza wyeliminowanie konieczności strojenia, weryfikacji/zmian konfiguracji oraz przeprowadzania testów strojonej platformy
3.	Całość rozwiązania musi pochodzić od jednego producenta, musi być zaoferowane z 36 miesięczną gwarancją oraz wsparciem realizowanym przez producenta tego rozwiązania działającym w trybie zgłoszeń 24x7 oraz reakcją NBD. Producent musi być odpowiedzialny za poprawność pracy całości rozwiązania czyli części SW oraz HW, co w szczególności oznacza: - tworzenie/dostarczanie poprawek oprogramowania oraz nowych wersji SW - dedykowanie odpowiednich wersji oprogramowania systemowego rekomendowanego dla eksploatowanej części SW - gwarancję optymalnej pracy całości dostarczonego rozwiązania (niedopuszczalny jest scenariusz w przypadku którego wewnętrzna przyczyna problemu powodującego nieprawidłowe zachowanie dostarczonego rozwiązania, określana jest jako zależna od pracy elementu w przypadku którego producent rozwiązania nie ponosi odpowiedzialności)
4.	Dostarczone urządzenie musi dysponować przestrzenią netto nie mniejszą niż 12TB przeznaczoną na gromadzenie deduplikatów, wymaga się aby urządzenie zajmowało maksymalnie 2U w szafie RACK.
5.	Dostarczone urządzenie musi umożliwiać dodatkową rozbudowę o warstwę typu CLOUD dedykowaną do długotrwałego przechowywania danych (tzw. Long Term Retention) – dane o określonej retencji (zgodnie z założoną polityka retencyjną), bez pośrednictwa dodatkowych urządzeń (typu GATEWAY) muszą zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę (wymagane wsparcie dla dla AWS, Microsoft Azure, Google GCP). Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Skalowanie w przypadku wykorzystywanej przestrzeni warstwy typu Cloud musi wynosić min. 180TB netto.
6.	Zastosowany algorytm deduplikacji musi bazować na bloku o zmiennej długości, dobieranej automatycznie dla kolejnych zapisywanych na urządzeniu danych. W celu osiągnięcia dużej efektywności deduplikacji maksymalna wielkość bloku wykorzystywanego w tym procesie nie może być większa niż 12 kB. Niedopuszczalna jest deduplikacja stałym blokiem o ustalonej tej samej długości, możliwość manulanej zmiany (bądź poprzez oskryptowanie) długości bloku deduplikacji również nie może zastąpić wymogu automatycznego doboru długości bloku na jaki dzielony jest każdy strumień danych. Oferowane urządzenie musi deduplikować dane in-line przed zapisem na nośnik dyskowy, na wewnętrznych dyskach urządzenia nie mogą być zapisywane dane w oryginalnej postaci (niezdeduplikowanej) z jakiegokolwiek fragmentu strumienia danych przychodzącego do

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego : Cyberbezpieczny Samorząd , Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).

	urządzenia.
7.	Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo skompresowane, wymaga się zastosowania HW układu dedykowanego wyłącznie do realizacji kompresji, umożliwiającego redukcję obciążenia CPU procesem kompresji.
8.	Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja muszą zostać usunięte podczas procesu czyszczenia tzw. cleaning.
9.	Część urządzenia dedykowana do przechowywania danych musi posiadać blokadę WORM sterowaną na poziomie wbudowanego oprogramownia backup'owego, wymagana: • możliwość uruchomienia blokady WORM dla określonych danych z poziomu oprogramowania backup'owego • możliwość określenia/wymuszenia okresu blokady z poziomu oprogramowania backup'owego, wymagana możliwość ustawienia innego czasu blokady backupu dla kazdego zadania backup'owego • możliwość raportowania od strony oprogramowania backup'owego danych zabezpieczonych przed usunięciem wymaganą blokadą WORM Blokada WORM musi działać w dwóch trybach: 1. Możliwość zdjęcia blokady przed upływem ważności danych 2. Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie normy SEC 17a-4(f)
10.	Wymaga się aby użycie blokady WORM było możliwe dla wszystkich systemów wspieranych przez oprogramowanie będące częścią oferowanego urządzenia.
11.	Wymagane porty służące do komunikacji z oferowanym urządzeniem: min. 4 x 10Gb/s Eth OP
12.	Skalowanie urządzenia musi zapewnić możliwość zwiększenie pojemności netto przeznaczonej do gromadzenia deduplikatów do min. 95TB netto, przy zachowaniu globalnej deduplikacji oraz zachowaniu zajętości w szafie RACK na poziomie maksymalnie 2U
13.	Osiągana wydajność zapisu danych w przypadku maksymalnej konfiguracji oferowanego urządzenia deklarowana w ogólnie dostępnej dokumentacji nie może być niższa niż 14TB/h.
14.	Możliwość równocześnie (równolegle) wykorzystywanych strumieni w przypadku maksymalnej konfiguracji oferowanego urządzenia nie może być mniejsza niż 18.
15.	Przestrzeń dyskowa dedykowana do gromadzenia deduplikatów powinna być zabezpieczona poprzez wykorzystanie RAID 6 lub rozwiązania równoważnego i odporna na jednoczesną awarię dwóch dysków.
16.	Oferowane rozwiązanie musi być dedykowane do montażu w szafie RACK, zajętość całości oferowanego rozwiązania z uwzględnieniem skalowania do wymaganej pojemości nie może

	zajmować więcej niż 2U.
17.	Oferowane rozwiązanie musi umożliwiać backup/ odtwarzanie: • dowolnej liczby maszyn wirtualnych jako obrazów („image level") • agentowo, dowolnej liczby baz danych, plików, ze środka maszyn wirtualnych • dowolnej liczby danych [TB] w zabezpieczanym środowisku (ograniczeniem w tym wypadku może być jedynie pojemność urządzenia)
18.	Wymaga się aby dla wszystkich rodzajów wspieranych środowisk, oferowane rozwiązanie wykonywało backup z deduplikacją na źródle, bez pośrednictwa jakichkolwiek dodatkowych serwerów.
19.	Backup z dededuplikacją na źródle musi być dostępny dla wszystkich typów danych w ramach oferowanego rozwiązania: pliki, bazy danych, obrazy maszyn wirtualnych, Kubernetes.
20.	Wymagana możliwość szybkiego backupu blokowego wielomilionowych systemów plików na maszynach Windows / Linux. W trakcie backupu wymagana realizacja kopii zapasowych fizycznych bloków a nie plików, jednocześnie wymagana jest możliwość odtworzenia • całego wolumenu • pojedynczego pliku W celu minimalizacji czasu backupu wymagana eliminacja indeksowania plików znajdujących się na zabezpieczanym wolumenie (zaindeksowanie wielu milionów plików powoduje duże wydłużenie czasu backupu).
21.	Wymaga się aby oprogramowanie backupowe zapewniało pełen backup (full backup) blokowy wielomilionowych systemów plików na maszynach Windows / Linux poprzez odczyt tylko zmienionych bloków, odczyt całości zabezpieczanego dysku może być wykonany jedynie podczas pierwszego backupu bądź po restarcie serwera. Wszystkie kolejne backupy mają odczytywać z dysku jedynie zmienione bloki w stosunku do ostatniego backupu (w efekcie na deduplikatorze muszą pojawić się kopie typu full backup). Oprogramowanie backupowe musi odczytywać, jedynie zmienione na dysku bloki (a nie całe pliki).
22.	Ze względów bezpieczeństwa rozwiązanie backupowe musi mieć możliwość wykonania kopii wewnętrznej bazy danych zapewniającej możliwość odtworzenia konfiguracji środowiska.
23.	Oprogramowanie backupowe musi umożliwiać zarządzanie replikacją backupów między urządzeniami oferowanego typu, bezpośrednio z poziomu interfejsu oprogramowania backupowego przy spełnieniu wszystkich poniższych wymagań • replikacji podlegają tylko te bloki które nie znajdują się na docelowym urządzeniu • replikacja między urządzeniami następuje w zdefiniowanych interwałach czasowych • oprogramowanie przechowuje informacje o wszystkich kopiach danych znajdujących się na urządzeniach (czyli kopii oryginalnej oraz zreplikowanej) oprogramowanie pozwala na wybór urządzenia z którego zostanie wykonane odtwarzanie bez konieczności przeprowadzania inwentaryzacji
24.	Oprogramowanie backupowe musi umożliwiać określenie różnych retencji dla danych na podstawowym nośniku i nośniku zawierającym kopię (replika backupu). Określenie czasu retencji przechowywania dla kopii (repliki) musi być możliwe w momencie definiowania zadania

	backupowego.
25.	Wymaga się aby z poziomu konsoli oprogramowania dostępna była możliwość definiowania wymaganej retencji danych (backupów) w oparciu o kryteria czasowe (dni, miesiące, lata). Po przekroczeniu okresu retencji, określone kopie backupowe muszą być automatycznie usunięte.
26.	Dla baz danych MSSQL wymagana możliwość inicjowania backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań: • backup jest wykonywany przez oprogramowanie backupowe • inicjowanie backupu z graficznego interfejsu będącego częścią MSSQL Management Studio • możliwość wyboru backupu pełnego, różnicowego, logów backup inicjowany przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego
27.	Dla baz danych MSSQL wymagana możliwość odtworzenia backupów przez administratora MSSQL przy spełnieniu wszystkich poniższych wymagań: • odtworzenie dowolnego backupu wykonanego przez oferowane rozwiązanie backupowe • zarządzanie odtwarzaniem z graficznego interfejsu będącego częścią MSSQL Management Studio • możliwość odtworzenia do dowolnego punktu w czasie wybranego przez administratora MSSQL w ramach przechowywanych przez oferowane oprogramowanie backupowe logów MSSQL • odtworzenie bazy danych przez administratora MSSQL nie może wymagać kontaktu z administratorem oferowanego rozwiązania backupowego
28.	Dla baz danych MSSQL wymagana możliwość realizowania samobackupującego się środowiska MS-SQL umożliwiającego automatyczny wybór backupowych baz danych w momencie startu backupu. Administrator definiuje reguły – jakie bazy danych mają być backupowane w ramach polityki – oprogramowanie backupowe backupuje wszystkie bazy danych spełniające określone reguły.
29.	Wymaga się aby reguły (o których mowa w poprzednim punkcie), umożliwiające określenie które bazy będą backupowane uwzględniały: • nazwy backupowanych baz danych • nazwy serwerów bazy danych • nazwy klastrów • typy hostów • nazwy aplikacji Reguły muszą pozwalać na wybór nazw: • zaczynających się od określonego tekstu • zawierających określony tekst • NIE zawierających określonego tekstu • kończących się określonym tekstem
30.	Rozwiązanie backupowe musi wspierać backup i odtwarzanie środowisk VMware Oprogramowanie backupowe musi umożliwiać w przypadku środowisk VMware następujące typy backupu: • backup pojedynczych plików i baz danych ze środka maszyny wirtualnej VMware.

	• backup całych maszyn wirtualnych (obrazów, plików vmdk reprezentujących wirtualną maszynę). - realizacja backupu nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk) • backup tylko wybranych dysków maszyny wirtualnej (wybranych plików vmdk systemu vmware) - realizacja backupu nie może wymagać bufora dyskowego na kopię obrazów maszyn wirtualnych (plików vmdk) • wszystkie backupy obrazów maszyn wirtualnych muszą być wykonywane przy pomocy technologii CBT systemu VMware to znaczy do medium backupowego z systemu VMware muszą być transferowane tylko zmienione bloki, z punktu widzenia systemu backupowego muszą to być backupy pełne (full backup). Powyższe metody backupu maszyn wirtualnych muszą podlegać deduplikacji ze zmiennym blokiem przed wysłaniem danych do oferowanego deduplikatora, metody te muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.
31.	Oferowane rozwiązanie backupowe musi umożliwiać odtwarzanie obrazów maszyn wirtualnych VMware przy zachowaniu następujących funkcjonalności: • odtworzenie całych maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu • odtworzenie pojedynczych dysków maszyn wirtualnych musi wykorzystywać mechanizm CBT systemu VMware – odtwarzane są tylko te bloki wirtualnej maszyny/dysku które uległy zmianie od ostatniego backupu • odtworzenie pojedynczych plików z backupu obrazu maszyny wirtualnej bez konieczności odtworzenia całej maszyny wirtualnej. Funkcjonalność musi być dostępna dla obrazów maszyn wirtualnych z zainstalowanym systemem operacyjnym Windows oraz Linux. Powyższe metody odtworzenia muszą być wbudowane w system backupu i w pełni automatyczne bez wykorzystania skryptów/dodatkowych komend.
32.	Skalowalność oferowanego rozwiązania dla środowisk VMware musi pozwalać na: • backup minimum 1000 maszyn wirtualnych w ramach pojedynczej instancji systemu backupu. • równoległy backup dysków w ramach backupu pojedynczej maszyny wirtualnej VMware
33.	Oferowane rozwiązanie backupowe musi umożliwiać jednoczesny backup minimum 18 maszyn wirtualnych.
34.	Wymaga się aby Administrator aplikacji backupowej za pośrednictwem GUI (graficzna konsola) miał dostępne następujące możliwości odtwarzania maszyn VMware: • odtworzenie całej maszyny wirtualnej VMware • odtworzenie pojedynczego dysku uprzednio zbackupwanej całej maszyny wirtualnej • odtworzenie plików / katalogów z backupu obrazu maszyny wirtualnej • uruchomienie maszyny wirtualnej bezpośrednio z backupu dostępnego na oferowanym urządzeniu bez wcześniejszego odtwarzania danych • naprawienie aktualnej instancji maszyny wirtualnej– odtworzenie tylko zmienionych bloków od ostatniego backupu

	Wszystkie w/w możliwości muszą być dostępne w postaci graficznych wizardów.
35.	Oferowane rozwiązanie backupowe musi umożliwiać zdefiniowanie polityk backupowych dostępnych dla administratora systemu VMware z poziomu vCenter. Administrator VMware musi mieć możliwość przyporządkowania nowo tworzonych maszyn wirtualnych do polityk backupowych, przy czym całość informacji dot. backupów środowisk VMware musi być przechowywana na serwerze backupu.
36.	Wymaga się aby maszyna wirtualna VMware zbackupowana poprzez serwer pośredniczący: A, mogła być odtworzona przez dowolny inny system pośredniczący np: B, C, ...
37.	Oferowane oprogramowanie backupowe musi samo dystrybuować zadania backupu/odtwarzania obrazów maszyn wirtualnych VMware między dostępne serwery pośredniczące zapweniając równomierne obciążenie.
38.	Wymaga się aby w przypadku środowisk VMware oferowane rozwiązanie backupowe automatycznie rozpoznawało nowo utworzone maszyny wirtualne oraz przypisywało je do odpowiednich polityk backupowych, wymagana możliwość konfiguracji/realizacji następującego scenariusza: - wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „krytyczna” muszą być backupowana automatycznie co godzinę - wszystkie nowo utworzone maszyny wirtualne zawierające w nazwie frazę „produkcja” muszą być backupowana automatycznie raz na dzień - pozostałe maszyny wirtualne są backupowane raz na tydzień Oferowane rozwiązanie backupowe musi umożliwiać realizację backupów wg. w/w scenariusza, bez jakichkolwiek akcji ze strony administratora backupu/VMware czy też jakiekolwiek innej osoby.
39.	Wymaga się aby w przypadku środowisk VMware oferowane rozwiązanie backupowe pozwalało na: - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych zawierających w nazwie maszyny wirtualnej podany tekst. - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się we wszystkich folderach zawierających w nazwie podany tekst. - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych których TAG zawiera podany tekst. - automatyczne dodanie do odpowiednich polityk backupowych wszystkich maszyn wirtualnych znajdujących się na wszystkich datastore’ach które w nazwie zawierają podany tekst.
40.	Wymaga się aby w środowisku VMware oferowane rozwiązanie backupowe pozwalało na automatyczne usuwanie maszyn wirtualnych z polityk backupowych w tym samym momencie w którym maszyna jest usunięta z vCenter, dotychczas wykonane kopie zapasowe muszą być przechowywane zgodnie z okeśloną wcześniej retencją, umożliwiając odtworzenie tej maszyny.
41.	Wymagany snapshot’owy tryb backup’u środowisk VMware bez pośrednictwa zewnętrznych serwerów proxy (pośredniczących), niezależny od rodzaju użytej macierzy dyskowej, nie

	wymagający zastosowania VMware vSphere Storage APIs - Data Protection (w celu redukcji utylizacji zasobów środowiska w tym CPU, pamięci masowej, pamięci wymaganej do tworzenia kopii zapasowych). Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności).
42.	Wymagane zapewnienie backupu środowisk VMware vSphere przy użyciu vSphere API for I/O (VAIO) Filtering framework (https://core.vmware.com/resource/vmware-vsphere-apis-io-filtering-vaio#section1) Zamawiający zastrzega możliwość prośby o dostarczenie dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności
43.	Oferowane rozwiązanie backupowe musi wspierać backup środowisk Kubernetes
44.	Wymaga się aby podpięcie środowiska Kubernetes do oferowanego rozwiązania backupowego było maksymalnie proste, ograniczało się do podania jedynie nazwy FQDN/IP środowiska i uprawnień.
45.	Wymaga się aby oprogramowanie backupowe automatycznie instalowało wymagane moduły w zabezpieczanym środowisku Kubernetes, wprost z repozytorium sieciowego producenta (np. github) Jeśli sieciowe repozytorium producenta jest niedostępne z poziomu środowiska Kubernetes, wymagana możliwość automatycznego pobierania modułów ze wskazanego repozytorium
46.	Oferowane rozwiązanie musi zapewniać backup dowolnych namespace znajdujących się w środowisku Kubernetes
47.	Wymagana możliwość wykluczenia dowolnych dysków PVC z backupu dowolnego namespace
48.	Wymagana możliwość skonfigurowania samobackupującego się środowiska Kubernetes - w momencie startu backupu następuje automatyczny wybór backupowanych namespace zgodnie z regułami określonymi przez Administratora
49.	Wymagana możliwość tworzenia w/w reguł używanych przy backupie określonych namespace w oparciu o: • nazwy backupowanych namespace • etykiety backupowanych namespace Reguły muszą pozwalać na wybór nazw : • zaczynających się od określonego tekstu • zawierających określony tekstu • NIE zawierających określonego tekstu kończących się określonym tekstem
50.	Wymaga się aby backup realizowany był zgodnie ze zdefiniowana polityką lub inicjowany ad hoc, uruchomiony ręcznie przez administratora
51.	W ramach dostarczonych licencji wymagana możliwość spójnego backupu baz danych i aplikacji Cassandra, MySQL, PostreSQL, MongoDB działających w obrębie zabezpieczanych środowisk

	Kubernetes
52.	Wymagana możliwość realizacji backupów syntetycznych. W przypadku środowisk Kubernetes działających w infrastrukturze VMware: odczyt jedynie zmienionych bloków, finalnie na oferowanym urządzeniu uzyskiwany jest pełen backup (full). Oferowane oprogramowanie musi umożliwiać automatyczną realizację powyższego scenariusza, nie może wymagać dodatkowych działań ze strony administratora backupu.
53.	W przypadku środowisk Kubernetes wymagana możliwość odtworzenia całych namespace lub wybranych dysków PVC
54.	W przypadku środowisk Kubernetes wymagana możliwość odtworzenia danych zarówno na oryginalne środowisko Kubernetes jak również inne środowisko Kubernetes
55.	Wymagana możliwość bezpośredniego odtwarzania danych zarówno przez administratora backupu jak również przez administratora Kubernetes
56.	Wymaga się aby zarządzanie zarówno w przypadku backupu, odtwarzania oraz wszystkich dostępnych funkcjonalności dla środowisk Kubernetes było dostępne za pośrednictwem jednej centralnej konsoli graficznej GUI HTML 5
57.	Wymaga się aby konsola oprogramowania backupowego umożliwiała definiowanie polityk backupowych obejmujących całość cyklu życia kopii zapasowej. W szczególności wymagana możliwość zdefiniowania polityki backupowej która dla dowolnej liczby zabezpieczanych systemów (zadań backupowych) zapewnia: 1. lokalny backup na oferowane urządzenie z 30-o dniową retencją 2. replikację (na poziomie bloków) do drugiego urządzenia oferowanego typu (retencja 60 dni) Całość wymaganych operacji musi być skonfigurowana poprzez pojedynczą politykę backupową stworzoną poprzez GUI oprogramowania backupowego w oparciu o dostępny „wizard”. Wymaga się aby administrator backupu za pośrednictwem konsoli (GUI) oferowanego oprogramowania backupowego mógł odtwarzać dane VMware/Kubernetes z dowolnych w/w kopii (1-2).

3.Macierz - dostawa i konfiguracja - 1 kpl

Element konfiguracji/cecha/ funkcjonalność	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U.
Przestrzeń dyskowa	Zainstalowane:

	2 x 3.84TB SSD SAS ISE, Read Intensive, up to 24Gbps 512e 2.5in Hot-Plug, AG Drive. 10 x 2.4TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drive
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 276 dysków twardych.
Obsługa dysków	Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i NL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID0, RAID1, RAID10, RAID5, RAID6 oraz RAID z tzw. rozproszoną wolną pojemnością, realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Macierz musi również oferować możliwość zdefiniowania grup dyskowych z tzw. rozproszoną wolną pojemnością, która nie wykorzystuje tradycyjnych dysków zapasowych (integracja dysków zapasowych i nieaktywnych do zwiększenia dostępności i wydajności macierzy, zwiększenie szybkości odbudowy macierzy na wypadek awarii dysku). Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków.
Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów.
Pamięć cache	Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
Interfejsy	Macierz musi posiadać, co najmniej 8 portów SAS 12Gb (4 porty na kontroler)
Kable/wkładki	Min. 4 kable 12Gb HD Mini-SAS/HD Mini-SAS min. 2m
Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Macierz musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów

	typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach macierzowych (wymagana obsługa standardu T10 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Tiering	Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. Dyski SSD mogą być wykorzystane zarówno do uzyskania pojemności w warstwie wydajności lub na potrzeby zwiększenia pamięci podręcznej odczytu w celu przyspieszenia operacji losowego odczytu z jednej lub wielu warstw napędów mechanicznych.
Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Migracja danych w obrębie macierzy	Macierz dyskowa musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności

	takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. Zamawiający wymaga dostarczenia wraz z ofertą dokumentu od producenta sprzętu lub też certyfikatu, który potwierdza, że zasilacze użyte w macierzy posiadają sprawności zasilacza minimum 80+ Gold.
Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
Standardy bezpieczeństwa	Urządzenie musi spełniać następujące standardy bezpieczeństwa: EN 62368-1 (European Union), IEC 60950-1 (International)
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Wykonawca musi przedstawić oświadczenie producenta, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.
Warunki gwarancji	Co najmniej 36 miesięcy gwarancji producenta. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia. Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych. Zamawiający wymaga od producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we

	współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

4. UPS -dostawa i konfiguracja – 1szt.

Element konfiguracji/cecha/ funkcjonalność	Wymagania minimalne
Typ obudowy	UPS musi być przystosowana do montażu w szafie rack 19”
Moc urządzenia	Moc pozorna: minimum 3000 VA Moc czynna: minimum 2700 W
Czas podtrzymania (obciążenie 100%)	minimum 6 min
Architektura UPS-a	line-interactive
Przebieg na wyjściu	Sinusoida
Typowy czas pełnego ładowania akumulatora	4 godz.
Liczba faz na wejściu	1 (230V)
Czas przełączenia (maks.)	10 ms
Porty zasilania we.	1 x IEC-C20
Porty zasilania wy.	Minimum 6 x IEC-C13
Złącza	Port szeregowy (RJ-45), Złącze na kartę komunikacyjną (z zainstalowana kartą do monitorowania i zarządzania UPS przez sieć komputerową.) Zainstalowana karta do monitorowania i zarządzania UPS musi mieć możliwość podłączenia czujników monitorowania środowiska.
Funkcjonalność	Funkcja korekcji niskich i wysokich napięć Filtrowanie napięcia Automatyczne włączenie UPS-a po powrocie zasilania Alarmy dźwiękowe Wskaźnik statusu LED Powiadomienie o awarii akumulatora
Gwarancja	minimum 36 miesięcy na urządzenie

	minimum 24 miesiące na akumulatory

5. Przełącznik dostępowy zarządzalny – 2 szt.

Element konfiguracji/cecha / funkcjonalność	Minimalne wymagania
Obudowa	Do montażu w szafie Rack 19”, o wysokości nie więcej niż 1U, wraz z kompletem odpowiednich szyn, wyposażona w zintegrowany zasilacz, możliwość instalacji redundantnego zasilacza Możliwość wyboru modelu przełącznika z kierunkiem przepływu powietrza przód-tył oraz tył-przód
Porty	Minimum 48 portów RJ45 10/100/1000Mb Minimum 4 zintegrowane porty 10Gb Ethernet SFP+ Minimum 1 port USB, 1 port RJ45 jako port konsoli Port typu Ethernet out-of-band-management
Wydajność przełacznika	Minimum 32000 adresów MAC Switch fabric min. 500Gbps Forwarding rate min. 800Mpps Pamięć RAM min. 4GB Bufor pamięci dla pakietów minimum 8MB
Funkcjonalność warstwy II	Obsługa minimum 4000 wirtualnych sieci VLAN Wsparcie dla agregacji LACP (802.3ad) Obsługa 64 grup LACP i 8 portów fizycznych per grupa Zgodność ze standardami wyspecyfikowanymi poniżej: 802.1D Bridging, Spanning Tree 802.1S Multiple Spanning Tree (MSTP) 802.1v Protocol-based VLANs 802.1W Rapid Spanning Tree (RSTP) 802.3ab Gigabit Ethernet (1000BASE-T) 802.3ad Link Aggregation with LACP 802.3ae 10 Gigabit Ethernet (10GBASE-X) 802.3u Fast Ethernet (100BASE-TX) 802.3z Gigabit Ethernet (1000BASE-X)
Funkcjonalnośc warstwy III	Obsługa protokołu routingu dynamicznego RIP1 oraz RIP2, OSPF Obsługa minimum 500 wpisów routingu statycznego Obsługa minimum 1000 wpisów routingu dynamicznego Obsluga mimimum 100 interfejsów warstwy 3 (virtual IP) Zgodność z protokołami: 1058 RIPv1 2453 RIPv2 2328 OSPFv2 3137 OSPF Stub Router Advert
Funkcjonalności z zakresu bezpieczeństwa i zarządzania	Obsługa list kontroli dostępu opartych o adresy MAC i IP Obługa minimum 100 list kontroli dostępu i 2000 reguł sumarycznie dla wszystkich list Obsługa SNMP v1/2/3 Obsługa telnet, SSH, TFTP Serwer
Inne	Przystosowanie do pracy w temperaturze 0-45 stopni Celcjusza
	Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT. Zaproponowane rozwiązanie musi posiadać następujące funkcjonalności: • Monitoring:

	○ ilość podłączonych oraz rozłączonych systemów ○ stan podłączonych urządzeń ○ informacje o potencjalnych zagrożeniach związanych z cyberbezpieczeństwem w oparciu o najlepsze praktyki i szczegółową analizę posiadanych systemów ○ Informacje o alertach z podziałem na minimum: krytyczne, błędy, ostrzeżenia ○ informacje o statusie gwarancji dla poszczególnych urządzeń ○ informacje o stanie licencji na posiadane oprogramowanie rozszerzające funkcjonalności urządzeń ○ informacje w oparciu o dane historyczne umożliwiające określenie trendów krótko- i długoterminowej prognozy wykorzystania przestrzeni na pamięciach masowych. ○ Wykrywanie anomalii w oparciu o analizę zajętości przestrzeni na pamięciach masowych ○ Wykrywanie anomalii wydajnościowych w oparciu o uczenie maszynowe oraz porównanie parametrów historycznych i bieżących. Funkcjonalność ta musi wspierać serwery, urządzenia sieciowe oraz systemy pamięci masowych. ○ Monitorowanie wydajności, przepustowości oraz opóźnień dla systemy pamięci masowych. ○ Zaimplementowana analityka predykcyjna umożliwiająca określenie szacowanego czasu awarii dla optyki przełączników FC. ○ Szczegółowe informacje dla serwerów o modelu, konfiguracji, wersjach firmware poszczególnych komponentów adresacji IP karty zarządzającej. ○ Monitoring parametrów serwerów z informacją o minimum: ▪ Obciążeniu procesora ▪ Zużyciu pamięci RAM ▪ Temperaturze procesorów ▪ Temperaturze powietrza wlotowego ▪ Zużyciu prądu ▪ Zmianach w fizycznej konfiguracji serwera ▪ Dla wszystkich wymienionych parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ○ Monitoring parametrów pamięci masowych z informacją o minimum: ▪ Opóźnieniach ▪ IOPS ▪ Przepustowości ▪ Utylizacji kontrolerów ▪ Pojemność całkowita i dostępna ▪ Wszystkie informacje muszą być dostępne zarówno dla całej pamięci masowej jak i poszczególnych LUN-ów. ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. ▪ Dane historyczne o wykorzystaniu przestrzeni pamięci masowej muszą być przechowywane co najmniej 2 lata ▪ Informacje o poziomie redukcji danych ▪ Informacje o statusie replikacji oraz snapshotów ○ Monitoring parametrów przełączników sieciowych z informacją o minimum: ▪ Modelu, oprogramowania, adresacji IP, MAC adres, nr seryjny

	▪ Stanie komponentów: zasilacze, wentylatory ▪ Podłączonych hostach ▪ Ilości i statusu portów ▪ Utylizacji procesora ▪ Utylizacji poszczególnych portów ▪ Dla wszystkich wymienionych powyżej parametrów muszą być dostępne dane historyczne oraz automatycznie generowana informacja o anomaliach. • Aktualizacja firmware o możliwość aktualizcji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania o możliwość aktualizcji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania • Raporty o Możliwość generowania raportów dla serwerów zawierających informację o: ▪ Nazwie hosta, modelu serwera, nr serwisowym, dacie końca okresu kontraktu serwisowego, zainstalowanym systemie operacyjnym, protokole komunikacyjnym z systemem pamięci masowej ▪ Średnim obciążeniu: procesorów, pamięci RAM, IO, o Możliwość generowania raportów dla systemów pamięci masowych zawierających informację o: ▪ Nazwie, nr seryjnym, lokalizacji urządzenia, modelu urządzenia, wersji oprogramowania, zajętości systemu oraz poziomu redukcją danych, informacje o utworzonych LUN-ach i systemach pliku, status replikacji o Generowanie raportów do plików CSV i PDF • Cyberbezpieczeństwo o Analiza środowiska w oparciu o najlepsze praktyki dotyczące cyberbezpieczeństwa sprawdzająca stan poszczególnych urządzeń w środowisku i przypisujący im odpowiedni wynik bezpieczeństwa. System musi informować administratora o wykrytych lukach bezpieczeństwa oraz sposobie ich zabezpieczenia. o Musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń. o Stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych. o Możliwość przypisania dedykowanych ról dla poszczególnych administratorów. • Wspierane urządzenia o Urządzenie Producenta dostarczane w ramach postępowania o Posiadane przez Zamawiającego serwery, urządzenia pamięci masowych, przełączniki sieciowe, przełączniki SAN, rozwiązania HCI, deduplikatory Producenta oferowanego urządzenia (jeśli takie są w posiadaniu Zamawiającego) • Wirtualny asystent o Wbudowana w platformę funkcjonalność wirtualnego asystenta w

	oparciu o algorytmy GenAI przy dostępie do bazy wiedzy producenta urządzeń oraz analizie danych z monitoringu poszczególnych elementów infrastruktury;
	• Możliwość rozszerzenia funkcjonalności
	  ○ Możliwość rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT.
	• Inne
	  ○ Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android
	• Certyfikaty
	  ○ Oferowana platforma musi być zaprojektowana zgodnie ze standardami:
	  ▪ ISO 27001
	  ▪ NIST Security and Privacy Controls for Federal Information Systems and Organization
	  ▪ CSA Cloud Control Matrix

Warunki gwarancji	Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres co najmniej 36 miesięcy. Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie, przez Internet oraz z wykorzystaniem aplikacji. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie Producenta (dla krytycznych zgłoszeń serwisowych). Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik Producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) powinien rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbyć w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę. Możliwość rozszerzenia gwarancji producenta o usługę diagnostyki sprzętu na miejscu w przypadku awarii. Charakterystyka usługi diagnostyki: • Możliwości utworzenia zgłaszania serwisowego w wyniku, którego proces diagnostyki odbędzie się na miejscu w siedzibie zamawiającego. • Po przyjeździe do siedziby Zamawiającego, pracownik serwisu przystąpi do rozwiązywania problemu. Jeśli do rozwiązania problemu będzie konieczna dodatkowa pomoc diagnostyczna lub części, pracownik serwisu może w imieniu Zamawiającego skontaktować się z producentem w celu uzyskania pomocy. • Reakcja na miejscu u Zamawiającego powinna nastąpić w okresie zgodnym z czasem reakcji przypisanym do urządzenia, które posiada wykupioną usługę

	serwisową. • Pracownik serwisu powinien skontaktować się z Zamawiającym przed przyjazdem na miejsce w celu sprawdzenia zgłoszenia, ustalenia harmonogramu i potwierdzenia wszelkich informacji niezbędnych do realizacji wizyty technika na miejscu. • Jeśli w trakcie wstępnego procesu rozwiązywania problemu na miejscu awarii zostanie ustalone, że do realizacji usługi jest niezbędna jakaś część, znajdujący się na miejscu pracownik serwisu zamówi nową część i przekaże dodatkowe zgłoszenie do działu obsługi technicznej. Technik pracujący na miejscu powróci do siedziby Klienta w celu wymiany wysłanej części w ciągu czasu reakcji ustalonego zgodnie z umową serwisową zakupionego produktu. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

6. Wdrożenie VPN

1.Instalacja sprzętu serwerowego

- **Montaż fizyczny**: Wykonawca dostarczy i zainstaluje nowe urządzenia serwerowe w istniejącej infrastrukturze, w tym montaż w szafach rackowych, podłączenie zasilania i okablowania sieciowego zgodnie z planem.

2.Konfiguracja i optymalizacja zaawansowanego zdalnego zarządzania

- **Zdalny dostęp przez dedykowany interfejs zarządzania**: Wykonawca skonfiguruje dedykowane interfejsy zdalnego zarządzania dla nowych serwerów, wykorzystując zaawansowane funkcje zdalnego zarządzania dostępne w urządzeniach serwerowych, takie jak:
    - **Pełny dostęp do BIOS/UEFI**: Możliwość zdalnej konfiguracji ustawień BIOS/UEFI bez potrzeby fizycznej obecności w serwerowni.
    - **Zdalne uruchamianie, wyłączanie i restart serwerów**: Zdalne zarządzanie stanem zasilania serwerów, w tym możliwość ich włączania, wyłączania, resetowania oraz dostępu do opcji zasilania w trybie awaryjnym.
    - **Monitorowanie sprzętowe**: Zdalne monitorowanie krytycznych parametrów serwera, takich jak temperatura, napięcie, status zasilania, wykorzystanie zasobów (CPU, RAM, storage) oraz alertów o stanie sprzętu.
    - **Zdalna konsola KVM**: Wykorzystanie funkcji KVM (Keyboard, Video, Mouse) do zdalnego dostępu do serwera na poziomie konsoli, umożliwiające pełną interakcję z serwerem, jakby administrator był fizycznie obecny przed nim.

3. Konfiguracja zabezpieczeń zdalnego dostępu

- **Uwierzytelnianie wieloskładnikowe – dostarczenie licencji na 400 tokenów w miesiącu na okres 2 lat (MFA)**: Wykonawca wdroży uwierzytelnianie wieloskładnikowe dla dostępu do systemu VPN, zapewniając wysoki poziom bezpieczeństwa. Wykorzystane mogą być jednorazowe hasła (OTP), tokeny sprzętowe lub aplikacje do MFA.
- **Zabezpieczenie połączeń zdalnych**: Wykonawca zapewni, że wszystkie połączenia do interfejsów zdalnego zarządzania będą zabezpieczone przez odpowiednio skonfigurowane protokoły szyfrowania (np. TLS/SSL). Konfiguracja powinna również obejmować restrykcje dostępu na poziomie adresów IP lub sieci, z których można uzyskiwać zdalny dostęp.

4. Testowanie funkcjonalności zdalnego zarządzania

- **Testy poprawności działania**: Wykonawca przeprowadzi szczegółowe testy wszystkich skonfigurowanych funkcji zdalnego zarządzania, w tym testy uruchamiania, zdalnego BIOS/UEFI, konsoli KVM oraz zdalnych nośników wirtualnych.
- **Testy wydajności i bezpieczeństwa**: Wykonawca przeprowadzi testy wydajnościowe, aby upewnić się, że zdalne zarządzanie nie wpływa negatywnie na wydajność serwerów oraz testy penetracyjne, aby sprawdzić, czy konfiguracja zdalnego dostępu jest odpowiednio zabezpieczona przed potencjalnymi zagrożeniami.
- **Szkolenie zespołu IT**: Wykonawca przeprowadzi szkolenie dla zespołu IT zamawiającego, obejmujące korzystanie z funkcji zdalnego zarządzania, konfigurację bezpieczeństwa oraz najlepsze praktyki w zakresie zdalnego zarządzania serwerami.

Realizacja powyższych wymagań zapewni zamawiającemu nie tylko pełną kontrolę nad nowo wdrożonymi serwerami na poziomie sprzętowym, ale także bezpieczeństwo i efektywność w zarządzaniu infrastrukturą IT zdalnie, bez konieczności fizycznej obecności w miejscu, gdzie znajdują się serwery.

Część 2 zamówienia

1.UTM oraz punkty dostępowe - dostawa i konfiguracja

1.1 UTM – 1kpl.

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.

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego : Cyberbezpieczny Samorząd , Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).

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 7 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:
   - 10 portami Gigabit Ethernet RJ-45.
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 700 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.8 Gbps.
4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6.5 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 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 630 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.

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego : Cyberbezpieczny Samorząd , Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).

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 5000 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.

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego : Cyberbezpieczny Samorząd , Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).

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.

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego : Cyberbezpieczny Samorząd , Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).

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.

Testy wydajnościowe oraz funkcjonalne

1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

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 realizowana inline, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen, Security compliance (audyt konfiguracji i polityk urządzenia) na okres co najmniej 24 miesięcy.

Gwarancja oraz wsparcie

1. 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.
2. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany 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.
3. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.

1.2. Access Point - 3 kpl.

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej.

1. Obudowa urządzenia musi umożliwiać montaż na suficie lub ścianie wewnątrz budynku i zapewniać prawidłową pracę urządzenia w następujących warunkach klimatycznych:

   a. Temperatura 0–50°C,

   b. Wilgotność 5–90%.

2. Urządzenie musi być dostarczone z elementami mocującymi. Obudowa musi być fabrycznie przystosowana do zastosowania linki zabezpieczającej przed kradzieżą i być wyposażone w złącze typu Kensington.

3. Urządzenie musi być wyposażone w trzy niezależne moduły radiowe pracujące w podanych poniżej pasmach i obsługiwać następujące standardy:

   a. 2.4 GHz 802.11b/g/n,

   b. 5 GHz 802.11a/n/ac/ax,

   c. 2.4/5/6 GHz 802.11a/b/g/n/ac/ax

4. Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 24 SSID.

5. Urządzenie musi być wyposażone w moduł BLE.

6. Urządzenie musi być wyposażone w dwa interfejsy Ethernet 100/1000/2500/5000 Base-TX

7. Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3bt lub zewnętrzny zasilacz.

8. Punkt dostępowy musi umożliwiać następujące tryby przesyłania danych:

   a. Tunnel,

   b. Bridge,

   c. Mesh.

9. Wsparcie dla QoS: 802.11e, konfigurowalne polityki QoS per użytkownik/aplikacja.

10. Wsparcie dla poniższych metod uwierzytelnienia: WEP, WPA, WPA2, WPA3, Web Captive Portal, MAC blacklist & whitelist, 802.1X (EAP-TLS, EAP-TTLS/MSCHAPv2, EAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST).

11. Interfejs radiowy urządzenia powinien wspierać następujące funkcje:

   a. MIMO – 4x4,

   b. Wymagana maksymalna przepustowość dla poszczególnych modułów radiowych:

      i. 1148 Mbps;

      ii. 2402 Mbps;

      iii. 4804 Mbps

   c. Wymagana moc nadawania:

i. min. 27 dBm dla pasma 2.4GHz z możliwością zmiany co 1dBm;

ii. min. 26 dBm dla pasma 5GHz z możliwością zmiany co 1dBm;

iii. min. 24 dBm dla pasma 6GHz z możliwością zmiany co 1dBm

d. Wsparcie dla 802.11n 20/40Mhz HT,

e. Wsparcie dla kanałów 80 i 160 MHz,

f. Anteny – wbudowane dla nadajników standardu 802.11 o zysku min. 4dBi dla pasma 2.4GHz, 6dBi dla pasma 5GHz, 5.7dBi dla pasma 6GHz.

g. Nieużywany moduł radiowy może zostać wyłączony programowo w celu obniżenia poboru mocy,

12. Maksymalna deklarowana liczba klientów na każdy moduł radiowy – 512

13. Funkcje dodatkowe:

a. OFDMA UL i DL

b. Spatial Reuse (BSS Coloring)

c. UL-MU-MIMO

d. DL-MU-MIMO

e. Enhanced Target Wake Time (TWT)

f. Wbudowany analizator widma

g. Wbudowane mechanizmy WIPS/WIDS

Gwarancja oraz wsparcie

Urządzenie musi mieć zapewnioną dożywotnią ograniczoną gwarancję producenta, tj. do 5 lat od zaprzestania produkcji oraz być objęte serwisem gwarancyjnym producenta przez okres minimum 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.

Signature Not Verified
Dokument podpisany przez Krzysztof Szoszorek; Gmina i Miasto Witkowo
Data: 2024.10.10 10:23:25 CEST

Projekt współfinansowany przez Unię Europejską w ramach konkursu grantowego : Cyberbezpieczny Samorząd , Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. - Wzmocnienie krajowego systemu cyberbezpieczeństwa w ramach programu FUNDUSZE EUROPEJSKIE NA ROZWÓJ CYFROWY 2021-2027 (FERC).