***Znak sprawy* *Załącznik nr 1A do SWZ***

Szczegółowy opis przedmiotu zamówienia publicznego pn. **„Cyberbezpieczny Samorząd - Gmina Lubenia”** realizowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), Priorytet II Zaawansowane usługi cyfrowe, Działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa, w ramach projektu grantowego „Cyberbezpieczny Samorząd” o numerze FERC.02.02-CS.01-001/23, zgodnie z udzielonym grantem o numerze FERC.02.02-CS.01-001/23/0551/ FERC.02.02-CS.01-001/23/2024.

Przedmiotem zamówienia jest dostawa sprzętu oraz licencji na oprogramowanie, nie aktywowane wcześniej na innym urządzeniu, dostarczone w najnowszej stabilnej wersji pochodzącej z oficjalnego kanału dystrybucyjnego producenta oprogramowania oraz nieobciążone prawami na rzecz osób trzecich. Dostarczone oprogramowanie i wszelkie jego nośniki (o ile występują) musi być wolne zarówno od wad fizycznych jak i prawnych. Zamawiający zastrzega sobie możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów u Producenta w przypadku wystąpienia wątpliwości co do ich legalności.

Poniższe parametry należy traktować jako wymagania minimalne. Jeżeli wskazano producenta lub inne cechy charakterystyczne dla danego produktu oznacza to, że powyższe informacje są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Potencjalni Wykonawcy korzystając z oficjalnych kanałów dystrybucyjnych mają możliwość zaoferowania produktów których cechy wyszczególniono poniżej i które z punktu widzenia Zamawiającego będą pożądane ze względu na zastosowane rozwiązania w swojej infrastrukturze, dotyczy to zarówno zasobów sprzętowych ale również zasobów ludzkich zaangażowanych w utrzymanie ciągłości działania urządzeń, systemów i sieci. Powyższe nie wyklucza możliwości zaoferowania rozwiązań równoważnych których cechy, funkcjonalność oraz późniejsza eksploatacja będą zgodne z wymaganiami Zamawiającego. Aby umożliwić Wykonawcom prawidłowe skalkulowanie oferty dla rozwiązań równoważnych, tam gdzie to konieczne przygotowano kryteria równoważności.

***Poz.1 Macierz dyskowa***

|  |  |
| --- | --- |
| Element  konfiguracji/cecha/funkcjonalność | Wartość/opis parametru |
| Ilość | **2 sztuki** |
| Typ obudowy | Urządzenie musi być przeznaczone do instalacji w szafie technicznej typu RACK 19”, dostarczone ze wszystkimi niezbędnymi komponentami do montażu. |
| Kontrolery | Minimum dwa kontrolery pracujące w trybie Symmetrical Active-Active (SAN-only), to znaczy w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów w trybie bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery muszą pozwalać na udostępnianie zasobów protokołem FC, iSCSI w zależności od zastosowanych kart komunikacyjnych. |
| Zarządzanie oraz komunikacja między kontrolerami | Komunikacja pomiędzy parą kontrolerów (synchronizacja cache) macierzy musi wykorzystywać wewnętrzną, dedykowaną magistralę zapewniającą wysoką przepustowość i niskie opóźnienia. Nie dopuszcza się w szczególności komunikacji z wykorzystaniem urządzeń aktywnych FC/Ethernet/Infiniband.  Zamawiający dopuszcza komunikację z wykorzystaniem urządzeń aktywnych przy klastrze wielu kontrolerów. Każdy z kontrolerów musi mieć możliwość jednoczesnej prezentacji (aktywny dostęp odczyt i zapis) wszystkich wolumenów utworzonych w logicznych ramach całego systemu dyskowego.  Urządzenie musi umożliwiać podniesienie wydajności i niezawodności poprzez rozbudowę do 2 par kontrolerów, tworzących jedną logiczną macierz dyskową. Rozbudowa musi być możliwa bez konieczności wymiany zaoferowanej pary kontrolerów na nowe. Za jedną logiczną macierz uznaje się rozwiązanie, w którym zarządzanie wszystkimi kontrolerami jest możliwe z jednego interfejsu GUI, CLI. Nie dopuszcza się rozwiązań opartych o wirtualizator.  Macierz musi umożliwiać rozbudowę do co najmniej 4 par kontrolerów dyskowych tworzących jedna logiczną macierz, bez konieczności wymiany zaoferowanej pary kontrolerów. |
| Sposób zabezpieczenia  danych | Macierz musi umożliwiać skonfigurowanie poziomu RAID zapewniającego odporność na jednoczesną awarię 3 dysków w grupie RAID.  Urządzenie musi obsługiwać poziomy RAID5 i RAID6 (RAID z dystrybuowaną przestrzenią zapasową typu hot-spare) lub równoważne poziomy RAID zabezpieczające przed awarią dwóch dysków jednocześnie |
| Przestrzeń danych | Macierz musi być skonstruowana wyłącznie do obsługi modułów pamięci SSD i w żadnej konfiguracji nie może obsługiwać przestrzeni danych użytkownika na dyskach obrotowych/talerzowych.  Całkowita pojemność brutto (fizyczna) urządzenia musi wynosić minimum 53 TB i musi być zbudowana wyłącznie w oparciu o moduły pamięci SSD. Rozmiar pojedynczego modułu nie może być większy niż 4 TB.  Macierz musi umożliwiać rozbudowę do co najmniej 70 sztuk oferowanego typu modułów pamięci, bez wymiany kontrolerów macierzowych oraz bez potrzeby zakupu dodatkowych licencji. Dopuszcza się rozbudowę poprzez dodawanie półek i modułów SSD.  Możliwość definiowania dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej. |
| Kontrolery - procesor oraz pamięć cache | Kontrolery łącznie muszą być wyposażone w procesory o sumarycznej ilości min. 48 rdzeni (ang.: core). Procesory w macierzy muszą obsługiwać protokół PCI Express Generacji 4.  Urządzenie zbudowane z dwóch kontrolerów musi być wyposażone w co najmniej 128 GB pamięci podręcznej cache obsługującej operacje odczytu i zapisu zbudowane w oparciu o wydajną pamięć RAM. Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć lub posiadać podtrzymywanie bateryjne min. 48 godzin. |
| Porty | Macierz musi posiadać minimum 12 portów 10Gb/s obsługujące protokół iSCSI. Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), Zamawiający wymaga dostarczenia odpowiednich wkładek wraz z urządzeniem.  Możliwość rozbudowy macierzy o minimum 8 portów 25Gb/s obsługujących protokół iSCSI w ramach zaoferowanej ilości kontrolerów oraz możliwość podłączania serwerów bezpośrednio do tych portów macierzy bez użycia przełączników. Możliwość rozbudowy o wskazane porty nie może ograniczać rozbudowy do wymaganej ilości modułów pamięci. |
| Budowa urządzenia | Brak pojedynczego punktu awarii. Wszystkie krytyczne komponenty takie jak adaptery HBA, kontrolery dyskowe, pamięć, zasilacze i wentylatory muszą być zaprojektowane nadmiarowo: tak, aby awaria pojedynczego elementu nie wpływała na ciągłość dostępu do danych całego systemu. Komponenty te muszą być wymienialne w trakcie pracy.  Urządzenie musi cechować wsparcie dla zasilania z dwóch niezależnych źródeł prądu jednofazowego o napięciu 200-240V i częstotliwości 50-60Hz poprzez nadmiarowe zasilacze typu Hot-Swap. |
|  | Wymagana jest funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Zarządzanie i konfiguracja | Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy (w tym monitorowanie wydajności) oraz możliwość konfigurowania jej zasobów. Wymagana możliwość monitorowania stanu żywotności modułów SSD. Konsola graficzna musi być dostępna poprzez przeglądarkę internetową i być elementem systemu operacyjnego macierzy. Wymaga możliwość dostępu do danych wydajnościowych historycznych z poziomu GUI co najmniej 1 rok wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożlwiającym zbieranie i przeglądanie danych historycznych. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania. |
| Tworzenie kopii | Urządzenie musi umożliwiać utworzenie 800 kopii migawkowych (ang. snapshot) w trybie ROW (ang. Redirect on Write) dla pojedynczego wolumenu oraz minimum 2000 dla całej macierzy. Niedopuszczalne jest wykonywanie kopii w technologii COW (ang. Copy-on-Write). Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje należy je dostarczyć wraz z urządzeniem.  Wymagana jest możliwość utworzenia harmonogramu snapshotów, które będą zabezpieczone przed modyfikacją oraz usunięciem przez wybrany okres czasu bez odpowiednich uprawnień celem przywrócenia danych w przypadku ataku ransomware. Musi być możliwość odtworzenia danych z dowolnej kopii (snapshot) wykonanej w ramach harmonogramu. Odtworzenie danych z jednej kopii nie może uniemożliwiać odtworzenia danych z innej kopii z innego punktu w czasie. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje należy je dostarczyć wraz z urządzeniem.  Rozwiązanie musi umożliwiać hierarchiczne tworzenie kopii migawkowych (np. kopia z kopii z kopii).  Zamawiający wymaga aby zaproponowane rozwiązanie posiadało następującą funkcjonalność: tworzenie na żądanie pełnej kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z woluminu źródłowego na docelowy oraz resynchronizację danych z woluminu docelowego na źródłowy np. w sytuacji uszkodzenia danych na woluminie źródłowym. |
| Kompresja i deduplikacja | Macierz musi mieć możliwość włączenia funkcjonalności deduplikacji i kompresji danych w trybie in-line, a ponadto musi ona umożliwiać:   * włączenie deduplikacji dla poszczególnych wolumenów, * wyłączenie deduplikacji dla poszczególnych wolumenów na których wcześniej deduplikacja była włączona, * włączenie kompresji dla poszczególnych wolumenów, * wyłączenie kompresji dla poszczególnych wolumenów na których wcześniej kompresja była włączona, * uruchomienia jednocześnie deduplikacji i kompresji dla dowolnego wolumenu,   Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje należy je dostarczyć wraz z urządzeniem. |
| Zabezpieczenie dostępu do danych w modelu HA | Macierz musi umożliwiać uruchomienie mechanizmów zdalnej replikacji danych z innymi macierzami (ten sam model/rodzina modeli) - w trybie synchronicznym i asynchronicznym - po protokołach FC lub iSCSI bez konieczności stosowania zewnętrznych urządzeń konwersji wymienionych protokołów transmisji, główek typu serwer/wirtualizator, itp. Funkcjonalność replikacji danych musi być zapewniona z poziomu oprogramowania wewnętrznego macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.  Model oferowanej macierzy musi wspierać rozwiązanie klastra „wysokiej dostępności” tj. zapewnienia wysokiej dostępności zasobów danych macierzy dla podłączonych platform software’owych i sprzętowych z wykorzystaniem synchronicznej replikacji danych po FC lub iSCSI pomiędzy minimum 2 macierzami. Pod użytym 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 macierzą bądź awarii samej macierzy, powodujących dla danego środowiska brak dostępu do zasobów macierzy podstawowej. Replikacja danych pomiędzy macierzami podstawową i zapasową, wykorzystanych w układzie „wysokiej dostępności”, musi wspierać klastrownie wybranych woluminów bez konieczności stosowania lustrzanej konfiguracji grup dyskowych pomiędzy macierzami podstawową i główną. Musi być możliwość dodawania woluminów objętych zabezpieczeniem w klastrze bez konieczności zatrzymywania replikacji. Funkcjonalność „wysokiej dostępności” musi pozwalać na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową w przypadku awarii macierzy podstawowej (tzw. automated failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na ręczne (zaplanowane) przełączanie obsługi środowisk produkcyjnych z macierzy podstawowej na zapasową (tzw. manual failover). Funkcjonalność „wysokiej dostępności” musi pozwalać na minimum ręczne przełączanie obsługi środowisk produkcyjnych z macierzy zapasowej na podstawową po usunięciu awarii macierzy podstawowej (tzw. failback). Funkcjonalność „wysokiej dostępności” musi wspierać konfiguracje z macierzą zapasową zainstalowaną w innej fizycznej lokalizacji o ile nadal spełnione są warunki dla realizacji synchronicznej replikacji danych pomiędzy lokalizacjami.  Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje należy je dostarczyć wraz z urządzeniem. |
| Wydajność | Macierz musi posiadać funkcjonalność zarządzania wydajnością, która dynamicznie przydziela zasoby macierzy w celu spełnienia określonych celów wydajnościowych aplikacji (QoS). Możliwość ustawiania priorytetów wydajności dla aplikacji w oparciu o zdefiniowane profile wolumenowe, dla wydajności w IOPS i przepustowości danych. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.  Wsparcie dla mechanizmów dynamicznego przełączania zadań I/O pomiędzy kanałami w przypadku awarii jednego z nich (path failover). Wymagane jest wsparcie dla odpowiednich mechanizmów oferowanych przez producentów systemów operacyjnych: Windows, Vmware, Linux.  Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Windows Server 2016/2019/2022 Vmware 8.0, Vmware 7.0, CentOS. |
| Dodatkowe cechy urządzenia | Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych.  Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta a także musi być objęte serwisem producenta na terenie RP. |
| Gwarancja oraz zgłaszanie usterek | Macierz dyskowa musi zostać objęta minimum 3 letnim okresem gwarancji producenta z gwarantowanym czasem reakcji najpóźniej w następnym dniu roboczym od momentu zgłoszenia usterki. Zamawiający dopuszcza realizacje gwarancji przez autoryzowanego partnera serwisowego producenta.  Wymagane jest, aby gwarancja świadczona była z zachowaniem poniższych warunków:   * bezpłatna możliwość aktualizacje firmware, * dostęp do bazy wiedzy producenta w zakresie dostarczanych urządzeń, * dostęp do centrum pomocy technicznej producenta, * otwieranie zgłoszeń serwisowych w przypadku podejrzenia możliwości błędu w oprogramowaniu/hardware, * otrzymywanie poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy   Zgłoszenia usterek muszą być akceptowane zarówno drogą email (w ofercie należy podać dedykowany adres email do zgłoszeń serwisowych) jak również drogą telefoniczną (ogólnie dostępna linia telefoniczna, kontakt w języku polskim, linia telefoniczna w polskiej strefie numeracyjnej - telefon stacjonarny. Nie dopuszcza się numerów specjalnych, komórkowych oraz numerów o podwyższonej płatności. |

***Poz.2 Serwer rack***

|  |  |
| --- | --- |
| Nazwa parametru | Wartość/opis parametru |
| Ilość | **2 sztuki** |
| Obudowa | Rack o wysokości max 1U, wyposażona w panel LCD umieszczony 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, możliwa obsługa procesorów 32 rdzeniowych.  Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.  Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| Chipset | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| Procesory | Zainstalowane dwa procesory min. 16-rdzeniowe, min. 2.0GHz, klasy x86, dedykowane do pracy z zaoferowanym serwerem, umożliwiające osiągnięcie wyniku min. 280 w teście SPECrate2017\_int\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej. |
| Funkcjonalność oraz wielkość pamięci RAM | * korygowanie odczytu (Demand Scrubing) * czyszczenie patrolowe (Patrol Scrubing) * stałe wykrywanie usterek (Permanent Fault Detection) * 256GB DDR5 RDIMM 5600MT/s |
| Dyski twarde | Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1. |
| Gniazda PCI | trzy sloty PCIe LP |
| Interfejsy sieciowe/FC/SAS | Wbudowane min. 6 interfejsów sieciowych 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Dwuportowa karta sieciowa 25Gb Ethernet SFP28. |
| Porty wbudowane | 4 porty USB w tym min: 1 port USB 3.0 z tyłu obudowy, 1 port micro USB z przodu obudowy, 2 port VGA z czego jeden z przodu obudowy.  Możliwość rozbudowy o port RS232. |
| Video | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| Zasilacze | Redundantne, Hot-Plug min. 1100W klasy Titanium |
| Elementy montażowe | Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych |
| 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 * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi spełniać zalecenia NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust). |
| 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 serwer * 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 o 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 * 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 |
| Oprogramowanie do monitorowania | 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:   * możliwość aktualizacji firmware, oprogramowania zarządzającego dla systemów pamięci masowych, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, oprogramowania zarządzającego dla serwerów, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, oprogramowania zarządzającego dla rozwiazań HCI, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, dla systemów przełączników FC, wraz z informacją o zalecanych wersjach oprogramowania * możliwość aktualizacji firmware, dla deduplikatorów, wraz z informacją o zalecanych wersjach oprogramowania   Raporty:   * 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 * 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 * Generowanie raportów do plików CSV i PDF   Cyberbezpieczeństwo:   * 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 * musi istnieć możliwość tworzenia własnych polityk bezpieczeństwa w oparciu o wzorce dla poszczególnych urządzeń * stała analiza środowiska IT umożliwiająca wykrycie ataku ransomware na podstawie analizy posiadanych danych * możliwość przypisania dedykowanych ról dla poszczególnych administratorów   Wspierane urządzenia:   * urządzenie Producenta dostarczane w ramach postępowania * 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:   * 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 rozbudowy systemu o zintegrowane i dodatkowe płatne moduły do monitoringu aplikacji oraz zarządzania incydentami w ramach infrastruktury IT. Oferowana platforma musi posiadać dedykowaną aplikację na urządzenia iOS oraz Android.  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 |
| Certyfikaty | * Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 * 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 – Wykonawca złoży dokument potwierdzający spełnianie wymogu na etapie dostawy. * 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 gwarancji Producenta z zakresu wdrażanej technologii na okres 2 lat. * 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. * 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. * 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 niezbędny dodatkowy podzespół 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.   **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 wraz dostawą urządzeń wraz z wykazem kontaktów serwisowych**  **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.** |

***Poz.3 Wielofunkcyjna zapora sieciowa (UTM)***

|  |  |
| --- | --- |
| Nazwa parametru | Opis |
| Ilość | **1 sztuka** |
| Wymagania ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.  Wykonawca dostarczy urządzenie które umożliwi połączenie z posiadanym przez Zamawiającego urządzeniem aby zwiększyć niezawodność, wydajność i skalowalność sieci (HA Cluster). Konfiguracja urządzeń pozwoli na rozłożenie obciążenia oraz zapewni redundancję w przypadku awarii jednego z urządzeń. Zamawiający oczekuje osiągnięcie funkcjonalności polegającej m.in. na możliwości zarządzania urządzeniami połączonymi w klaster za pomocą wspólnego panelu administracyjnego. Zamawiający informuje iż obecnie użytkuje urządzenie Fortigate 60f.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 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 | * 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. * Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. * Monitoring stanu realizowanych połączeń VPN. * System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| Interfejsy, Dysk, Zasilanie | System realizujący funkcję Firewall dysponuje co najmniej 10 portami Gigabit Ethernet RJ-45  System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.  System jest wyposażony w zasilanie AC. |
| Parametry wydajnościowe | * W zakresie Firewall’a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps. * Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps. * Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.3 Gbps. * Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 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:   * Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. * Kontrola Aplikacji. * Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. * Ochrona przed malware. * Ochrona przed atakami - Intrusion Prevention System. * Kontrola stron WWW. * Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. * Zarządzanie pasmem (QoS, Traffic shaping). * Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). * 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. * Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3. * Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system. * 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 | Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  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.   W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.  Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.  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. . |
| Połączenia VPN | 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.   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:   * Routingu statycznego. * Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP). * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM. * Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu. * ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu. * BFD (Bidirectional Forwarding Detection). * Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| Funkcje SD-WAN | * System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN. * SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| Zarządzanie pasmem | * System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. * System daje możliwość określania pasma dla poszczególnych aplikacji. * System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP. * System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | * Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). * Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS. * 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. * System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów. * System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). * Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * 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. * System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików. * Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta. * Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | * Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. * System chroni przed atakami na aplikacje pracujące na niestandardowych portach. * Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur. * System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. * Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty). * Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http. * Wykrywanie i blokowanie komunikacji C&C do sieci botnet. * Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| Kontrola aplikacji | * Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. * Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. * Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. * Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. * Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur. * Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021). * 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 | * Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. * 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. * Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard. * Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. * Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex). * Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony. * Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo. * Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW. * System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | 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.   System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  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.  Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | * 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. * Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów. * Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. * System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow. * System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. * Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. * Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone. * Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM). * Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | * 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. * 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. * Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa. * Możliwość włączenia logowania per reguła w polityce firewall. * System zapewnia możliwość logowania do serwera SYSLOG. * Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| Testy wydajnościowe oraz funkcjonalne | 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: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 24 miesięcy. |
| Gwarancja oraz wsparcie | 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. |
| Wymagania dodatkowe | * **Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej) – dołączyć wraz dostawą urządzeń wraz z wykazem kontaktów serwisowych** * **Certyfikat ISO 9001 podmiotu serwisującego – dołączyć wraz dostawą urządzeń wraz z wykazem kontaktów serwisowych** * **Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań- dołączyć wraz dostawą urządzeń wraz z wykazem kontaktów serwisowych** |

***Poz.4 Przełącznik sieciowy***

|  |  |
| --- | --- |
| Nazwa parametru | Opis parametru |
| Ilość | **2 sztuki** |
| Wymagania ogólne | W ramach postępowania wymaganym jest dostarczenie przełączników sieciowych współpracujących z oferowanym w poz. 3 OPZ systemem bezpieczeństwa za pomocą wspólnego panelu administracyjnego. |
| Parametry fizyczne | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. * Zasilanie AC 230V. * Maksymalny pobór mocy: 60 W. * Minimalny zakres temperatury pracy: 0-40ᵒC. |
| Interfejsy sieciowe - wymagania minimalne | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:   * 48 porty GE RJ-45 * 4 porty 10 GE SFP+ |
| Zarządzanie | * Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). * Wsparcie dla SNMP w wersjach 1-3 * Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. * Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. * Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. * Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). * Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. * Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. * Automatycznie wykonywane rewizje konfiguracji. |
| Wydajność | * Przepustowość urządzenia - min. 175 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 250 Mpps. * Tablica adresów MAC o pojemności co najmniej 32k wpisów. * Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund. |
| Wymagane funkcje | * Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. * Obsługa Jumbo Frames. * Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). * Agregacja portów zgodna ze standardem 802.3ad. * Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q * Obsługa routingu statycznego. * Port-mirroring. * Uwierzytelnianie 802.1x na poziomie portu. * Uwierzytelnianie 802.1x w oparciu o adres MAC. * W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). * W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. * W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. * Obsługa protokołu sFlow. |
| Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC | Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:   * Centralne zarządzanie konfiguracją urządzenia * Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania * Centralne zarządzanie sieciami VLAN. * Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u * Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp.. * Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. * Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. * Automatyczna detekcja i rekomendacje konfiguracji. * Przesyłanie logów na zewnętrzny serwer syslog. * Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników. * Obsługa białych i czarnych list adresów MAC. * Wykrywanie aplikacji komunikujących się w sieci.   Konfiguracja urządzeń pozwoli na redundantne połączenie z elementami zarządzającymi.  W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa | System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.  System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |
| Gwarancja oraz wsparcie | System musi być objęty serwisem gwarancyjnym producenta przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7. |
| Wymagania dodatkowe | Dla zapewnienia wysokiego poziomu usług podmiot serwisujący musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług serwisowych. Zgłoszenia serwisowe będą przyjmowane w języku polskim w trybie 24x7 przez dedykowany serwisowy moduł internetowy oraz infolinię. Oferent winien przedłożyć dokumenty:   * Oświadczanie Producenta lub Autoryzowanego Dystrybutora świadczącego wsparcie techniczne o gotowości świadczenia na rzecz Zamawiającego wymaganego serwisu (zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej). * Certyfikat ISO 9001 podmiotu serwisującego. * Oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań |

***Poz.5 Zasilacz awaryjny***

|  |  |
| --- | --- |
| Nazwa parametru | Opis parametru |
| Ilość | **2 sztuki** |
| Moc pozorna | 5000 VA |
| Moc rzeczywista | 4500 W |
| Topologia | On-line z korekcją współczynnika mocy |
| Sprawność przy pracy normalnej (100% obc.) | 93% |
| Sprawność w trybie podwyższonej sprawności (100% obc.) | 98% |
| Współczynnik mocy | 0,9 |
| Czas przełączenia na baterię | 0 ms |
| Możliwość pracy równoległej | Tak |
| Liczba, typ gniazd wyjściowych | Listwa zaciskowa, 8 x IEC C13 (2 grupy gniazd sterowalnych), 2 x IEC C19 16A |
| Typ gniazda wejściowego | Listwa zaciskowa |
| Czas podtrzymania dla 100% obciążenia dla pf=0,9 | 3 min |
| Czas podtrzymania przy 50% obciążenia dla pf=0,9 | 10 min |
| Dodatkowe baterie | Możliwość dodania dodatkowych modułów baterii w celu wydłużenia czasu podtrzymania do min. 240 minut dla 100% obciążenia przy pf=0,9 |
| Napięcie znamionowe | 230 V |
| Tolerancja napięcia wejściowego | 180V – 270 V |
| Częstotliwość znamionowa | 50/60 Hz autodetekcja |
| Tolerancja częstotliwości | 40 – 70 Hz |
| Kształt napięcia | Sinusoidalny |
| Napięcie znamionowe wyjściowe | 230 V (domyślnie) / możliwość wyboru 200/208/220/240 V |
| Zakres zmian napięcia | +/-1% napięcia nominalnego |
| Częstotliwość wyjściowa | 50/60 Hz +/-0,5% |
| Współczynnik szczytu | 3:1 |
| Dopuszczalny zakres współczynnika mocy obc. Liniowego | 0,5 indukcyjny - 0,5 pojemnościowy |
| Baterie wymieniane przez użytkownika "na gorąco" | Tak |
| Ochrona przed przeładowaniem | Tak |
| Ochrona przed głębokim rozładowaniem | Tak |
| Okresowy automatyczny test baterii | Tak |
| System zarządzania pracą baterii | System nieciągłego ładowania baterii |
| Zdolność zwarciowa | 90A |
| Możliwość uruchomienia bez napięcia w sieci | Tak |
| Baterie wewnętrzne | min. 5Ah 12V, minimum 15 szt. |
| Czas ładowania baterii | do 1,5 godz. do 90% pojemności użytkowej |
| Interfejs komunikacyjny | * USB * RS232 DB-9 żeński (HID) * styki przekaźnikowe * miniport wyłącznik ON/OFF * SNMP/Ethernet |
| Panel sterowania z wyświetlaczem LCD | Panel LCD obrotowy. Wskazania min.: stan pracy urządzenia, poziom obciążenie, napięcie wyjściowe, częstotliwość wejściowa/wyjściowa, test baterii, numer seryjny urządzenia, pozostały czas podtrzymania, wydajność, zużycie energii. |
| Sygnały akustyczne | Awaria, niski stan naładowania baterii, przeciążenie, serwis |
| Dane techniczne karty SNMP | Network Support: Ethernet 1.0 Gbps - Full duplex / HTTP 1.1, SNMP V1, SNMP V3/ NTP, SMTP, DHCP/. Dostępny port USB (serwisowy) |
| Typ obudowy | Uniwersalna Rack max 3U |
| Wyposażenie standardowe | Instrukcja bezpieczeństwa, kabel RS-232, kabel USB, szyny 19", podstawka do montażu wieżowego, uchwyty kablowe, karta sieciowa SNMP/Ethernet |
| Dołączone oprogramowanie | Monitorujące i zarządzające UPS |
| Zgodność ze standardem Energy Star | Tak |
| Maksymalny ciężar | 50 kg |
| Poziom hałasu w odl. 1m | do 45 dBA dla pracy normalnej |
| Znaki bezpieczeństwa | CE, IEC/EN 62040-1, IEC/EN 62040-2, IEC/EN 62040-3 |
| Gwarancja producenta | 24 miesiące dla elektroniki oraz baterii |
| Bypass elektroniczny automatyczny | TAK |

***Poz.6 Listwa zasilająca (PDU)***

|  |  |
| --- | --- |
| Nazwa parametru | Opis parametru |
| Ilość | **2 sztuki** |
| Gniazo wejściowe | IEC C20 16A |
| Gniazda wyjściowe | 12x IEC C13 + 12x IEC C39 (obsługujące wtyczki C14 lub C20) |
| Maksymalna moc obciążeniowa listwy | 3.5 kW |
| Maksymalna temperatura pracy | co najmniej 60°C. Możliwość pracy z tyłu szafy rack (w ciepłych korytarzach powietrznych) |
| Standardy | Dyrektywa RoHS, REACH, Dyrektywa WEEE |
| Certyfikaty | CE, IEC 62368-1, IEC 63000 |
| Gwarancja | 24 miesiące |

***Poz.7 Przełącznik sieciowy (core)***

|  |  |
| --- | --- |
| Nazwa parametru | Opis parametru |
| Ilość | **2 sztuki** |
| Wymagania ogólne | Jeżeli poniżej użyto słowa „Obsługa” oznacza to, że urządzenie powinno posiadać mechanizmy konfiguracji oraz kontroli dla danej funkcjonalności, ponadto osiągnięcie żądanej funkcjonalności nie będzie wymagało zakupu dodatkowych licencji wraz z urządzeniem jak również nie będzie wiązało się z zakupem dodatkowych licencji w przyszłości. |
| Zasilanie oraz parametry fizyczne | * Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa 1U * Zasilanie AC 100-240VAC, 50-60Hz * Maksymalny pobór mocy: 60 W * 2x zasilacze typu Hot-swap |
| Interfejsy sieciowe - wymagania minimalne | Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi w ilości:   * 24x 10G SFP+ * 2x 40G QSFP+ |
| Wydajność oraz parametry sieciowe | * Szybkość przełączania 640 Gbps * Szybkość przekazywana 480 Mbps * Bufor pakietów 9MB * Pamięc podręczna 8GB * Pamięć RAM 2GB * Wielkość tablicy MAC 96K * Wielkość tablicy ARP min. 12000 * Ramki Jumbo o ładowności min. 9600 B * Wsparcie dla następujących metod autentykacji: 802.1X, AAA * Protokoły zarządzania zdalnego: SNMP, RMON, HTTP, Telnet, SSH |
| Funkcje sieciowe | * Obsługa pełnego dupleksu, półdupleksu i autonegocjacji dupleksu * Obsługa automatycznej negocjacji prędkości portu * Obsługa ramki Jumbo * Obsługa kontroli przepływu * Obsługa burzy rozgłoszeniowej (Storm Control) * Obsługa blokowanie portów * Obsługa izolacji portów * Obsługa tunelowania protokołów warstwy 2 |
| Funkcje VLAN | * Obsługa minimum 4000 sieci VLAN * Obsługa trybu dostępu VLAN: Dostęp/Trunk * Obsługa domyślnej sieci VLAN * Obsługa klasyfikacji VLANów * Obsługa podwójnego tagowania ramek VLAN (podstawowego QinQ, selektywnego QinQ) * Obsługa statystyk VLAN * Obsługa prywatnych sieci VLAN * Obsługa sieci VLAN dla gości * Obsługa głosowych sieci VLAN |
| Funkcje tablicy adresów MAC | * Obsługa statycznych adresów MAC * Obsługa dynamicznego uczenia się i starzenia adresów MAC * Obsługa uczenia sprzętowego * Obsługa czarnych dziur adresów MAC * Obsługa detekcji MAC Flap |
| Funkcje agregacji łączy | * Obsługa statycznej agregacji łączy * Obsługa protokołu LACP * Obsługa statycznego równoważenia obciążenia (SLB) * Obsługa dynamicznego równoważenia obciążenia (DLB) * Obsługa samonaprawiania równoważenia obciążenia (SHLB) |
| Funkcje związane z poprawą niezawodności | * Obsługa protokołu STP/RSTP/MSTP * Obsługa ochrony protokołu STP (BPDU Filter/Guard, Root Guard, LoopGuard, Anti TC-BPDU attack) * Obsługa pojedynczego pierścienia ERPS / stycznych pierścieni ERPS / przecinających się pierścieni ERPS * Obsługa wykrywania pętli zwrotnej portu * Obsługa BFD * Obsługa VRRP * Obsługa MLAG * Obsługa monitorowania procesów (Sysmon) * Obsługa dla sprzętowego Watch Dog |
| Funkcje ARP | * Obsługa dynamicznego przechylania i starzenia ARP * Obsługa Gratuitous ARP * Obsługa proxy ARP i local proxy ARP * Obsługa VARP |
| Funkcje IPV4 | * Obsługa tras statycznych IPv4 * Obsługa tras statycznych IPv4 współpracujących z IP SLA * Obsługa VRF * Obsługa weryfikacji uRPF * Obsługa protokołów RIPv1, RIPv2 * Obsługa OSPFv2 * Obsługa IS-IS * Obsługa BGP * Obsługa map tras i list prefiksów * Obsługa routingu opartego na zasadach (PBR) * Obsługa przekierowań ICMP i nieosiągalnych ICMP * Obsługa ECMP |
| Funkcje IPV6 | * Obsługa protokołu ICMPv6 * Obsługa NDP * Obsługa PMTU * Obsługa tras statycznych IPv6 * Obsługa protokołu RIPng * Obsługa OSPFv3 * Obsługa protokołu IPv6 przez tunel IPv4 * Obsługa tunelu 6to4 * Obsługa tunelu ISTAP * Obsługa DHCPv6 * Obsługa listy prefiksów IPv6 |
| Funkcje dystrybucji informacji (multicast) | * Obsługa protokołu IGMP v1/v2/v3 * Obsługa protokołu IGMP Snooping * Obsługa agenta IGMP * Obsługa mapowania IGMP SSM * Obsługa PIM-SM, PIM-SSM, PIM-DM * Obsługa MLDv1/v2, MLDv1/v2 snooping * Obsługa MVR i MVR6 * Obsługa PIM-SMv6 |
| Funkcje QoS | * Obsługa klasyfikacji ruchu na podstawie COS/DSCP (prosta klasyfikacja) * Obsługa klasyfikacji ruchu na podstawie ACL (klasyfikacja złożona) * Obsługa planowania kolejek w oparciu o klasyfikację ruchu * Obsługa oznaczania pól priorytetowych (COS/DSCP) pakietu * Obsługa przekierowania przepływu * Obsługa lustrzanego odbicia przepływu * Obsługa nadzorowania ruchu * Obsługa kształtowania ruchu * Obsługa statystyk ruchu * Obsługa planowania SP (Strict Priority) * Obsługa planowania WDRR (Weighted Deficit Round Robin) * Obsługa planowania mieszanego SP+WDRR * Obsługa TD (Tail Drop) * Obsługa WRED (Weighted Random Early Detection) |
| Funkcje bezpieczeństwa | * Obsługa SSH * Obsługa Radius * Obsługa TACAS+ * Obsługa AAA * Obsługa dot1x opartego na portach i dot1x opartego na adresie MAC * Obsługa konfiguracji dot1x Guest za pomocą polecenia lub serwera Radius * Obsługa list kontroli dostępu (ACL) * Obsługa klasyfikacji ruchu na podstawie źródłowego i docelowego adresu IP/ sourceanddestination i docelowego adresu MAC/source i docelowej warstwy dla numeru protokołu/VLANID * Obsługa dopasowywania ACL do pól zdefiniowanych przez użytkownika (UDF) * Obsługa aktywnej listy ACL na podstawie zakresu czasu * Obsługa inspekcji ARP * Obsługa ochrony źródła IP * Obsługa zabezpieczeń portów w celu ograniczenia uczenia się adresów MAC na interfejsie * Obsługa zabezpieczeń VLAN w celu ograniczenia uczenia się adresów MAC na interfejsie * Obsługa czarnej i białej listy CoPP (Control Plane Protect) oraz funkcji limitu szybkości * Obsługa limitu przepływu CPU (mechanizm ochrony procesora przed złośliwymi przepływami poprzez wstrzykiwanie ogromnej ilości PDU do przełączników) * Obsługa zapobiegania atakom DDOS * Obsługa filtrowania ACL Logowanie Telnet/SSH * Obsługa 802.1AE (MACsec) * Obsługa wykrywania przeplotu łącza (Link-Flapping) |
| Funkcje konfiguracji | * Obsługa serwera DHCP * Obsługa przekazywania DHCP * Obsługa funkcji DHCP Snooping * Obsługa klienta DHCP * Obsługa DHCP Option82 * Obsługa RMON * Obsługa sFlow * Obsługa IP SLA * Obsługa EFD (Elephant Flow Detection) * Obsługa NTP * Obsługa wykrywania i odzyskiwania stanu Errdisable dla portu * Obsługa konfiguracji statycznego klienta DNS * Obsługa protokołu LLDP * Obsługa pętli zwrotnej portu * Obsługa sprzętowej pętli zwrotnej (wewnętrznej/zewnętrznej) * Obsługa konfiguracji czasu systemowego * Obsługa konfiguracji strefy czasowej |
| Funkcje diagnostyczne | * Obsługa diagnostyki opartej na modułach * Obsługa wyświetlania i alarmowania użycia procesora/pamięci * Obsługa wyświetlania temperatury urządzenia / PSU / wentylatora / stanu i alarmu * Obsługa dzienników operacji użytkownika * Obsługa zarządzania dziennikami, alarmami i informacjami diagnostycznymi * Obsługa VCT (Virtual Cable Test) * Obsługa gromadzenia szczegółowych informacji diagnostycznych * Obsługa rejestrowania informacji o ponownym uruchomieniu * Obsługa diagnostyki sieci (ping/traceroute) * Obsługa mirroringu: obsługa źródła mirroringu dla port/vlan/cpu * Obsługa port/port grupa/vlan/cpu jako miejsca docelowego kopii lustrzanej * Obsługa ERSPAN * Obsługa statystyk pakietów do CPU/od CPU * Obsługa ping L2 * Obsługa UDLD (jednokierunkowe wykrywanie łącza) |
| Funkcje zarządzania | * Obsługa zarządzania portami w modelu wdrożeniowym in-band oraz out-of-band * Obsługa uprzywilejowanych uprawnień użytkownika i uprzywilejowanych poleceń * Obsługa zarządzania siecią w oparciu o SNMPv1/v2/v3 * Obsługa MIB - publicznego i prywatnego * Obsługa Trap - publicznych i prywatnych * Obsługa konfiguracji i zarządzania w oparciu o WEB UI * Obsługa konfiguracji i zarządzania w oparciu o RPC-API * Obsługa SmartConfig (automatyczna konfiguracja po uruchomieniu systemu) * Obsługa zmiany specyfikacji systemu poprzez wybór różnych profili STM * Obsługa konfiguracji funkcji w oparciu o licencję * Obsługa przywracania domyślnej konfiguracji fabrycznej * Obsługa ręcznego / zaplanowanego restartu * Obsługa aktualizacji za pomocą lokalnego pliku obrazu / zdalnego serwera TFTP * Obsługa aktualizacji online U-Boot |
| Gwarancja na urządzenie | Urządzenie musi być objęte serwisem gwarancyjnym producenta przez okres 24 miesięcy. |

***Poz.8 Klucze sprzętowe (U2F)***

|  |  |
| --- | --- |
| Nazwa parametru | Opis parametru |
| Ilość | **25 sztuk** |
| Zastosowanie | * klucz sprzętowy umożliwi wdrożenie metody uwierzytelniania określanej jako „key wrapping”. * klucz sprzętowy zapewnia wsparcie dla mechanizmów FIDO U2F i FIDO2 WebAuth |
| Interfejs | USB |
| Obsługa NFC | TAK |
| Szyfrowanie | ECC p256, ECC p384, RSA 2048, RSA 4096 (PGP) |
| Kolor | czarny |
| Gwarancja na urządzenie | Urządzenie musi być objęte serwisem gwarancyjnym przez okres 24 miesięcy. |