# **Host wirtualizacyjny**

|  |
| --- |
| ***Obudowa:***   * Obudowa Rack o wysokości max 1U * 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 144 rdzeniowych. * Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. * Na płycie głównej powinny znajdować się minimum 32 sloty przeznaczone do instalacji pamięci. * Płyta główna powinna obsługiwać do 8TB pamięci RAM. |
| ***Chipset:***   * Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych. |
| ***Procesor:***   * Zainstalowane dwa procesory min. 8-rdzeniowe, min. 3.5GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 307 w teście SPECspeed®2017\_fp\_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej oferowanego serwera. |
| ***Pamięć RAM:***   * 8x 32GB DDR5 RDIMM 6400MT/s, |
| ***Dyski twarde:***   * Zainstalowane dwa dyski M.2 NVMe SSD o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1. |
| ***Dyski twarde:***   * Dwa sloty PCIe LP |
| ***Interfejsy sieciowe/SAS:***   * 4 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) * 2 wkładki 25GbE SFP28 SR * Czteroportowa karta 12Gb SAS HBA |
| ***Wbudowane porty:***   * 3 porty USB w tym min: * 1 port USB 2.0 Type-C * 2 porty USB 3.1 * Port VGA z tyłu obudowy |
| ***Video:***   * Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |
| ***Zasilacze:***   * Redundantne, Hot-Plug min. 800W klasy Titanium |
| ***Elementy montażowe:***   * Komplet wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych * Ramię (organizer) do kabli ułatwiające wysuwanie serwera do celów serwisowych |
| ***Bezpieczeństwo:***   * Zatrzask górnej pokrywy oraz blokada na ramce panelu zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych. * 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. * 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 V3 * 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 być zgodna z zaleceniami 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 dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * 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 SNMP; IPMI2.0, VLAN tagging, SSH * 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 sześciu administratorów jednocześnie * Wsparcie dla automatycznej rejestracji DNS * wsparcie dla LLDP * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy. * Monitorowanie zużycia dysków SSD * Automatyczne zgłaszanie alertów do centrum serwisowego producenta * Automatyczne update firmware dla wszystkich komponentów serwera * Możliwość przywrócenia poprzednich wersji firmware * Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON * Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych * Automatyczne tworzenie kopii ustawień serwera w opraciu o harmonogram. * Możliwość wykrywania odchyleń konfiguracji na poziomie konfiguracji UEFI oraz wersji firmware serwera * kontrola stanu BIOS pod kątem naruszenia integralności oprogramowania * możliwość modyfikacji reguł chłodzenia kart w slotach PCIe, z możliwością własnych ustawień * możliwość ustawienia limitu temperatury powietrza wychodzącego z serwera * możliwość ustawienia dopuszczalnego wzrostu temperatury powietrza przepływającego przez serwer * możliwość ustawienia maksymalnej temperatury powietrza dochodzącego do slotów PCIe * możliwość rozszerzenia funkcjonalności o: * możliwość wysyłania danych o stanie procesora, kart sieciowych, zasilaczy, kart GPU, lokalnych dysków i urządzeń NVMe, jak również dane wydajnościowe serwera do zewnętrznych narzędzi analitycznych jak Splunk, Grafana, ElasticSearch * możliwość wykorzystania tokenu lub aplikacji SecurID do uwierzytelniania wielkoskładnikowego przy logowaniu do karty zarządzającej * Automatyczne odświeżanie certyfikatów SSL * monitorowanie przepływu powietrza na bieżąco (w CFM) |
| ***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. * 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. * Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin: * wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów * wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityka konfiguracji * z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny) * inwentaryzacja komponentów w serwerze i ich mikrokodów * historia poboru mocy i temperatury serwera * zbieranie danych diagnostycznych serwera do paczki serwisowej |
| ***Oprogramowanie do monitorowania:***  Oparta na chmurze aplikacja Producenta oferowanego urządzenia, która zapewnia proaktywne monitorowanie i rozwiązywanie problemów infrastruktury IT oraz integrację z platformą wirtualizacji VMware. 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 rozwiązań 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 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:***   * 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](http://www.epeat.net) potwierdzający spełnienie normy co najmniej Epeat Silver, dla kraju, w którym produkt będzie użytkowany, według normy wprowadzonej w 2019 roku - 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 2022, Microsoft Windows Server 2025. |
| ***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 5 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * 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 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. * 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. * 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. * Wykonawca załączy do oferty certyfikat ISO 27001:2022 na projektowanie sprzedaż i wdrażanie rozwiązań teleinformatycznych, świadczenie usług serwisowych i konsultingowych. |
| ***Ilość:***   * Należy dostarczyć dwa jednakowe hosty wirtualizacyjne |
| ***System operacyjny:***  Oprogramowanie Microsoft Windows Server DataCenter 2025 zgodnie z polityką licencjonowania producenta oraz 60 sztuk licencji dostępowych dla użytkowników na całe rozwiązanie – Windows Server 2025 user CAL lub równoważne spełniające poniższe warunki zgodności:   * Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i sześciu wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. * Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. * Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. * Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. * Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. * Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. * Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. * Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading; * Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. * Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. * Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET. * Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów. * Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych. * Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe. * Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji. * Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play). * Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu. * Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath). * Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. * Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty. |

# **Macierz**

|  |
| --- |
| ***Obudowa:***   * Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 2U z możliwością instalacji min. 24 dysków 2.5” |
| ***Dyski twarde:***  Zainstalowane:   * 7x dysk SAS o pojemności min. 2.4TB, Hot-Plug * 5x dysk SSD SAS MU o pojemności min. 1.6TB, Hot-Plug |
| ***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 12Gb SAS (4 porty na kontroler) |
| ***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. * Zasilacze użyte w macierzy powinny spełniać wymagania dotyczące sprawności dla 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). Wymagane dołączenie do oferty oświadczenia Producenta potwierdzające spełnienie powyższych zaleceń. |
| ***Inne:***   * Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym * producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. * Oferowany model macierzy w momencie składania oferty nie może mieć ogłoszonej daty końca sprzedaży. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego urządzenia, potwierdzające brak ogłoszenia takiej daty. * Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. * Deklaracja zgodności CE. |
| ***Warunki gwarancji:***   * Zamawiający wymaga zapewnienia gwarancji Producenta z zakresu wdrażanej technologii na okres 5 lat. * Zamawiający oczekuje możliwości zgłaszania zdarzeń serwisowych w trybie 24/7/365 następującymi kanałami: telefonicznie i przez Internet. * Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania Producenta, w tym także sprzedanego oprogramowania. * Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy. * 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 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. * 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. * 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. * Wykonawca załączy do oferty certyfikat ISO 27001:2022 na projektowanie sprzedaż i wdrażanie rozwiązań teleinformatycznych, świadczenie usług serwisowych i konsultingowych. |
| ***Dodatkowe wyposażenie:***   * 4x kabel 12Gb HD Mini-SAS/HD Mini-SAS o długości min. 2m |

# **Deduplikator**

|  |
| --- |
| Urządzenie musi być przeznaczone do deduplikacji i przechowywania kopii zapasowych. Urządzenie musi spełniać wymagania wyspecyfikowane w niniejszej tabeli. |
| Dostarczone urządzenie musi oferować przestrzeń min. 16TB netto (powierzchni użytkowej) bez uwzględniania mechanizmów protekcji – przestrzeń dedykowana do gromadzenia deduplikatów, wymagana skalowalność do min. 250TB netto (powierzchni użytkowej widocznej po założeniu systemu plików) |
| Dostarczone urządzenie powinno umożliwiać 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) powinny zostać przemigrowane (w postaci zdeduplikowanej) na dodatkową warstwę, wymagane wsparcie dla AWS, Microsoft Azure oraz Google GCP. Wymagana enkrypcja danych przechowywanych na warstwie typu Cloud. Wymagane dostarczenie licencji na przestrzeń min. 80TB netto dla warstwy CLOUD. |
| Oferowane urządzenie musi posiadać minimum   * 4 portów 10/25Gb/s Eth OP (wymagana pełna obsada wkładek)   wymagana możliwość obsługi każdym z w/w portów protokołów CIFS, NFS, deduplikacja na źródle |
| Oferowane urządzenie musi umożliwiać jednoczesny dostęp wszystkimi poniższymi protokołami:   * CIFS, NFS * zapewniającym deduplikację na źródle, wymagane wsparcie dla aplikacji Commvault (co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator), Veeam Backup and Replication (co najmniej na poziomie Veeam Data Mover), NetWorker na poziomie standardowego klienta * VTL (min. 10 jednocześnie) |
| Wymagane jest dostarczenie licencji, pozwalającej na jednoczesną obsługę protokołów CIFS, NFS, deduplikacja na źródle, VTL do oferowanej pojemności urządzenia |
| Oferowane pojedyncze urządzenie musi osiągać zagregowaną wydajność (dla maksymalnej konfiguracji) protokołami: NFS co najmniej 25 TB/h (dane podawane przez producenta) oraz co najmniej 50 TB/h z wykorzystaniem deduplikacji na źródle (dane podawane przez producenta). |
| Urządzenie musi pozwalać na jednoczesną obsługę minimum 250 strumieni w tym jednocześnie:   * zapis danych minimum 150 strumieniami * odczyt danych minimum 50 strumieniami * replikacja minimum 50 strumieniami   pochodzących z różnych aplikacji oraz dowolnych protokołów (CIFS, NFS, VTL, deduplikacja na źródle) oraz dowolnych interfejsów (FC, LAN) w tym samym czasie.  Wymienione wartości 250 jednoczesnych strumieni dla wszystkich protokołów (czyli jednocześnie 150 dla zapisu i jednocześnie 50 strumieni dla odczytu i jednocześnie 50 strumieni dla replikacji) musi mieścić w przedziale oficjalnie rekomendowanym i wspieranym przez producenta urządzenia.  Wszystkie zapisywane strumienie muszą podlegać globalnej deduplikacji przed zapisem na dysk (in-line) jak opisano w niniejszej specyfikacji. |
| Oferowane urządzenie musi mieć możliwość emulacji następujących bibliotek taśmowych:   * StorageTek L180 * IBM TS 3500 |
| Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych min. LTO5 oraz LTO7 |
| Urządzenie musi umożliwiać (w przypadku VTL’a) emulację minimum 250 napędów, emulację min. 30 000 slotów w przypadku poj. biblioteki taśmowej oraz emulację sumarycznie min. 60 000 slotów. |
| 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 urządzenia. |
| Technologia deduplikacji musi wykorzystywać algorytm bazujący na zmiennym, dynamicznym bloku jednak o wielkości nie większej niż 12 kB.  Algorytm ten musi samoczynnie i automatycznie dopasowywać się do otrzymywanego strumienia danych co oznacza, że urządzenie musi dzielić otrzymany pojedynczy strumień danych na bloki o różnej długości, bez konieczności podejmowania czynności mających na celu ustalenie predefiniowanej długości bloków używanych do deduplikacji danych określonego typu. Deduplikacja zmiennym, dynamicznym blokiem oznacza, że wielkość każdego bloku (na jaki są dzielone dane pojedynczego strumienia backupowego) może być inna niż poprzedniego oraz jest indywidualnie ustalana przez algorytm deduplikacji zastosowany w urządzeniu, oferowane urządzenie nie może dzielić jakiegokolwiek pojedynczego strumienia danych backupowych na bloki o ustalonej, tej samej długości. |
| Oferowany produkt musi posiadać obsługę mechanizmów globalnej deduplikacji dla danych otrzymywanych jednocześnie wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie całego urządzenia co oznacza, że przechowywany na urządzeniu fragment danych nie może być ponownie zapisany bez względu na to, jakim protokołem zostanie ponownie otrzymany. Wszystkie emulowane jednocześnie w obrębie urządzenia biblioteki wirtualne (VTL) oraz udziały NFS/CIFS również powinny podlegać globalnej deduplikacji – blok danych otrzymany i zapisany w wirtualnej bibliotece „A”, nie może zostać ponownie zapisany jeśli trafi do innej wirtualnej biblioteki „B” w obrębie tego samego urządzenia (to samo dotyczy udziałów NFS/CIFS). Przestrzeń składowania zdeduplikowanych danych musi być jedna dla wszystkich protokołów dostępowych, co oznacza zastosowanie pojedynczej bazy deduplikatów bez względu na ilość/rodzaj używanych jednocześnie protokołów dostępowych. |
| Proces deduplikacji musi odbywać się in-line – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Zapisowi na system dyskowy muszą podlegać tylko unikalne bloki danych nie zapisane jeszcze na system dyskowy urządzenia. Dotyczy to każdego fragmentu przychodzących do urządzenia danych. Wymaganie nie będzie spełnione jeżeli deduplikacja in-line realizowana będzie przez zewnętrzną aplikację backup’ową. Wymaganie deduplikacji in-line dotyczy zapisu danych przez każdy z wymaganych intefejsów, w przypadku interfejsów: NFS, CIFS oraz VTL realizacja deduplikacji in-line nie może w żadnym stopniu zależeć od konkretnej aplikacji backu’owej, dane zapisywane poprzez interfejsy NFS CIFS bez użycia jakiejkolwiek aplikacji backup’owej również muszą być deduplikowane w sposób in-line |
| Proponowane rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej) w celu ich późniejszej deduplikacji (wymagana deduplikacja in-line) |
| Wszystkie unikalne bloki przed zapisaniem na dysk muszą być dodatkowo kompresowane. |
| Tryb zapisu zabezpieczanych danych nie może umożliwiać nadpisywania danych, dane mogą być zapisywane jedynie w trybie append-only, dane dla których wygasła retencja powinny zostać usunięte podczas procesu czyszczenia tzw. Cleaning, wymaganie dotyczy wszystkich danych zapisanych na urządzeniu a nie wybranych grup danych objętych działaniem blokad zabezpieczających przed usunięciem/modyfikacją danych. |
| Oferowane urządzenie musi wspierać (wymagane formalne wsparcie producenta urządzenia), co najmniej następujące aplikacje: Commvault, Veeam Backup and Replication, NetWorker.  W przypadku współpracy z każdą z poniższych aplikacji:   * Commvault * Veeam Backup and Replication * NetWorker   urządzenie musi umożliwiać deduplikację na źródle (w przypadku Commvault: co najmniej na poziomie Media Server a także Client Direct przy użyciu storage accelerator, w przypadku Veeam Backup and Replication co najmniej na poziomie Veeam Data Mover), w przypadku NetWorker na poziomie standardowego klienta) i przesłanie nowych, nie znajdujących się jeszcze na urządzeniu bloków poprzez sieć LAN.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć LAN jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| W przypadku przyjmowania backupów z Commvault, Veeam Backup and Replication, NetWorker, urządzenie musi umożliwiać deduplikację na źródle (co najmniej na poziomie Media Server dla CommVault, Data Mover dla Veeam, klienta dla NetWorker) i przesłanie nowych, nieznajdujących się jeszcze na urządzeniu bloków poprzez sieć FC.  Deduplikacja w wyżej wymienionych przypadkach musi zapewniać aby do oferowanego urządzenia były transmitowane poprzez sieć FC jedynie fragmenty danych nie znajdujące się dotychczas na urządzeniu. |
| Oferowane urządzenie musi umożliwiać uruchamianie maszyn wirtualnych VMware bezpośrednio z danych backupowych bez konieczności odtwarzania danych. |
| Wymagana funkcjonalność Load Balancing oraz Link Failover w obrębie portów (Eth) wykorzystywanych przez aplikację backupową. |
| Wymagane wsparcie dla backupów typu Virtual Synthetics w przypadku aplikacji Commvault, Veeam Backup and Replication oraz NetWorker. |
| W przypadku deduplikacji na źródle poprzez sieć IP (LAN oraz WAN), wymagana możliwość szyfrowania komunikacji kluczem minimum 256 bitów. |
| Urządzenie powinno umożliwiać zaszyfrowanie przechowywanych danych, wymagane licencje umożliwiające zaszyfrowanie i przechowywanie zaszyfrowanych danych w obrębie maksymalnej pojemności oferowanego urządzenia. |
| Urządzenie musi wspierać deduplikację na źródle poprzez sieć FC (SAN) minimum dla następujących systemów operacyjnych:   * Windows * Linux (RedHat, SuSE) |
| Oferowane urządzenie musi umożliwiać bezpośrednią replikację danych do drugiego urządzenia takiego samego typu. Konfiguracja replikacji musi być możliwa w każdym z trybów:   * jeden do jednego * wiele do jednego * jeden do wielu * kaskadowej (urządzenie A replikuje dane do urządzenia B, które te same dane replikuje do urządzenia C).   Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane mogą być tylko te fragmenty danych (bloki) które nie znajdują się na docelowym urządzeniu. Ewentualna licencja na replikację jest przedmiotem postępowania. |
| Urządzenie musi umożliwiać wydzielenie określonych portów Ethernet dedykowanych do replikacji. |
| W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami. |
| W przypadku replikacji danych między dwoma urządzeniami oferowanego typu, wymagana możliwość kontroli przez: Commvault oraz NetWorker muszą być możliwe do uzyskania jednocześnie wszystkie następujące funkcjonalności:   * replikacja odbywa się bezpośrednio między dwoma urządzeniami bez udziału serwerów pośredniczących * replikacji podlegają tylko te fragmenty danych (na poziomie bloków używanych do deduplikacji), które nie znajdują się na docelowym urządzeniu * replikacja zarządzana jest z poziomu wymaganej aplikacji * aplikacja posiada informację o obydwu kopiach zapasowych znajdujących się w obydwu urządzeniach bez konieczności przeprowadzania procesu inwentaryzacji |
| Oferowane urządzenie musi działać poprawnie przy zapełnieniu danymi na poziomie co najmniej 90%. Dokumentacja urządzenia nie może wskazywać na ew. problemy, obostrzenia, które są efektem zapełnieniu urządzenia zabezpieczanymi danymi, na poziomie mniejszym niż 90%. |
| Wymagana możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami – oferowane urządzenie powinno być wyposażone w mechanizm umożliwiający zarządzaniem stopnia wykorzystania pasma na potrzeby replikacji. |
| Zdeduplikowane i skompresowane dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID 6 bądź równoważnej. |
| Oferowane urządzenie musi pozwalać na realizację oraz przechowywanie SnapShot’ów, czyli umożliwiać zamrożenie obrazu danych (stanu backupów) w urządzeniu na określoną chwilę. Oferowane urządzenie musi również umożliwiać odtworzenie danych ze Snapshot’u.  Odtworzenie danych ze Snapshot’u nie może wymagać konieczności nadpisania danych produkcyjnych jak również nie może oznaczać przerwy w normalnej pracy urządzenia (przyjmowania/odtwarzania backupów). |
| Urządzenie musi pozwalać na przechowywanie minimum 500 Snapshotów jednocześnie w obrębie oferowanej przestrzeni, przy zachowaniu globalnej deduplikacji oraz standardowego trybu pracy urządzenia – umożliwiającego wykorzystanie wszystkich dostępnych funkcjonalności. |
| Urządzenie musi umożliwiać podział na logiczne części. Dane znajdujące się w każdej logicznej części muszą być między sobą deduplikowane (globalna deduplikacja między logicznymi częściami urządzenia). |
| Urządzenie musi mieć możliwość podziału na minimum 10 logicznych części pracujących równolegle. Producent musi oficjalnie wspierać pracę minimum 10 logicznych części pracujących równolegle z pełną wydajnością urządzenia. |
| Dla każdej z w/w logicznych części oferowanego urządzenia musi być możliwość zdefiniowania oddzielnego użytkownika zarządzającego daną logiczną częścią deduplikatora. Użytkownicy zarządzający logiczną częścią A muszą widzieć tylko i wyłącznie zasoby logicznej części A i nie mogą widzieć żadnych innych zasobów oferowanego urządzenia. |
| Wymagana możliwość zaprezentowania każdej z logicznych części oferowanego urządzenia, jako niezależnego urządzenia dostępnego za pośrednictwem:   * CIFS * NFS * VTL * deduplikacja na źródle |
| Urządzenie musi umożliwiać zdefiniowanie blokady skasowania danych (funkcjonalność WORM). Blokada skasowania danych musi chronić plik w zdefiniowanym czasie przed usunięciem pliku, modyfikacją pliku.  Blokada skasowania danych musi działać w dwóch trybach (do wyboru przez administratora):   * Możliwość zdjęcia blokady przed upływem ważności danych * Brak możliwości zdjęcia blokady przed upływem ważności danych (COMPLIANCE), w tym wypadku wymagane wsparcie norm SEC 17a-4(f) oraz ISO Standard 15489-1 w zakresie ochrony danych, wymagane oficjalne wsparcie wymaganej blokady przez aplikację Commvault, Veeam Backup and Replication oraz NetWorker – wymagane potwierdzenie na oficjalnych stronach w/w aplikacji backup’owych oraz producenta oferowanego deduplikatora   Licencje na blokadę usunięcia/zmiany przechowywanych plików muszą być dostarczone wraz z urządzeniem.  Wymagana możliwość automatycznego uruchamiania blokady (podczas zapisu) WORM dla danych zapisywanych na obszar objęty działaniem wspomnianej blokady. W każdym przypadku wymagana również możliwość używania blokady WORM dla obrazu danych uzyskanych poprzez użycie wymaganej funkcjonalności SnapShot. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). |
| Urządzenie musi mieć możliwość przechowywania danych niezmienialnych:   * Video * Grafika * Nagrania dźwiękowe * Pliki pdf   na udziałach CIFS/NFS. |
| Urządzenie musi weryfikować dane po zapisie (nie chodzi o ew. weryfikację danych indeksowych generowanych przez urządzenie ale o weryfikację wszystkich zabezpieczanych danych backup’owych). Każda zapisana na dyskach porcja danych musi być odczytana i porównana z danymi otrzymanymi przez urządzenie. Powyższa weryfikacja musi być realizowana w locie, czyli przed usunięciem z pamięci oryginalnych danych (otrzymanych z aplikacji backupowej), musi być realizowana w trybie ciągłym (a nie ad-hoc), wymagane parametry wydajnościowe urzadzenia muszą uwzględniać tę funkcjonalność.  Wymagane potwierdzenie opisanej funkcjonalności w oficjalnej dokumentacji producenta oferowanego urządzenia. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności). |
| Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nie należące do backupów o aktualnej retencji) w procesie czyszczenia. |
| Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu / odtwarzania danych (zapisu / odczytu danych z zewnątrz do systemu). |
| Wymagana możliwość zdefiniowania maksymalnego obciążenia urządzenia procesem usuwania przeterminowanych danych (poziomu obciążenia procesora), wymagane potwierdzenie w ogólno dostępnej dokumentacji. Zamawiający zastrzega możliwość prośby o dostarczenie ogólnodostępnej dokumentacji oferowanego produktu potwierdzającego spełnienie wymaganej funkcjonalności) |
| Wymagana możliwość zdefiniowania harmonogramu wg. którego wykonywany jest proces usuwania przeterminowanych danych (czyszczenia), realizowany równolegle z procesami backup/restore/replication. |
| Standardowa częstotliwość usuwania przeterminowanych danych (czyszczenie) nie powinna być większa niż 1 raz na tydzień - minimalizując czas w którym backupy/odtworzenia narażone są na spowolnienie (weryfikacja wymagania na podstawie dokumentacji typu DOBRE PRAKTYKI publikowanej przez producenta). |
| Urządzenie musi umożliwiać systemowo (wbudowana funkcjonalność) - realizację procesu pierwszego czyszczenia dopiero po przekroczeniu 75% zajętości oferowanej przestrzeni |
| Urządzenie musi mieć możliwość zarządzania poprzez   * Interfejs graficzny dostępny z przeglądarki internetowej * Poprzez linię komend (CLI) dostępną z poziomu ssh (secure shell) |
| Oprogramowanie do zarządzania musi rezydować na oferowanym urządzeniu deduplikacyjnym. |
| Oferowane urządzenie musi mieć możliwość sprawdzenia pakietu upgrade’ującego firmware urządzenia (GUI lub CLI), to znaczy sprawdzenia czy nowa wersja systemu nie spowoduje problemów z urządzeniem. |
| Urządzenie musi być rozwiązaniem kompletnym, appliancem sprzętowym pochodzącym od jednego producenta. Zamawiający nie dopuszcza stosowania rozwiązań typu gateway. Oferowany typ urządzenia musi być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania. |
| Oferowane urządzenie powinno być objęte 5 letnim wsparciem producenta działającym w trybie Next Business Day . Uszkodzone nośniki pozostają u Zamawiającego bez ponoszenia dodatkowych kosztów. |

# **Oprogramowanie do backupu oraz backupu maszyn wirtualnych**

|  |
| --- |
| ***Wymagania ogólne:***   * Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie : - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5, * Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.x, 7.x i 8.0 oraz Microsoft Hyper-V 2012, 2012R2, 2016, 2019, 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej * Oprogramowanie musi współpracować z infrastrukturą Nutanix w wersji 6.5.x - 6.7.x, Red Hat Virtualization 4.4 SP1, Oracle Linux Virtualization 4.5.4 lub nowszy oraz Proxmox VE 8.2 lub nowszy. * Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS, obiektowych pamięci masowych kompatybilnych z Microsoft Azure, AWS S3 i urządzeń kompatybilnych z protokołem S3 oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux. * Oprogramowanie musi umożliwiać backup dla 10 maszyn wirtualnych i posiadać wsparcie techniczne na okres min. 24 miesiące. * Musi istnieć możliwość użytkowania oprogramowania nawet po wygaśnięciu wsparcia technicznego, bez prawa do aktualizacji. |
| ***Całkowite koszty posiadania:***   * Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej * Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków * Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji * Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu. * Oprogramowanie musi zapewniać warstwę abstrakcji nad poszczególnymi urządzeniami pamięci masowej, pozwalając utworzyć jedną wirtualną pulę pamięci na kopie zapasowe. Wymagane jest wsparcie dla nieograniczonej liczby pamięci masowych to takiej puli. * Oprogramowanie musi pozwalać na tworzenie repozytorium kopii zapasowych bezpośrednio na zasobach Microsoft Azure Blob, Google Cloud Storage, Amazon S3, Wasabi Cloud Storage oraz na innych kompatybilnych z S3 przestrzeniach obiektowych. Dodatkowo, oprogramowanie musi wspierać archiwizowanie tych danych do Microsoft Azure Archive Blob Storage oraz Amazon S3 Glacier. * Oprogramowanie musi wspierać niezmienność kopii zapasowych na potrzeby ochrony przed ransomware poprzez niedopuszczenie do usunięcia lub modyfikacji kopii zapasowej w zadanym okresie czasu. * Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania * Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL, Oracle oraz PostgreSQL (w tym odtwarzanie point-in-time) * Oprogramowanie musi zapewniać możliwość delegacji uprawnień do odtwarzania na portalu * Oprogramowanie musi mieć możliwość integracji z innymi systemami poprzez wbudowane RESTful API * Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji * Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji * Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania * Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych. * Oprogramowanie musi posiadać natywne mechanizmy uwierzytelniania wieloskładnikowego (MFA) w celu dostępu do konsoli administracyjnej * Oprogramowanie musi wymagać autoryzacji dwóch administratorów backupu do wykonania krytycznych operacji (np. skasowanie backupu, dodanie kolejnego administratora) * Oprogramowanie musi posiadać integracje z systemami zarządzania kluczami szyfrującymi (KMS) * Oprogramowanie musi posiadać integracje z systemami typu SIEM * Oprogramowanie musi posiadać asystenta produktu opartego o AI, pozwalającego na przeszukiwanie dokumentacji technicznej. Powinna istnieć możliwość wyłączenia tej opcji. |
| ***Wymagania RPO:***   * Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej * Oprogramowanie musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych. * Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych z dokładnością do pojedynczego datastoru * Oprogramowanie musi zapewniać tworzenie kopii zapasowych z bezpośrednim wykorzystaniem snapshotów macierzowych. Musi też zapewniać odtwarzanie maszyn wirtualnych z takich snapshotów. Proces wykonania kopii zapasowej nie może wymagać użycia jakichkolwiek hostów tymczasowych. Opisana funkcjonalność powinna działać w środowisku VMware. * Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware. * Oprogramowanie musi wspierać kopiowanie backupów oraz zasobów plikowych na taśmy (LTO oraz IBM 3592). * Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son) * Oprogramowanie musi wspierać bezpośrednią integrację z urządzeniami deduplikacyjnymi. Minimalnie wsparcie wymagane dla Dell DataDomain, HPE StoreOnce, ExaGrid, Fujitsu CS800, Quantum DXi oraz Infinidat InfiniGuard. * Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS. * Oprogramowanie musi mieć możliwość kopiowania backupów oraz replikacji wirtualnych maszyn z wykorzystaniem wbudowanej akceleracji WAN. * Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji. * Oprogramowanie musi mieć możliwość replikacji ciągłej, opartej o VMware VAIO, włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere. Dla replikacji ciągłej musi być możliwość zdefiniowania dziennika pozwalającego na odzyskanie danych z dowolnego punku w ramach ustalonego parametru RPO. * Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik * Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding) * Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN) |
| ***Wymaganie RTO:***   * Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware, Hyper-V oraz Nutanix AHV niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych. * Dodatkowo dla środowiska vSphere, Hyper-V i Nutanix AHV powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) * Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami * Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre * Oprogramowanie musi pozwalać na uruchomienie zasobów plikowych SMB oraz baz danych MS SQL, Oracle i PostgreSQL bezpośrednio ze skompresowanego i skompresowanego pliku backupu. Dodatkowo wspierana musi być migracja on-line tak uruchomionych zasobów na środowisko produkcyjne. * Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków * Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform. * Oprogramowanie musi umożliwić odtworzenie plików/folderów lub ich uprawnień na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików * Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy natywnego API dla platformy VMware i PowerShell Direct dla platformy Hyper-V. * Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, BSD, Solaris, Mac, Novell * Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM * Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej. * Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników, dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA, elementów AD Sites oraz pozwalać na odtworzenie haseł. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2013SP1 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"). Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2008 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku point-in-time, całych baz lub pojedynczych tabeli, widoków oraz procedur. * Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2013 i nowszych. Odtwarzanie musi być możliwe bezpośrednio do środowiska produkcyjnego dla odzysku całych witryn, bibliotek oraz pojedynczych dokumentów wraz z historią ich wersji. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych PostgreSQL z opcją odtwarzanie point-in-time. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Linux. * Oprogramowanie musi wspierać granularne odtwarzanie baz danych SAP HANA do oryginalnej lub innej lokalizacji * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez Oracle RMAN * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez SAP HANA, SAP Oracle * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez MS SQL VDI * Oprogramowanie musi posiadać natywną integrację dla backupów wykonywanych poprzez IBM Db2 * Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN |
| ***Ograniczenie ryzyka:***   * Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu. Powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna) * Dla VMware’a oprogramowanie musi pozwalać na uruchomienie takiego środowiska dla replik maszyn wirtualnych oraz bezpośrednio ze snapshotów macierzowych stworzonych na wspieranych urządzeniach. * Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem * Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32. * Oprogramowanie musi analizować indeksy systemów plików zabezpieczanych maszyn w poszukiwaniu rozszerzeń, notatek żądania okupu oraz innych oznak obecności ransomware/malware * Oprogramowanie musi mieć możliwość skanowania plików backupu przy pomocy znanych sygnatur złośliwego oprogramowania * Oprogramowanie, bazując na wyuczonym modelu maszynowym (machine learning) musi w locie wykrywać oznaki złośliwego oprogramowania (malware, ransomware) oraz cyberataków * Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego. |
| ***Środowiska fizyczne:***   * Rozwiązanie musi wykonywać kopię zapasową systemu Windows oraz Linux wykorzystując agenta znajdującego się wewnątrz systemu operacyjnego * Rozwiązanie musi wspierać systemy operacyjne Windows w wersjach klienckich oraz serwerowych * Rozwiązanie musi wspierać co najmniej następujące dystrybucje systemów Linux: Debian, Ubuntu, RHEL, CentOS, Oracle Linux, SLES, Fedora, openSUSE * Rozwiązanie musi wspierać system operacyjny macOS * Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z systemów Windows, Linux, MacOS, Unix * Rozwiązanie musi mieć możliwość instalacji oraz zarządzania wykorzystując tryb niezależny (per agent) jak również zcentralizowany (poprzez centralną konsolę zarządzającą) * Rozwiązanie musi wspierać systemy oparte o Microsoft Failover Cluster * Rozwiązanie musi wspierać zabezpieczanie do oraz odzyskiwanie z urządzeń blokowych pozwalając na odzysk całej maszyny (tzw. bare metal recovery) wybranych wolumenów, oraz wybranych plików i folderów * Rozwiązanie musi wspierać backup podłączonych dysków USB * Kopia zapasowa całej maszyny oraz pojedynczych wolumenów musi być wykonywana na poziomie blokowym * Rozwiązanie musi pozwalać na przechowywanie kopii zapasowych na zasobach lokalnych (wewnętrznych) dyskach zabezpieczanej maszyny, Direct Attached Storage (DAS), takich jak zewnętrzne dyski USB, eSATA lub Firewire, Network Attached Storage (NAS) pozwalającym na wystawienie swoich zasobów poprzez SMB (CIFS) lub NFS, bezpośrednio na zasobach obiektowych (w tym chmury) * Rozwiązanie musi wspierać deduplikacje oraz kompresję na źródle. Dane wysyłane na repozytorium muszą być już odpowiednio przetworzone * Rozwiązanie musi wspierać kontrolę pasma sieciowego * Rozwiązanie musi wspierać ograniczenie wykonywania backupów dla konkretnych sieci bezprzewodowych * Rozwiązanie musi wspierać ograniczenia wykonywania backupów dla połączeń VPN * Rozwiązanie musi wspierać śledzenie zmienionych bloków podczas wykonywania kopii zapasowych. Dla systemów Windows technologia śledzenia bloków dla systemów serwerowych musi być certyfikowana przez Microsoft * Rozwiązanie musi wspierać technologię BitLocker * Rozwiązanie musi wspierać uruchamianie z nośnika odtwarzania * Rozwiązanie musi wspierać odzysk pojedynczych elementów aplikacji z jednoprzebiegowej kopii zapasowej dla Microsoft Exchange 2013SP1 i nowszych, Microsoft Active Directory 2008 i nowszych, Microsoft Sharepoint 2013 i nowszych, Microsoft SQL 2008 i nowszych, Oracle 11g i nowszych oraz PostgreSQL 12 i nowszych * Rozwiązanie musi wspierać odzysk do konkretnego punktu w czasie (point-in-time) dla wspieranych systemów bazodanowych * Rozwiązanie musi umożliwiać natychmiastowe publikowanie baz MS SQL, Oracle I PostgreSQL poprzez bezpośrednie uruchomienie ich z pliku backupu. * Rozwiązanie musi wspierać odzysk obrazów kopii zapasowych bezpośrednio do vSphere, Hyper-V, Nutanix AHV, Microsoft Azure, Microsoft Azure Stack, Amazon EC2 oraz Google Cloud Platform * Rozwiązanie musi wspierać szyfrowanie * Rozwiązanie musi wspierać możliwość wykonywania kopii zapasowych stacji klienckich, lokalnie do repozytorium tymczasowego (cache) gdy połączenie sieciowe do głównego repozytorium kopii zapasowych jest niedostępne * Rozwiązanie musi posiadać funkcjonalność automatycznego zmniejszenia szybkości przetwarzania danych, aby nie dopuścić do obniżenia wydajności systemu zabezpieczanego * Rozwiązanie musi posiadać ochronę przed ransomware poprzez automatyczne odmontowanie nośnika po wykonanym backupie stacji klienckiej * Rozwiązanie musi wspierać tworzenie wielu zadań backupowych |
| ***Monitoring:***   * System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich * System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie. * System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. * System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter * System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn * System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel * System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk * System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora * System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów * System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard) * System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna * System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego * System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta * System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych. * System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu. * System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware * System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji od 10.x do 10.6 |
| ***Raportowanie:***   * System musi umożliwiać raportowanie środowiska wirtualizacyjnego VMware w wersji 6.x, 7.x oraz 8.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie * System musi umożliwiać raportowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2012, 2012R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie. * System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów. * System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V * System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF * System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc * System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach * System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów * System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych * System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych * System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury * System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta * System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych. * System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’. * System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware * System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots) * System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie |

# **Klaster UTM, tokeny do obsługi MFA**

|  |
| --- |
| Zamawiający posiada obecnie urządzenie Fortinet FG-100F o numerze seryjnym: FG100FTK21053748 w ramach postępowania należy dostarczyć urządzenie spełniające poniższe funkcjonalności, następnie zestawić oba urządzenia w klaster wysokiej dostępności. |
| ***Wymagania ogólne:***   * System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. * System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN. * System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu. * System wspiera protokoły IPv4 oraz IPv6 w zakresie: * Firewall. * Ochrony w warstwie aplikacji. * Protokołów routingu dynamicznego. |
| ***Redundancja, monitoring i wykrywanie awarii:***   * 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 poniższą liczbą i rodzajem interfejsów: * 18 portami Gigabit Ethernet RJ-45. * 8 gniazdami SFP 1 Gbps. * 2 gniazdami SFP+ 10 Gbps. * System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. * System jest wyposażony w zasilanie 2xAC. |
| ***Parametry wydajnościowe:***   * W zakresie Firewall’a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 55 tys. nowych połączeń na sekundę. * Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B. * Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps. * Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 11 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 2.5 Gbps. * Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps. * Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps. |
| ***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). |
| ***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. * Amazon Web Services (AWS). * Microsoft Azure. * Cisco ACI. * Google Cloud Platform (GCP). * OpenStack. * VMware NSX. * Kubernetes. |
| ***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. * Możliwość rozbudowania Systemu o dodatkową funkcjonalność wstrzymania dostarczenia pliku, dla którego jest realizowana analiza z wykorzystaniem systemu Sandbox, do czasu otrzymania werdyktu z systemu Sandbox. |
| ***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. * Możliwość rozbudowania Systemu o sygnatury do ochrony przed atakami na systemy przemysłowe SCADA. |
| ***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. * Możliwość rozbudowania Systemu o dodatkowe usługi: logowania, raportowania, korelacji zdarzeń realizowanych w chmurze. |
| ***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:***   * Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 24 miesiące, 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 ogólne:***   * Zamawiający wymaga, aby wsparcie serwisowe świadczył zespół (minimum 3 osoby) certyfikowanych inżynierów w zakresie administracji systemami UTM, legitymujący się ważnymi certyfikatami Certified Professional Network Security. * Wykonawca przedstawi oświadczanie o gotowości świadczenia wymaganego serwisu zawierające: adres strony internetowej serwisu i numer infolinii telefonicznej. * Wykonawca musi posiadać certyfikat ISO 27001:2022 na projektowanie sprzedaż i wdrażanie rozwiązań teleinformatycznych, świadczenie usług serwisowych i konsultingowych – załączyć do oferty |
| ***Wymagania dodatkowe:***   * W ramach postępowania powinny zostać dostarczone co najmniej 50 tokenów programowych współpracujących z Zamawianym urządzeniem, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów oraz w ramach połączeń VPN typu client-to-site. * Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile. * Dla tokenów na system iOS i Android wymaga się: * aktywacji z systemu firewall * generowania kodu (cyfr) co 30 lub 60 sekund, * możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne), * ochrony dostępu poprzez konfigurowalny kod PIN. |

# **Przełącznik światłowodowy**

|  |
| --- |
| Przełącznik musi być dedykowanym urządzeniem sieciowym o wysokości 1U przystosowanym do montowania w szafie rack. |
| Przełącznik musi posiadać 24 porty pozwalających na obsadzenie modułami optycznymi SFP+ 1/10Gbps |
| Przełącznik musi posiadać nie mniej niż 2 wbudowane porty uplink 100 Gigabit Ethernet |
| Musi istnieć możliwość wykorzystania interfejsu 100 GbE jako 4x10GbE lub 4x25GbE |
| Przełącznik musi umożliwiać rozbudowę o nie mniej niż 4 porty 10/25 Gigabit Ethernet SFP+. |
| Przełącznik musi wspiera metodę przełączania store-and-forward. |
| Przełącznik musi umożliwiać stworzenie stosu (w postaci pętli) liczącego nie mniej niż 10 urządzeń. Do łączenia w stos mogą zostać zastosowane wbudowane interfejsy 100 Gigabit Ethernet. W ramach urządzeń, z którymi może tworzyć stos musza być urządzenia wspierająca PoE oraz urządzenia wspierające prędkości portów 1 / 2,5/5/10Gbps |
| Stos musi być odporny na awarie, tzn. przełącznik kontrolujący pracę stosu (master) musi być automatycznie zastąpiony przełącznikiem pełniącym rolę backup’u – wybór przełącznika backup nie może odbywać się w momencie awarii przełącznika master. |
| Przełącznik musi posiadać dwa wymienne zasilacze AC. Urządzenie musi posiadać co najmniej 2 moduły wentylacji. Zarówno zasilacz, jak i moduł wentylacji muszą posiadać możliwość wymiany podczas pracy urządzenia (hot swap). |
| Przełącznik musi być wyposażony w port konsoli oraz dedykowany interfejs Ethernet do zarządzania OOB (out-of-band). |
| Przełącznik musi być wyposażony w nie mniej niż 20 GB storage oraz 4 GB pamięci DRAM |
| Zarządzanie urządzeniem musi odbywać się za pośrednictwem interfejsu linii komend (CLI), przez port konsoli, telnet, ssh. |
| Wydajność przełączania nie może być niższa niż 1080 Gbps (bidirectional). Przełącznik posiadać możliwość obsługi co najmniej 112 000 adresów MAC. |
| Przełącznik musi obsługiwać ramki Jumbo (9216 bajtów). |
| Przełącznik musi obsługiwać sieci VLAN zgodne z IEEE 802.1q w ilości nie mniejszej niż 4093. |
| Urządzenie musi obsługiwać agregowanie połączeń zgodne z IEEE 802.3ad - nie mniej niż 128 grup LAG, nie mniej niż 16 portów w grupie. |
| Przełącznik musi obsługiwać protokół Spanning Tree i Rapid Spannig Tree, zgodnie z IEEE 802.1D-2004, a także Multiple Spanning Tree zgodnie z IEEE 802.1Q-2003 (nie mniej niż 64 instancje MSTP). |
| Przełącznik musi obsługiwać protokół LLDP oraz LLDP-MED |
| Urządzenie musi posiadać możliwość obsługi 128 000 prefiksów unicast IPv4. |
| Urządzenie musi obsługiwać ruting statyczny |
| Urządzenie musi posiadać możliwość rozbudowy licencji o obsługi protokołu VRRP, protokołów rutingu dynamicznego OSPFv2/v3 oraz rutingu multicast w postaci PIM-SM, PIM-SSM, PIM-DM. Licencja nie jest przedmiotem niniejszego postępowania. |
| Urządzenie musi posiadać możliwość rozbudowy licencji o funkcję MacSec, np. poprzez zastosowanie licencji. Licencja nie jest przedmiotem niniejszego postępowania. |
| Urządzenie musi posiadać możliwość rozbudowy funkcji, np. poprzez zastosowanie licencji, o obsługę protokołów routingu dynamicznego IS-IS, BGP oraz MBGP. Licencja nie jest przedmiotem niniejszego postępowania. |
| Urządzenie musi wspierać EVPN-VXLAN L2 GW w zakresie active-active multi-homing oraz proxy arp i arp suppression. |
| Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym (QoS) w warstwie 2 i 3. Klasyfikacja ruchu musi odbywać się w zależności od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP. Urządzenie musi obsługiwać sprzętowo nie mniej niż 12 kolejek per port fizyczny (8 unicast i 4 multicast). |
| Urządzenie musi obsługiwać mechanizm Weighted Random Early Detection (WRED). |
| Urządzenie musi obsługiwać filtrowanie ruchu co najmniej na poziomie portu i sieci VLAN dla kryteriów z warstw 2-4. W regułach filtrowania ruchu musi być dostępny mechanizm zliczania dla zaakceptowanych lub zablokowanych pakietów. Musi być dostępna funkcja edycji reguł filtrowania ruchu na samym urządzeniu. |
| Przełącznik musi obsługiwać takie mechanizmu bezpieczeństwa jak limitowanie adresów MAC, Dynamic ARP Inspection, DHCP snooping, IP Source Guard. |
| Urządzenie musi obsługiwać protokół SNMP (wersje 2c i 3), oraz grupy RMON 1, 2, 3, 9. Musi być dostępna funkcja kopiowania (mirroring) ruchu na poziomie portu i sieci VLAN. |
| Architektura systemu operacyjnego urządzenia musi posiadać budowę modularną (poszczególne moduły muszą działać w odseparowanych obszarach pamięci), m.in. moduł przekazywania pakietów, odpowiedzialny za przełączanie pakietów musi być oddzielony od modułu rutingu IP, odpowiedzialnego za ustalanie tras rutingu i zarządzanie urządzeniem. |
| Urządzenie musi posiadać system montażowy producenta. |
| Urządzenie musi posiadać dwa kable zasilające AC z wtyczką UPS (C14). |
| Urządzenie musi być wyposażone w we wkładki: 2 szt. 1G Base-T, 22 szt. 10G SR. |
| Urządzenie musi posiadać mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. Pomoc techniczna oraz szkolenia z produktu muszą być dostępne w Polsce. Usługi te świadczone być muszą w języku polskim. |
| Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego przez producenta kanału sprzedaży, na terenie Unii Europejskiej – do oferty należy dołączyć oświadczenie producenta lub autoryzowanego dystrybutora sprzętu i oprogramowania poświadczające pochodzenie sprzętu z autoryzowanego kanału sprzedaży. |
| Wraz z urządzeniem wymagane jest dostarczenie opieki technicznej i gwarancji ważnej przez okres 24 miesięcy. Opieka musi zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu w ciągu 4 dni, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. |
| Wymagane jest także zapewnienie szkolenia z zakresu konfiguracji i zarządzania urządzenia. Szkolenie musi być przeprowadzone dla min. 2 osób w języku polskim i musi obejmować praktyczne ćwiczenia na środowisku Zamawiającego. |
| Wykonawca musi posiadać udokumentowaną aktualną certyfikację z zakresu rozwiązań sieciowych na poziomie min. Certified Network Professional dla dostarczanego przełącznika oraz wykazać posiadanie co najmniej 3 inżynierów legitymujących się wskazaną certyfikacją – załączyć do oferty |
| Wykonawca załączy do oferty certyfikat ISO 27001 na projektowanie sprzedaż i wdrażanie rozwiązań teleinformatycznych, świadczenie usług serwisowych i konsultingowych. |

# **Oprogramowanie klasy SIEM**

|  |
| --- |
| Oprogramowanie musi pozwalać na monitorowanie sieci pod względem incydentów bezpieczeństwa (oprogramowanie typu NSM – Network Security Monitoring). |
| Oprogramowanie musi pozwalać na pełne przechwytywanie pakietów sieciowych oraz wykrywanie sieci i punktów końcowych (endpoints). |
| Przechwytywanie pakietów: Oprogramowanie musi pozwalać na: |
| a) przechwytywanie całego ruchu sieciowego; |
| b) automatyczne czyszczenie starych (archiwalnych) danych przed zapełnieniem zasobów dyskowych; |
| c) Generowanie i przechowywanie logów diagnostycznych; |
| d) przeglądanie pakietów za pomocą kwerend |
| Wykrywanie sieci i punktów końcowych: Oprogramowanie musi pozwalać na: |
| a) wykrywanie złośliwego, anomalnego lub podejrzanego ruchu w sieci na podstawie zestawu reguł (NIDS – Network-based Intrusion Detection System); |
| b) wykrywanie włamań do sieci opartych na analizie ruchu w czasie rzeczywistym; |
| c) wykorzystanie agentów do monitorowania punktów końcowych w sieci (HIDS – Host-based Intrusion Detection System), w tym: |
| a. analiza dzienników systemowych; |
| b. monitorowanie zestawów predefiniowanych zasad; |
| Oprogramowanie musi udostępniać graficzny interfejs WWW, który umożliwia: |
| a) dostęp jedynie zalogowanym użytkownikom (login oraz hasło); |
| b) podstawowy podgląd alertów bezpieczeństwa z systemów NIDS oraz HIDS; |
| c) rozszerzony podgląd alertów z określeniem miejsca zdarzenia oraz dokładnym opisem zdarzenia wraz z jego klasyfikacją; |
| d) wizualizację incydentów bezpieczeństwa w postaci graficznej (wykresów, diagramów); |
| e) interfejs do pełnego przechwytywania pakietów (PCAP – packet capture); |
| f) monitoring zasobów systemowych; |
| g) interfejs do reagowania na incydenty bezpieczeństwa oraz zarządzania sprawami utworzonymi na podstawie alertów; |
| h) interfejs dla narzędzia pozwalającego na operację na danych pochodzących z alertów systemu; |
| i) dostęp publiczny do interfejsu z wykorzystaniem protokołu HTTPS z wykorzystaniem certyfikatu od CA lub lokalny oraz poprzez połączenie tunelowe VPN. |
| Oprogramowanie musi pozwalać na niezależne wykorzystanie przynajmniej dwóch interfejsów sieciowych, w tym: |
| a) interfejs do zarządzania; |
| b) interfejs do nasłuchu ruchu sieciowego. |
| Oprogramowanie musi pozwalać na zarządzanie jego komponentami i przegląd zdarzeń systemowych za pomocą interfejsu konsolowego (CLI). |
| W zakresie zarządzania agentów HIDS oprogramowanie musi pozwalać na: |
| a) instalację agentów na urządzeniach z systemami Windows, MacOS, Linux; |
| b) rejestracja agentów poprzez REST API; |
| c) zarządzanie agentami poprzez interfejs konsolowy; |
| d) zabezpieczenie REST API z wykorzystaniem połączenia HTTPS; |
| e) tworzenie grup agentów i zdalne zarządzanie nimi; |
| f) zdalna aktualizacja agentów. |
| W zakresie HIDS oprogramowanie musi pozwalać na: |
| a) zbieranie danych z dzienników systemowych urządzenia agenta; |
| b) zbieranie informacji o systemie i jego zasobach; |
| c) monitorowanie integralności plików systemowych; |
| d) audyt zmian danych w systemie oraz przez kogo zostały dokonane; |
| f) monitorowanie polityk bezpieczeństwa; |
| g) monitorowanie wykonywanych poleceń systemowych; |
| Oprogramowanie musi pozwalać na wizualizację zbieranych danych o incydentach bezpieczeństwa w postaci wykresów oraz posiadać predefiniowane zestawienia / kokpity (dashboards) i umożliwiać ich tworzenie z poziomu interfejsu graficznego WWW. |
| Oprogramowanie ma pozwalać na zbieranie logów za pomocą protokołu syslog |
| Oprogramowanie musi pozwalać na zdalne dodawanie nowych integracji przetwarzających logi z urządzeń: m.in. Fortinet, Palo Alto, Juniper, PulseSecure |
| Firma wdrażająca w celu ochrony danych zleceniodawcy musi posiadać certyfikację ISO 27001:2022 |
| W celu zagwarantowania jakości usług zleceniobiorca musi wykazać wiedzę z zakresu cyberbezpieczeństwa poprzez odpowiednią certyfikację.  Wykonawca musi posiadać certyfikaty potwierdzające wiedzę i umiejętności oraz kwalifikacje potwierdzone renomowanymi standardami branży cyberbezpieczeństwa oraz następującymi certyfikatami: CISSP, CySA+, Certified Ethical Hacker lub równoważne dla mi jednego specjalisty – załączyć do oferty. |

# **Oprogramowanie do kontroli dostępu NAC**

|  |
| --- |
| Podstawowa funkcjonalność systemu NAC:   * System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych. * System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor) * System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek. * System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji. * System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji. * System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych. * System musi umożliwiać obsługę co najmniej 100 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania. * Licencja ma być zwalniana po rozłączeniu urządzenia końcowego. * System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (Bring Your Own Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia. * System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym: * VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, Citrix XenServer w wersji min 4.x * Maszyny fizyczne - serwery wspierane przez producenta. * System musi posiadać funkcjonalność serwerów: * serwera RADIUS dla infrastruktury sieciowej, * serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+, * serwera SYSLOG, * serwera TACACS+, * serwera Monitoringu, * serwera DHCP, * serwera polityk uwierzytelniania i kontroli dostępu 802.1X, * serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego. * System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP. * System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC. * System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google Workspace, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC. * System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now. * Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email. * System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci. * System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania. * System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników. * System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie. * System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status). * System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania. * Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim). * System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci. * System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP. * System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia. * System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP. * System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP. * Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu. * System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej. * System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP. * System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci. * System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3. * System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+. * System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych. * System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD). * System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook, Google, LinkedIn. * System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS. * System musi posiadać funkcję personalizacji strony gościnnej. * Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon. * Captive Portal musi umożliwiać rejestrację gości potwierdzanych przez konta typu sponsor. * Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS. * Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory. * Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory. * Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu. * Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru. * Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim). * Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP. * Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni. * Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań. * System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP. * System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego. * System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny. * System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176. * System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych. * System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF. * System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc). * System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA. * System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej: * Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności * Czy włączony jest firewall * Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur * Czy jest włączone szyfrowanie dysku systemowego * Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory * Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora * Czy w systemie są uruchomione procesy wskazane przez administratora * Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności * Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem: * Wartości klucza rejestru * Typu wartości: Number, String, Version * System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal. * System musi współpracować z serwerem tokenów. * System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej: * Microsoft Windows * Mac OS * iOS * Android * System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci). * System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory. |
| **Mechanizmy uwierzytelniania:**   * System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS. * System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły: * MAC, * PAP/ASCII, * CHAP, * SNMP, * 802.1X. * wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp. * System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości. * System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych. * System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant). * System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły: * Tożsamość/Urządzenie końcowe, * Grupa tożsamości/urządzeń końcowych, * Parametry urządzeń końcowych, min: system operacyjny, wersja, * Atrybuty Active Directory, * Jednostka organizacyjna tożsamości/urządzeń końcowych, * Urządzenia sieciowe sieci przewodowej, bezprzewodowej, * Grupy urządzeń sieciowych, * Porty urządzeń sieciowych, * Grupy portów urządzeń sieciowych, * Jednostka organizacyjna portów, * Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID), * Data, czas ważności polityki, * Wewnętrzny Captive Portal, * Metoda autoryzacji. * System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks. * System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC. * System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI. * System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli. * System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV. * System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV. * System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach. * System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal. * System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC. * System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC. * System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www. * System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników. * System musi umożliwiać przesyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP. |
| **Obsługa serwerów certyfikatów CA:**   * System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA. * Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności: * możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych. * możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych. * Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol). * usługę OCSP (Online Certificate Status Protocol). |
| **Obsługa serwerów DHCP:**   * System musi posiadać funkcję zintegrowanego serwera DHCP. * System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP. * System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP: * Uruchamianie usługi dla wybranych podsieci, * Przypisanie ustalonego adresu IP dla adresu MAC. * Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci, * Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC, * Możliwość określania braku dostępu dla wybranych adresów MAC, * Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC, * Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP, * Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego, * Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi, * Dokonywanie zmian bez konieczności wyłączania usług. |
| **Obsługa serwerów TACACS+:**  System musi umożliwiać tworzenie grup uprawnień do kontroli dostępów urządzeń sieciowych:   * System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów. * System musi umożliwiać tworzenia haseł administratorom. * System musi umożliwiać tworzenie listy komend uprawnień dla administratorów * System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych. * System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu. * System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory. * System musi wspierać logowanie administratorów za pomocą tokenów OTP. * System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji. |
| **Raportowanie i monitoring:**  System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:   * Monitoring autoryzacji. * Monitoring dla zdarzeń systemowych. * Monitoring dla zdarzeń DHCP. * Monitoring dla tożsamości. * Monitoring dla urządzeń końcowych. * Monitoring dla urządzeń sieciowych. * Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email. * Raport ze zdarzeń logowania z informacją o nadam adresie IP. * Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług. * Raport z logów DHCP z informacją o polityce dostępu logowania do sieci. * System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym. * System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie. * System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku. * System musi wpierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych. * System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja. * System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi. * Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS. * Raport zdarzeń Microsoft Active Directory, minimum: * Logowania, wylogowania z system w tym błędne logowania * Logowania do sieci 802.1X |
| **Alarmy:**   * System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą: * wiadomości e-mail, * Syslog, * notyfikacji systemowych. * Alarmy mogą być generowane w sytuacjach, min: * Ilości obsługiwanych transakcji RADIUS, * Opóźnienie obsługi transkacji RADIUS, * Statusu krytycznego modułów. * System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym: * badanie łączności IP za pomocą ping, traceroute, * tcpdump protokołów RADIUS, TACACS+, * wyszukiwanie zdarzeń RADIUS z uwzględnieniem: * nazwy użytkownika, * adresu MAC, * statusu uwierzytelnienia (udana lub nieudana), * powodu, jeżeli uwierzytelnienie nieudane, * zakresu czasowego, co do dnia, godziny i minuty, * wykonanie zdalnego polecenia na urządzeniu sieciowym. |
| Wymagania dotyczące wdrożenia i harmonogram ramowy:   * Dostawa, instalacja, konfiguracja wstępna i zalicencjonowanie produktu w środowisku klienta. * Podstawowa konfiguracja Systemu NAC (integracja z domeną, konfiguracja urzędu certyfikacji, uruchomienie HA). * Konfiguracja urządzenia firewall (dodatnie VLAN-u gościnnego, ustawienie polityk, etc.). * Import urządzeń końcowych i tożsamości (z AD oraz dostarczonych przez Zamawiającego list). * Integracja dostarczanych urządzeń sieciowych (switche, AP itp.) z Systemem NAC, w ramach funkcjonalności dostępnych na urządzeniach. * Uruchomienie uwierzytelniania w oparciu o 802.1X (EAP-TLS) na urządzeniach końcowych wzorcowych po jednym z każdej serii, testy. * Uruchomienie uwierzytelniania w oparciu o adres MAC w korelacji z innymi możliwościami np. DHCP, SNMP, skan portów, testy. |
| **Szkolenia/warsztaty:**   * Wykonawca zapewni 2-dniowe warsztaty (2 dni x 6h) w zakresie użytkowania i administrowania wdrożonym systemem NAC * Warsztaty zostaną przeprowadzone dla maksymalnie 2 osób i będą uwzględniać informacje z zakresu wdrożonego systemu NAC * Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu NAC * Warsztaty odbędą się w formie zdalnej. * Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej. * Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym |
| **Licencja wsparcia technicznego producenta oprogramowania:**  Wykonawca dostarczy wraz dożywotnią licencją systemu NAC – 24 miesięczną licencję na wsparcie  producenta oprogramowania. Licencja ta powinna obejmować minimum:   * Kontakt mailowy z działem wsparcia technicznego w celu rozwiązania problemów związanych z wdrożeniem lub obsługą systemu NAC * Rozwiązywanie powtarzalnych i rozwiązywalnych problemów związanych z oprogramowaniem a także wsparcie przy identyfikacji problemów trudnych do powtórzenia. * Wsparcie przy rozwiązywaniu problemów oraz pomoc w określaniu parametrów dla konfiguracji oprogramowania oraz wstępne obejścia dla wykrytych problemów. * Dostęp do dokumentacji i instrukcji na stronie internetowej. * Dostęp do aktualizacji i poprawek, które powinny być dostępne z poziomu interfejsu oprogramowania. |

# **Usługi instalacyjne i wdrożeniowe**

|  |
| --- |
| W ramach postępowania Wykonawca zobowiązany jest do: |
| * opracowania projektu wdrożeniowego obejmującego instalację i konfigurację rozwiązań |
| * dostarczenia sprzętu i oprogramowania na wskazanej lokalizacji |
| * przeniesienia własności na urządzenia oraz gwarancje, udostępnienia licencji niezbędnych do uruchomienia sprzętu i oprogramowania, |
| * montażu i konfiguracji urządzeń we wskazanym miejscu w szafie RACK. Wymagane jest aby usługa montażu była wykonana z zachowaniem należytej staranności i przestrzeganiem przepisów BHP. Okablowanie sieciowe powinno być opisane tak aby możliwa była identyfikacja połączeń, |
| * instalacji i konfiguracji dostarczanego oprogramowania w oparciu o projekt wdrożeniowy oraz przygotowanie dokumentacji powdrożeniowej wraz ze schematami graficznymi wdrożonego rozwiązania, |
| * wykonania prac wdrożeniowych obejmujących: * Instalację i aktualizację systemów operacyjnych, firmware poszczególnych urządzeń. * Przygotowanie klastra wysokiej dostępności na bazie dostarczonych systemów operacyjnych, serwerów i macierzy. * Przeniesienie wskazanych na etapie wdrożenia przez Zamawiającego systemów obecnie używanych na klaster wysokiej dostępności. * Instalacja oprogramowania do backup na dostarczonym klastrze, konfiguracja tego oprogramowania do współpracy z dostarczanym deduplikatorem. * Przygotowanie polityk backupu wraz z harmonogramem ich wykonywania w uzgodnieniu z Zamawiającym. * Konfiguracja urządzeń UTM z uwzględnieniem konfiguracji obecnie wykorzystywanych urządzeń dostępowych (adresacje IP, vlany, polityki bezpieczeństwa, vpn itp.) oraz uwzględnienie niezbędnej konfiguracji do prawidłowego działania całego wdrożenia. * Konfiguracja przełącznika niezbędna do prawidłowego działania całego środowiska Zamawiającego, z uwzględnieniem o ile to możliwe redundancji połączeń. * Instalacja oprogramowania typu SIEM i NAC na dostarczonym klastrze konfiguracja do współpracy z infrastrukturą Zamawiającego i w uzgodnieniu z Zamawiającym. |
| * przeprowadzenia szkolenia pracowników w zakresie zarządzania, administrowania i działania w ramach dostarczonych rozwiązań, |
| * zapewnienia pomocy technicznej eksperta, |
| * dostarczenia wszystkich niezbędnych materiałów instalacyjnych (przewodów, wkładek światłowodowych) do realizacji przedmiotu zamówienia |

# **Audyt bezpieczeństwa informacji**

|  |
| --- |
| Przedmiotem zamówienia jest usługa polegająca na przeprowadzeniu audytu zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i Ustawą o Krajowym Systemie Cyberbezpieczeństwa w zakresie jednostek sektora finansów publicznych o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych w szczególności obejmująca weryfikację:   * Wdrożonej dokumentacji dotyczącej Systemu Zarządzania Bezpieczeństwa Informacji, * Zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia, * Utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. * Przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy * Podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, * Bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, * Zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji z uwzględnieniem aspektów związanych z bezpieczeństwem informacji, * Zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami * Ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość * Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie, * Ustalonych zapisów zawieranych w umowach serwisowych gwarantujących odpowiedni poziom bezpieczeństwa informacji, * Ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych * Zapewnienia odpowiedniego określonego przez KRI poziomu bezpieczeństwa w systemach teleinformatycznych * Sposobu postępowania z incydentami związanymi z bezpieczeństwem informacji. * Analiza posiadanej dokumentacji ochrony danych osobowych pod kątem aktualności i zgodności z prawem, * Zbadanie przesłanek legalności przetwarzania danych osobowych i wrażliwych, * Weryfikacja celu, zakresu przetwarzania danych oraz adekwatności do celu przetwarzania. * Weryfikacja procesów przetwarzania danych osobowych oraz określenie konieczności prowadzenia rejestru przetwarzania. * Analiza fizycznych i logicznych zabezpieczeń infrastruktury informatycznej, * Weryfikacja funkcjonalności aplikacji i poziomu ich zabezpieczeń, * Weryfikacja poziomu zabezpieczeń procesów danych osobowych przetwarzanych w formie papierowej, * Weryfikacja poziomu wiedzy i świadomości pracowników w zakresie ochrony danych osobowych, * Weryfikacja zawartych umów pod kątem powierzenia przetwarzania danych osobowych * Rozszerzenie audytu o zagadnienia potrzebne do wypełnienia zał. nr 6 konkursu grantowego – Ankiety Dojrzałości Cyberbezpiczeństwa. |
| Audyt powinien zakończyć się opracowaniem raportu zawierającego wykryte niezgodności oraz dotyczące ich zalecenia oraz wypełnieniem ankiety dojrzałości cyberbezpieczeństwa stanowiącą załącznik do regulaminu konkursu grantowego „Cyberbezpieczny Samorząd” |
| Pozostałe parametry dotyczące audytu przedstawione są poniżej.   * Zasoby: * Liczba Pracowników Urzędu: 59 * Liczba stacji roboczych w Urzędzie: 64 * Liczba serwerów fizycznych z systemem Windows Serwer: 2 * Liczba serwerów wirtualnych z systemem Windows Serwer: 0 * Liczba serwerów fizycznych z systemem Linux: 4 (2x qnap, citrix XEN, XCP-ng) * Liczba serwerów wirtualnych z systemem Linux: 6 * Serwer w chmurze z systemem Windows Serwer: 0 * Serwer w chmurze z systemem Linux: 0 * Audyt należy przeprowadzić w trybie stacjonarnym, w siedzibie. * Wykonawca zobowiązuje się do opracowania Planu audytu zawierającego czynności audytowe * Wykonawca zobowiązany jest do pokrycia wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia, w tym koszty swojego ewentualnego zakwaterowania, dojazdu i wyżywienia. * Wykonawcy ubiegający się o realizację zamówienia powinni posiadać niezbędną wiedzę i doświadczenie oraz dysponować odpowiednimi zasobami umożliwiającymi wykonanie przedmiotu zamówienia. O udział w postępowaniu mogą ubiegać się Wykonawcy, którzy spełniają następujące warunki: * co najmniej jedna osoba z zespołu przeprowadzającego audyt u Zamawiającego musi posiadać certyfikat określony w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999) lub będącego audytorem zewnętrznym systemu zarządzania bezpieczeństwem informacji według normy PN-ISO/IEC 27001 * w okresie dwóch ostatnich lat wykonali (tj. świadczyli, zrealizowali, zakończyli) co najmniej 2 usługi obejmujące swoim zakresem: * audyt bezpieczeństwa informacji zgodnie z wymaganiami SZBI/KRI (audyt SZBI/ KRI), * audyt bezpieczeństwa systemów informatycznych. |
| W związku z koniecznością podpisania z Wykonawcą umowy powierzenia danych, przy ocenie ofert brane będą pod uwagę wyłącznie podmioty spełniające wymogi art. 28 ust.1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.). |
| Wymagania dotyczące zasobów oraz kompetencji wykonawców usług:   * Wykonawca musi posiadać przynajmniej dwuletnie doświadczenie w przeprowadzaniu projektów w obszarze cyberbezpieczeństwa, audytów KRI oraz przedstawić stosowne referencje od podmiotów publicznych. * Osoba przeprowadzająca Audyt musi posiadać przynajmniej jeden z certyfikatów określonych w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (Dz.U.2018 poz. 1999). * Wykonawca powinien posiadać w zespole projektowym wyznaczonym do wykonania zamówienia co najmniej trzy osoby legitymujące się certyfikatami Audytora Wiodącego nomy ISO 27001 zgodnego z akredytacją PCA (Polskie Centrum Akredytacji) w celu zapewnienia zastępowalności w realizacji zadań w projekcie. * Wykonawca powinien wykazać się osobą w zespole projektowym poświadczającą wiedzę: * Dyplom ukończenia studiów podyplomowych z zarządzania cyberbezpieczeństwem. * Certyfikat Auditor wewnętrzny systemu zarządzania ciągłością działania wg ISO 22301:2019 * Zarządzania ryzykiem w Systemie Zarządzania Bezpieczeństwem Informacji (ISO 27005) * Wykonawca załączy do oferty pisemne referencje z min 3 podmiotów publicznych, z których wynika, że przedmiotowa usługa była lub jest realizowana należycie z zakresu opracowania polityki bezpieczeństwa Informacji, szkoleń, audytów bezpieczeństwa. * Wykonawca złoży pisemne referencji potwierdzające realizację projektów w programie Cyfrowa Gmina min 5 podmiotów publicznych. * Wykonawca powinien posiadać kopię polisy odpowiedzialności cywilnej na świadczone obowiązki na kwotę co najmniej 1 000 000 zł. Kopię polisy Wykonawca załącza do oferty * Wykonawca powinien posiadać w zakresie wykonywania szkoleń certyfikat SUS 2.0. lub równoważny, który określa wymagania wobec firm szkoleniowych w zakresie przygotowania, realizacji i ewaluacji oferowanych usług. Kopię certyfikatu wykonawca załącza do oferty. Dodatkowo powinien wykazać wpis do Rejestru Instytucji Szkoleniowych. * Osoby wyznaczone do realizacji projektu powinny być pracownikami Wykonawcy zatrudnionymi na umowę o pracę. Zamawiający zastrzega sobie prawo do wglądu w niniejsze umowy w celu weryfikacji prawidłowości realizacji postanowień zapytania. * Wykonawca zobowiązuje się do wykonania niniejszej usługi za pomocą własnych zasobów. |

# **Przełącznik dostępowy warstwy 2/3 z możliwością zarządzania przez FortiGate 100F**

|  |
| --- |
| Przedmiotem zamówienia jest **dostawa przełącznika dostępowego** warstwy 2/3, przystosowanego do montażu w szafie RACK 19″, **w pełni kompatybilnego z zaporą sieciową FortiGate 100F**, z możliwością **centralnego zarządzania za pośrednictwem FortiLink** (bez konieczności stosowania oddzielnego kontrolera lub systemu zarządzającego). |
| **Kompatybilność** |
| * Urządzenie musi umożliwiać pełną integrację i zarządzanie z poziomu zapory FortiGate 100F w trybie FortiLink. Wymagana zgodność z aktualnymi wersjami FortiOS. |
| **Porty dostępowe** |
| * Minimum 48 portów RJ45 1 GbE (1000BASE-T). |
| **Porty uplink** |
| * Minimum 4 porty SFP+ 10 GbE (10GBASE-X) do połączeń z urządzeniami nadrzędnymi (np. FortiGate 100F lub agregacyjnymi switchami). |
| **Obsługa VLAN** |
| * Minimum 4000 VLAN-ów, zgodność z IEEE 802.1Q. |
| **Agregacja łączy (LAG)** |
| * Obsługa grup łączy LACP (IEEE 802.3ad), minimum 8 grup LAG. |
| **Przepustowość** |
| * Przepustowość przełączania ≥ 170 Gbps. |
| **Bufor pakietów** |
| * Co najmniej 2 MB. |
| **MAC Address Table** |
| * Minimum 32 000 wpisów. |
| **Opóźnienia** |
| * Maksymalne opóźnienie < 1 µs. |
| **Zasilanie** |
| * Urządzenie zasilane sieciowo 230V AC, **bez funkcjonalności PoE**. |
| **Chłodzenie** |
| * Praca w trybie 24/7, aktywne chłodzenie, konstrukcja przystosowana do pracy w środowisku serwerowni. |
| **Wymiary** |
| * Montaż w szafie RACK 19″, wysokość maks. 1 RU. |
| **Zarządzanie** |
| * Możliwość pełnego zarządzania i monitorowania z poziomu FortiGate 100F. * Obsługa protokołów standardowych (np. SNMP, Syslog, RADIUS, TACACS+). |
| **Bezpieczeństwo** |
| * Obsługa ACL, port security, autoryzacja 802.1X. |
| **Oprogramowanie** |
| * Licencja umożliwiająca aktualizacje firmware przez okres minimum 12 miesięcy; możliwość rozszerzenia do 5 lat. |
| **Certyfikaty i zgodność** |
| * **CE,** FCC, RCM, VCCI, BSMI, UL, CB, RoHS2 |
| **Gwarancja i wsparcie** |
| * Minimum 3 lata gwarancji producenta, z możliwością rozszerzenia serwisu i wsparcia technicznego (SLA 8x5 lub równoważne). |