**ZAŁĄCZNIK NR 1**

|  |
| --- |
|  |
| Opis Przedmiotu Zamówienia |
| Oprogramowanie oraz  infrastruktura sprzętowa |

|  |
| --- |
|  |

Spis treści

[UTM Unified Threat Management - klaster firewalli z zaawansowanymi funkcjami bezpieczeństwa 3](#_Toc181036692)

[Serwer - klaster dwóch serwerów pracujących w trybie wysokiej dostępności 21](#_Toc181036693)

[Network Attached Storage NAS - Urządzenie wraz z oprogramowaniem do backupu 32](#_Toc181036694)

[Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1 - Switche Core – 2szt. 38](#_Toc181036695)

[Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2 - Switche dostępowe– 4szt. 41](#_Toc181036696)

[Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 3 - Switche przed klastrem UTM – 2szt. 45](#_Toc181036697)

[Oprogramowanie antywirusowe - Antywirus z XDR dla 50 stanowisk z szyfrowaniem i modułem aktualizacji 47](#_Toc181036698)

[Szkolenia typ 1 - Certyfikowane szkolenie producenta z obsługi programu antywirusowego – 2szt. 47](#_Toc181036699)

[Szkolenia typ 2 - Certyfikowane szkolenie producenta dla administratorów z obsługi firewalla – 2szt. 48](#_Toc181036700)

[Szkolenia typ 3 - Certyfikowane szkolenie producenta z obsługi rozwiązania do backupu – 2szt. 49](#_Toc181036701)

[Usługi informatyczne - Wdrożenie serwerów z migracją oraz z posawieniem systemu logów 49](#_Toc181036702)

# UTM Unified Threat Management - klaster firewalli z zaawansowanymi funkcjami bezpieczeństwa

W ramach dostawy Wykonawca musi dostarczyć klaster firewalli UTM spełniający poniższe wymagania.

Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.

Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania.  Rozwiązanie powinno być wyposażone w moduł kryptoraficzny zgodny ze standardem FIPS 140-2.  Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca)  Rozwiązanie powinno być dostarczone w formie klastra active-passive.  System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej.  Rozwiązanie powinno być wyposażone w wysokowydajny wielordzeniowy procesor x86 (CPU) oraz dodatkowo w procesor (NPU) do akceleracji ruchu dla warstwy aplikacji.  Rozwiązanie musi być wyposażone w co najmniej jeden dysk SSD służący m.in. do przechowywania logów i raportów bezpośrednio na urządzeniu.  Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy.  Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB).  Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie.  Wbudowany port USB umożliwiający podłączenie pamięci flash i przeprowadzenie konfiguracji w trybie Zero Touch.  Możliwość rozbudowy o dodatkowe moduły interfejsów sieciowych.  Rozwiązanie powinno ofertować możliwość zamontowanie redundantnego zasilacza.  Urządzenie musi być wyposażone w wielofunkcyjny wyświetlacz LCD umożliwiający sprawdzenie statusu urządzenia i wykonywanie podstawowych czynności administracyjnych bezpośrednio na urządzeniu  Pamięć operacyjna RAM nie mniej niż (GB): 8  Przestrzeń do przechowywania logów i raportów nie mniej niż (GB): 110  Liczba fizycznych interfejsów Gigabit Ethernet nie mniej niż: 8  Liczba fizycznych interfejsów SFP Fiber: 4  Liczba fizycznych interfejsów SFP+ Fiber: 4  Liczba interfejsów może zostać uzyskana poprzez zastosowanie kart rozszerzających |
| Wydajność | Wydajność Firewall nie mniej niż (Mbps): 29 000  Wydajność Firewall IMIX nie mniej niż (Mbps): 15 000  Wydajność IPS nie mniej niż (Mbps): 6000  Wydajność FW+IPS+AV nie mniej niż (Mbps): 1 200  Wydajność NGFW nie mniej niż (Mbps): 5 000  Liczba równoczesnych połączeń nie mniejsza niż: 6000000  Liczba nowych połączeń na sekundę nie mniejsza niż: 125 000  Wydajność IPsec VPN nie mniej niż (Mbps): 4900  Wydajność dla inspekcji ruchu SSL/TLS nie mniej niż (Mbps): 1000  Liczba równoczesnych połączeń SSL/TLS nie mniejsza niż: 18000  Liczba równoczesnych tuneli SSL VPN nie mniejsza niż: 2300 |
| Zarządzanie | Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym.  Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA).  Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN.  Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter.  Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.  Rozwiązanie powinno oferować wiersz poleceń dostępny z poziomu graficznego interfejsu administraotra, portu konsolowego oraz za pośrednictwem protokołu SSH z uwierzytelnianiem przy użyciu kluczy RSA, DSA lub ECDSA o długości min. 2048 bitów.  Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności.  System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.  System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.  Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).  System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.  Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm).  System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog).  Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej.  System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS).  Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta.  System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpwiednika).  System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia.  System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta, przy czym w podstawowej wersji utrzymywany i udostępniany jest on bezpłatnie i nie wymaga zakupu osobnych subskrypcji.  Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP, via email jak i dodatkowo do centralnego systemu zarządzania w chmurze.  Rozwiązanie powinno oferować wbudowany mechanizm pozwalający na automatyczne tworzenie szyfrowanych hasłem kopii zapasowych konfiguracji w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.  Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.  Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.  Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu licencyjnego a synchronizacja subskrypcji powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.  Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware). Informacja o dostępności nowej wersji powinna pojawiać się w Web GUI.  Producent powinien oferować mechanizm automatycznego łatania wykrytych w oprogramowaniu systemowym podatności przez tzw. hotfixies, przy czym administrator powinien móc funkcjonalność tą wyłączyć.  Rozwiązanie powinno oferować mechanizm szyfrowania danych takich jak loginy, hasła, klucze które przechowywane są w konifiguracji urządzenia. Dane powinny być zabezpieczone dedykowanym kluczem szyfrującym tworzonym na podstawie bezpiecznie składowanego poza urządzeniem hasła.  Rozwiązanie powinno zapewniać możliwość zmiany nazw interfejsów sieciowych. |
| Zapora sieciowa | Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection.  System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6.  Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas.  System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.  System powinien pozwalać na selektywne wyłączanie reguł zapory sieciowej (bez konieczności ich usuwania).  System powinien pozwalać na grupowanie reguł zapory. Wymagana jest funkcjonalność automatycznego wiązania nowotworzonych reguł do właściwych grup na podstawie kryteriów opisujących grupę.  Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.  System ochrony powinien zawierać predefiniowane strefy zapory typu: LAN, WAN, DMZ, VPN.  Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.  System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).  Rozwiązanie powinno oferować narzędzie do symulowanego testu reguł zapory w oparciu o zadane przez administratora kryteria takie jak IP, strefa zapory, użytkownik, dzień, godzina.  System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika. |
| Trasowanie ruchu | Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing.  Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.  Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów.  Rozwiązanie powinno umożliwiać rozkładanie ruchu w oparciu o wagi interfejsów WAN.  Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.  Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).  Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).  Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6. |
| Translacja adresów i portów | Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT.  Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT  Rozwiązanie powinno pozwalać na automatyczne tworzenie reguł NAT typu loopback czy reflexive rule. |
| Kształtowanie pasma i jakość usług | System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji.  Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.  System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.  Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6.  Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet (od 1 Business Critical do 7 Best Effort). |
| Podstawowa ochrona przed atakami DoS i DDoS | System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection). |
| Pozostałe | Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.  Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).  System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.  System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP.  Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).  System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp.  Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd).  Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo).  Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych. |
| Kontroler sieci bezprzewodowej | System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania.  Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Access Point, Wireless Bridge oraz Wireless Repeater.  Uruchomienie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu.  Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej.  Rozgłaszane sieci bezprzewodowe powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując przy tym możliwość izolacji klientów sieci bezprzewodowej.  Rozwiązanie powinno umożliwiać rozgłaszanie wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej (Hide SSID).  Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.  Rozwiązanie powinno zapewniać wsparcie dla uwierzytelniania klientów w oparciu o IEEE 802.1X (RADIUS Authentication).  Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition).  System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów.  Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.  System powinien zapewniać możliwość tworzenia odseparowanej sieci dla gości w wariancie walled garden.  System powinien pozwalać na rozgłaszanie sieci bezprzedowodych w oparciu o harmonogramy czasowe.  Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection). |
| Uwierzytelnianie i obsługa użytkowników | Wymagane uwierzytelniaine użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta.  Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników.  System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+.  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.  System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm).  Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server.  System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android.  Rozwiązanie powinno umożlwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu. |
| Koncentrator VPN | System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2.  System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519).  System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN.  Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN.  Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback.  Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego.  Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth.  Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN.  Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN.  Urządzenie musi obsługiwać połączenia L2TP over IPsec.  Połączenia VPN terminowane muszą być dedykowanej strefie zapory sieciowej. |
| Logowanie i raportowanie | System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym.  System powinien umożliwiać składowanie oraz archiwizację logów.  Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.  Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów.  Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa  System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali.  System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących.  Rozwiązanie powinno umożliwiać wysyłanie raportów via email.  Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV.  Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.  System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.  System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację.  Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.  System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora. |
| Intrusion Prevention System i Advanced Threat Protection | Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur.  Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.  Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS.  Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS.  System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet. |
| Ochrona przed Malware | Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP.  Rozwiążanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania.  Dodatkowo rozwiązanie powinno umożliwiać uruchomienie silnika antywirusowego firmy trzeciej.  Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń.  System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.  Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek.  Rozwiązanie musi przeprowadzać emulację skryptów Java.  Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta.  Rozwiązanie powinno umożliwiać blokowanie potencjalnie niechcianych aplikacji (tzw. Potentially Unwanted Applications - PUAs)  System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates) |
| Inspecja ruchu SSL/TLS | Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów.  Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2.  Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP.  Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443).  Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web.  Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen. |
| Filtr Web | Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron Web oraz umożliwiać dodawanie własnych kategorii stron.  Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy.  Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól.  System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji.  Rozwiązanie powinno umożliwiać filtrowanie stron web analzując ich zawartość wykorzystując tzw. Content Filtering na bazie haseł kluczowych.  Rozwiązanie powinno oferować ochronę przed Pharmingiem. |
| Ochrona przed nieznanymi zagrożeniami | Rozwiązanie klasy Sanbox do ochrony przez zadrożeniami typu Zero-Day.  Rozwiązanie oferujące statyczną i dynamiczną analizę kodu przesyłanego w ramach ruchu web czy email.  Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll.  Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf.  Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf.  Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.  System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS.  System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu.  System zapewniający analizę strukury kodu w tym analizę przeprowadzaną przez mechanizmy głębokiego uczenia maszynowego.  System zapewniający ochronę przed exploitami i złośliwym kodem ransomware.  System badający reputację pliku w zewnętrznych bazach takich jak np.Virustotal.  System powinien oferować szczegółowe raporty dowodzące przeprowadzanie analizy dla w/w mechanizmów. |
| Licencje | Licencje na opisane funkcjonalności muszą być ważne przynajmniej do 10.04.2026 |
| Gwarancja | Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przynajmniej do 10.04.2026 |

# Serwer - klaster dwóch serwerów pracujących w trybie wysokiej dostępności

W ramach dostawy Wykonawca musi dostarczyć klaster serwerów (nodów) ze wspólną przestrzenią dyskową (macierz) spełniający poniższe wymagania.

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla serwera (noda)** |
| **Obudowa** | Obudowa Rack 19” o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. |
| **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera. |
| **Procesor** | Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej:  SPECrate2017\_int\_base wynik min. 131pkt  SPECrate2017\_int\_peak wynik min. 135pkt  SPECrate2017\_fp\_base wynik min. 149pkt  SPECrate2017\_fp\_peak wynik min. 151pkt  Maksymalny TDP dla procesora 125W  Wynik testu musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/> w dniu złożenia oferty.  Do oferty należy załączyć wyniki testów |
| **RAM** | 128GB (w układzie 4x32GB)o częstotliwości taktowania minimum 3200MHz, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczone do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM. |
| **Funkcjonalność pamięci RAM** | ·        Demand Scrubbing,  ·        Patrol Scrubbing,  ·        Permanent Fault Detection (PFD) |
| **Gniazda PCI** | Minimum 5 slotów PCIe x16 generacji 4 |
| **Interfejsy sieciowe/** | Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 2 interfejsy sieciowe 10Gb SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) wraz z wkładkami 10Gb MM LC |
| **Kontroler SAS HBA** | Zainstalowana 4 portowa karta SAS HBA umożliwiająca podłączenie oferowanej macierzy  Ko każdego serwera należy dostarczyć 2 kable SAS 2m umożliwiające podłączenie opisanej dalej macierzy |
| **Dyski twarde** | Zainstalowane 2 dyski M.2 NVMe SSDs o pojemności min. 480GB Hot-Plug z możliwością konfiguracji RAID 1.  Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde |
| **Wbudowane porty** | 3 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim. |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1280x1024 |
| **Zasilacze** | Redundantne, Hot-Plug min. 700W każdy. Klasy Titanium |
| **Bezpieczeństwo** | * Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. * Możliwość wyłączenia w BIOS funkcji przycisku zasilania. * BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła * Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. * Moduł TPM 2.0 * Możliwość dynamicznego włączania i wyłączania portów USB na obudowie – bez potrzeby restartu serwera. * Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem. * Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi 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). |
| **Diagnostyka** | Serwer musi być wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze. |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej; * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); * szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; * wsparcie dla IPv6; * wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; * integracja z Active Directory; * wsparcie dla dynamic DNS; * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. * możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera * możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001, ISO-14001, ISO-50001 - **dołączyć do oferty jako przedmiotowy środek dowodowy**.  Serwer musi posiadać deklarację CE - **dołączyć do oferty jako przedmiotowy środek dowodowy**. |
| **System operacyjny** | Zamawiający wymaga dostarczenia oprogramowania systemowego w najnowszej aktualnej wersji, nieograniczonej czasowo. Licencja musi uprawniać do uruchamiania oprogramowania systemowego (dalej: SSO) w postaci **6** wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji.  Dostarczona licencja musi być kompatybilna z dostarczonym serwerem oraz musi być zgodna z prawami licencyjnymi producenta.  SSO musi posiadać następujące, wbudowane cechy:  a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym,  b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny,  c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania min. 8000 maszyn wirtualnych,  d) 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,  e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy,  f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy,  g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego,  h) możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading),  i) wbudowane wsparcie instalacji i pracy na wolumenach, które:  I. pozwalają na zmianę rozmiaru w czasie pracy systemu,  II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL),  j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość,  k) wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających min. certyfikat FIPS 140-2  l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET,  m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów,  n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych,  o) graficzny interfejs użytkownika,  p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,  q) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play),  s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu,  t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa,  u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,  III. zdalna dystrybucja oprogramowania na stacje robocze,  IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej,  V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  1) dystrybucję certyfikatów poprzez http,  2) konsolidację CA dla wielu lasów domeny,  3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen,  VI. szyfrowanie plików i folderów,  VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec),  VIII. możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów,  IX. serwis udostępniania stron WWW,  X. wsparcie dla protokołu IP w wersji 6 (IPv6),  XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:  1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  2) obsługi ramek typu jumbo frames dla maszyn wirtualnych,  3) obsługi 4-KB sektorów dysków,  4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,  6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model),  v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet,  w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath),  x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego,  y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty,  z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.  **Należy dostarczyć dodatkowo 60 licencji dostępowych USEr CAL na cały Klaster** |
| **Warunki gwarancji** | 1. Minimum 24 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  2. 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.  3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  5. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.  6. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.  7. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  8. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  9. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.  10. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  11. 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.  12. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych – dokumenty potwierdzające należy załączyć do oferty.  13. Firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny link do strony producenta urządzenia z ogólnodostępnym dokumentem np. certyfikat lub oświadczenie, potwierdzającym autoryzację dla firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku braku takiego linku lub ogólnodostępnego dokumentu producenta, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski.  **Wymagane dokumenty i oświadczenia dołączyć do oferty jako przedmiotowy środek dowodowy**  Uwaga! Kryterium punktowane za rozszerzenie gwarancji, wsparcia technicznego i aktualizacyjnego do 60 miesięcy |

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla macierzy** |
| Typ obudowy | Macierz musi być przystosowana do montażu w szafie rack 19”, w oferowanej konfiguracji o wysokość maksymalnie 2U. |
| Przestrzeń dyskowa | Zainstalowane:   1. 2 dyski SSD  1.92TB SSD SAS Read Intensive Hot-Plug 2. 11 dysków HDD  2,4TB SAS 12Gbps 10 tys rpm Hot-Plug |
| Możliwość rozbudowy | Macierz musi obsługiwać (bez wymiany kontrolerów macierzy), co najmniej 264 dyski twarde. |
| Obsługa dysków | 1. Macierz musi mieć możliwość obsługiwania dysków SSD, SAS i Nearline SAS. 2. 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 | 1. 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). 2. Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. 3. 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). 4. Macierz musi umożliwiać obsługę dysków różnej pojemności w ramach grupy dysków. |
| Tryb pracy kontrolerów macierzowych | 1. Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe. 2. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów. |
| Pamięć cache | 1. Macierz musi posiadać minimum sumarycznie 32 GB pamięci cache. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. 2. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. 3. 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 | 1. Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. 2. 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 | 1. Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. 2. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej. |
| Zarządzanie grupami dyskowymi oraz dyskami logicznymi | 1. Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. 2. 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. 3. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Thin Provisioning | 1. Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. 2. 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). 3. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Tiering | 1. Macierz musi posiadać funkcjonalność Tiering między dyskami SSD i SAS i między dyskami SAS i NL SAS. 2. Tiering musi obejmować wszystkie woluminy w danej puli dyskowej. 3. 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 | 1. Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. 2. 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. 3. Macierz musi wspierać minimum 1012 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Wewnętrzne kopie pełne | 1. Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. 2. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia. |
| Migracja danych w obrębie macierzy | 1. 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. 2. 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. |
| Zdalna replikacja danych | 1. Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. 2. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem. |
| Podłączanie zewnętrznych systemów operacyjnych | 1. Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). 2. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, RHEL, SLES, Vmware, Citrix. 3. 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. 4. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie. |
| Redundancja | 1. 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. 2. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap”, a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. 3. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. |
| Dodatkowe wymagania | 1. Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. 2. 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. 3. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie. |
| Warunki gwarancji | 1. Minimum 24 miesiące gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  2. 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.  3. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.  4. Zamawiający oczekuje rozpoczęcia diagnostyki telefonicznej / internetowej już w momencie dokonania zgłoszenia. Certyfikowany Technik wykonawcy / producenta z właściwym zestawem części do naprawy (potwierdzonym na etapie diagnostyki) ma rozpocząć naprawę w siedzibie zamawiającego najpóźniej w następnym dniu roboczym (NBD) od otrzymania zgłoszenia / zakończenia diagnostyki. Naprawa ma się odbywać w siedzibie zamawiającego, chyba, że zamawiający dla danej naprawy zgodzi się na inną formę.  5. Zamawiający oczekuje bezpośredniego dostępu do wykwalifikowanej kadry inżynierów technicznych a w przypadku konieczności eskalacji zgłoszenia serwisowego wyznaczonego Kierownika Eskalacji po stronie wykonawcy.  6. Zamawiający wymaga pojedynczego punktu kontaktu dla całego rozwiązania producenta.  7. Zgłoszenie przyjęte jest potwierdzane przez zespół pomocy technicznej (mail/telefon / aplikacja / portal) przez nadanie unikalnego numeru zgłoszenia pozwalającego na identyfikację zgłoszenia w trakcie realizacji naprawy i po jej zakończeniu.  8. Zamawiający oczekuje możliwości samodzielnego kwalifikowania poziomu ważności naprawy.  9. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji urządzenia.  10. Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.  11. 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.  12. Firma serwisująca musi posiadać ISO 9001 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  13. Firma serwisująca musi posiadać autoryzacje producenta urządzeń – na potwierdzenie należy załączyć ogólnodostępny link do strony producenta urządzenia z ogólnodostępnym dokumentem np. certyfikat lub oświadczenie, potwierdzającym autoryzację firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia. W przypadku braku takiego linku i ogólnodostępnego dokumentu producenta, Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski.  **Uwaga! Kryterium punktowane za rozszerzenie gwarancji, wsparcia technicznego i aktualizacyjnego do 60 miesięcy** |

# Network Attached Storage NAS - Urządzenie wraz z oprogramowaniem do backupu

W ramach dostawy Wykonawca musi dostarczyć rozwiązanie spełniający poniższe wymagania.

Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.

Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.

Wykonawca jest zobowiązany do uruchomienia systemu backupowego i jego skonfigurowania zgodnie z zaleceniami Zamawiającego.

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | ●   System powinien być dostarczony w ramach sprzętowego appliance z zainstalowanymi i skonfigurowanymi wszystkim usługami, niezbędnymi do pracy systemu.  ●   Konsola zarządzająca może być również instalowana w chmurze producenta zlokalizowanej na terenie Polski,  ●   Interfejs systemu dostępny jest w języku:  ○   polskim,  ○   angielskim,  ○   ukraińskim,  ●   System wykonuje kopię własnej bazy danych, która umożliwia odtworzenie wszystkich ustawień i całej konfiguracji, w tym z możliwością odtworzenia w postaci usługi uruchomionej w chmurze producenta zlokalizowanej na terenie Polski,  ●   Oprogramowanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej),  ●   Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania, ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych. |
| Sprzętowe | Obudowa: Rack 1U  Procesor: Intel Xeon E-2336 lub równoważny posiadający taką samą lub wyższą punktację w rankingu benchmark  Pamięć RAM: 16 GB DDR4  Przestrzeń backupowa dostępna przy konfiguracji RAID 5 : min. 24 TB  Osobny dyski SSD min. 2x 240 GB na konsolę zarządzającą  Urządzenie powinno posiadać już zainstalowane dyski oraz skonfigurowany RAID 5 lub 6 i być gotowe do pracy zgodnie z w/w wymaganiami „Ogólne”  Redundantne zasilacze o mocy min.600 W  Interfejsy sieciowe:  - min. 2szt. Ethernet typu 1000BaseT  - min. 1szt. SFP+ |
| Zarządzanie | ●   Zarządzanie całością działania systemu (backup, przywracanie)z poziomu jednej konsoli, dostępnej za pośrednictwem przeglądarki WWW,  ●   Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego,  ●   Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem,  ●   Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem,  ●   Monitorowanie postępu działania zadania,  ●   Posiada system powiadamiania poprzez e-mail bądź Slack o zdarzeniach w następujących przypadkach:  ○   Zadanie zostało zakończone pomyślnie,  ○   Zadanie zostało zakończone z ostrzeżeniami,  ○   Zadanie zostało zakończone z błędem,  ○   Zadanie zostało anulowane,  ○   Zadanie nie zostało uruchomione.  ●   System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego  ●   System umożliwia wysyłanie powiadomień  o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,  ●   Możliwość zdefiniowania okna backupowego dla każdego z zadań,  ●   Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów i innych sekretów, wykorzystywanych przez System,  ●   System pozwala na klonowanie planów kopii zapasowych,  ●   System umożliwia reset hasła administratora w przypadku jego utraty,  ●   Oprogramowanie umożliwia definiowanie retencji według schematów:  ○   GFS(Grandfather-Father-Son),  ○       FIFO(First-In, First-Out).  ●   Oprogramowanie umożliwia tworzenie grup urządzeń,  ●   Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).  ●   System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.:  ○   System Administrator,  ○   Backup operator,  ○   Restore operator,  ○   Viewer.  ●   Administrator Systemu powinien mieć możliwość logowania się z wykorzystaniem kont Google |
| Składowanie danych | ●   Dane są składowane w ramach dostępnej macierzy wymienionej w wymaganiach sprzętowych OPZ  ●   Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako miejsce replikacji danych:  ○   Lokalnie:  ■       Zasób SMB,  ■       Zasób NFS,  ■       Zasób ISCSI,  ■       Zasób S3,  ■       Katalog zabezpieczonego urządzenia.  ○   W chmurze:  ■       Amazon Web Service,  ■       Magazyn zgodny z S3,  ■       Dostarczanej przez producenta.  ●   System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.  ●   System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.  ●   System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych,  ●   System obsługuje mechanizm WORM (Write Once Ready Many) w chmurowych oraz lokalnych repozytoriów kopii, |
| Odtwarzanie | ●   Odtwarzanie granularne:  ○   Pojedynczych plików z kopii obrazu dysku,  ○   Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365.  ●   Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów:  ○   Windows: 7+,  ○   Windows Server: 2008 R2+,  ●   Odtwarzanie Bare Metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.  ●   Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive’a,  ●   Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V.  ●   Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(RAW, VHD, VHDX, VMDK),  ●   Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL),  ●   Odtwarzanie zasobów plikowych z prawami dostępu,  ●   Przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows),  ●   Odtwarzanie danych według harmonogramu,  ●   Przywracanie danych z określonego urządzenia/użytkownika,  ●   Przywracanie kopii z wybranego magazynu.  ●   Przywracanie danych Microsoft 365:  ○   do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku .pst  ○   do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji),  ●   System posiada możliwość nieodwracalnego kasowania danych,  ●   Przywracanie repozytoriów GIT:  ○   Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket/GitLab),  ○   przywracanie między kontami. |
|  | ●   Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych dla:  ○   Systemów operacyjnych:  ■       Alpine 3.10+,  ■       Debian: 9+,  ■       Ubuntu: 16.04+,  ■       Fedora: 29+,  ■       centOS: 7+,  ■       RHEL: 6+,  ■       openSUSE: 15+,  ■       SUSE Enterprise Linux(SLES): 12 SP2+,  ■       macOS: 10.13+,  ■       Windows: 7 i nowsze  ■       Windows Server: 2008 R2 i nowsze  ○   Środowisk wirtualnych:  ■       Hyper-V,  ■       VMware,  ■       Dowolnych innych – agentowo.    ○   Repozytoriów GIT:  ■       GitHub,  ■       Bitbucket  ■       GitLab  ○   Jira Cloud  ●   Wykonywanie pełnych, różnicowych oraz przyrostowych kopii zapasowych dla:  ○   Baz danych**:**  ■       Microsoft SQL,  ■       MySQL,  ■       PostgreSQL,  ■       Firebird,  ■       Oracle  ■       Dowolnych innych przez podpięcie skryptów pre/post.  ●   Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości:  ○   128 bit,  ○   192 bit,  ○   256 bit.  ●   Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów:  ○   ZStandard,  ○   LZ4.  ●   Oprogramowanie umożliwia zarządzanie poziomem kompresji,  ●   System dostarcza agenta backupu w postaci kontenera Docker, umożliwiającego wykonywanie kopii zapasowych z dowolnych środowisk kontenerowych, w tym popularnych rozwiązań NAS,  ●   System dostarcza agenta backupu w postaci instalatora MSI, umożliwiającego masową instalację w systemach Windows z wykorzystaniem narzędzi Active Directory - SCCM oraz GPO  ●   Wykonywanie kopii zapasowej otwartych plików(VSS),  ●   System umożliwia uruchamianie skryptów przed i po backupie,  ●   System umożliwia uruchamianie skryptów po wykonaniu migawki VSS,  ●   System umożliwia wykonywanie spójnej kopii danych pracujących aplikacji na urządzeniach z systemem Windows oraz wspieranych środowiskach wirtualnych,  ●   System pobiera jedynie zmodyfikowane bloki danych podczas przyrostowej i różnicowej kopii maszyn wirtualnych VMware,  ●   System umożliwia wykonywanie kopii maszyn wirtualnych VMware z zastosowanie zaawansowanych trybów transportu (HotAdd, LAN, SAN), w tym metodą LAN-Free,  ●   System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów,  ●   Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT,  ●   Backup plikowy,  ●   Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe,  ●   Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia,  ●   Oprogramowanie pozwala na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej,  ●   Oprogramowanie pozwala na backup zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption |
| GIT | ●   Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych),  ●   Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki). |
| Licencjonowanie | ●   Licencje powinny pozwalać na zabezpieczenie:  ○   Nielimitowanej ilości maszyn wirtualnych  ○   Nielimitowanej ilości serwerów fizycznych  ○   Nielimitowanej ilości stacji roboczych  ○   Licencje powinny być dostępne w opcji wieczystej. Wsparcie techniczne nie powinno być wymagane dla poprawnego działania systemu |
| Wsparcie techniczne | ○   Wsparcie techniczne producenta świadczone przynajmniej do 10.04.2026  ○   Wsparcie świadczone jest w języku polskim przez producenta,  ○   Dostęp do aktualizacji oprogramowania,  ○   Możliwość korzystanie z połączeń zdalnych producenta, systemu ticketowego oraz wsparcia telefonicznego,  ○   Obowiązuje przez okres analogicznie do długości wsparcia warstwy sprzętowej. |
| Gwarancja sprzętowa | Minimum 24 miesiące gwarancji producenta.  Uszkodzone dyski pozostają własnością Zamawiającego |

# Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 1 - Switche Core – 2szt.

W ramach dostawy Wykonawca musi dostarczyć klaster dwóch przełączników spełniający poniższe wymagania.

Dostarczone rozwiązane należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego oprogramowaniem i sprzętem.

Dostarczone rozwiązanie musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.

|  |  |
| --- | --- |
| Nazwa parametru | Minimalna wartość parametru |
| Ogólne | • Ilość portów: minimum 8 portów 10Gb SFP+ oraz minimum 8 portów 10GBaseT  • Chłodzenie od przedu do tyłu obudowy  • Tablica MAC min. 16K  • Tablica ARP/NDP min. 888  • Bufor 16Mb  • MTBF min. 195000 godzin  • Port USB  • Port zarządzania Out-of-band  • CPU min 800 Mhz  • Minimum 1GB RAM  • Minimum 256MB Flash |
| Wydajność | • Wydajność min. 350 Mpps  • Przepustowość min. 480 Gbps |
| Zarządzanie | * Web GUI * HTTPs * CLI * Telnet * SSH * SNMP |
| Protokoły i funkcjonalności | * MIB RSPAN * Radius * TACACS+ * DiffServ * Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram * IPv4/IPv6 Multicast filtering * IGMPv3 MLDv2 Snooping * ASM & SSM * IGMPv1,v2 Querier * Auto-VoIP * Auto-iSCSI * Policy-based routing (PBR) * LLDP-MED * Spanning Tree * Green Ethernet * STP * MTP * RSTP * PV(R)STP * BPDU/STRG Root Guard * EEE (802.3az) * GVRP/GMRP * Q in Q, * Private VLAN * DOT1X * MAB * Captive Portal * DHCP Snooping * Dynamic ARP * Inspection * IP Source Guard * Min ilość obsługiwanych VLAN 4K * DHCP Server min 2K rezerwacji * sFlow * Ilość interfejsów IP 128 * Double VLAN Tagging (QoQ) * Yes * PIM-DM (Multicast Routing - dense mode) * PIM-DM (IPv6) * PIM-SM (Multicast Routing - sparse mode) * PIM-SM (IPv6) * RIPv1 * RIPv2 * OSPFv2 * RFC 2328 * RFC 1583 * OSPFv3 * OSPFv2 min. sąsiadów 400 * OSPFv3 min. sąsiadów 400 * OSPFv3 min. sąsiadów na interfejs 100 * UDLD * LLPF * DHCPv6 Snooping * wysyłanie alertów na email * MMRP * Ilość ACL min. 100 * Ilość reguł na listę min. 1023 na wejściu i 511 na wyjściu |
| Stakowanie | * Minimalna ilość przełączników w stosie: 8 * Możliwość łączenia w stos przełączników z dominującymi portami 10Gb/s oraz 1Gb/s * Możliwość łączenia w stos za pomocą interfejsów 10Gb/s * Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh * Non-stop forwarding (NSF) * Distributed Link Aggregation (LAGs across the stack) |
| Gwarancja sprzętowa | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie minimum door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |

# Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 2 - Switche dostępowe– 4szt.

|  |  |
| --- | --- |
| Nazwa parametru | Minimalna wartość parametru |
| Charakterystyka sprzętowa | 24 x 1Gb Base-T IEEE 802.3ab  Porty muszą wspierać standard IEEE 802.3x Flow Control dla trybu Full-Duplex oraz Back Pressure dla trybu Half-Duplex i automatyczne krosowanie (Auto MDI/MDI-X).  Musi istnieć możliwość zmiany prędkości i dupleksu każdego portu i wyłączenia trybu FlowControl dla każdego portu.  4 x SFP+ IEEE 802.3ae/802.3ae. Porty SFP+ muszą obsługiwać również moduły SFP 1000Base-X IEEE 802.3z;  Konsola szeregowa RS-232.  Łączenie urządzeń w stosy o wielkości co najmniej 6 jednostek. Awaria żadnego pojedynczego urządzenia nie może spowodować przerwania pracy stosu. Praca w topologii pierścienia. Przepustowość magistrali stosu co najmniej 40 Gb/s. Port-Channel oraz Mirroring ruchu przy użyciu dowolnych portów w stosie.  Zasilanie AC 230V.  Pojemność przełączania nie mniej, niż 128 Gb/s. Wydajność przełączania nie mniej niż 95 Mb/s.  Architektura nieblokującą (wire-speed).  Pojemność tablicy MAC nie mniej, niż 16K. Możliwość wprowadzenia co najmniej 510 wpisów statycznych.  Ilość RAM nie mniej, niż 256 MB. Pamięć Flash - nie mniej niż 32 MB.  Obsługa ramek Jumbo o rozmiarze co najmniej 9210 B.  Bufor pakietów nie mniej, niż 1,5 MB.  Temperatura pracy w zakresie co najmniej od -5C do 50 stopni Celsjusza.  MTBF > 500000 godzin.  Obudowa urządzenia powinna być wyposażona w mocowanie umożliwiające przypięcie zabezpieczenia fizycznego typu Kensington Lock. |
| Funkcjonalność warstwy 2 | IGMP Snooping v3 - obsługa nie mniej, niż 510 grup multicast w tym co najmniej 256 grup statycznych.  MLD Snooping v2 - obsługa nie mniej, niż 31 grup multicast w tym co najmniej 31 grup statycznych.  IEEE 802.1D, 802.1w, 802.1s (co najmniej 16 instancji). Funkcja 802.1Q Restricted Role oraz 802.1Q Restricted TCN.  Wykrywanie pętli w L2 dla przyłączonych urządzeń bez protokołu rodziny STP.  Tworzenie interfejsów Port-Channel - nie mniej niż 8 portów na grupę oraz 32 grup na urządzenie z obsługą LACP.  LLDP (802.1AB) oraz LLDP-MED.  ERPS (ITU-T G.8032) w wersji co najmniej 1. Jednoczesna obsługa co najmniej 1 pierścieni.  DHCP Relay w tym opcji 60 i 61 oraz opcji 82, DHCP Local Relay + opcja 82. DHCP Relay dla IPv6.  Port monitoring/mirroring/span. Możliwość monitorowania tylko wybranego ruchu. |
| Obsługa sieci VLAN | 802.1Q VLAN, co najmniej 4094, 802.1v GVRP.  Przełącznik powinien umożliwiać automatyczne przypisywanie urządzeń monitoringu wizyjnego do specjalnie wydzielonej w tym celu sieci VLAN.  Powinna być możliwość tworzenia sieci VLAN w oparciu o adresy MAC urządzeń. Urządzenie powinno akceptować co najmniej 1020 wpisów MAC dla takiej sieci VLAN.  Urządzenie powinno także umożliwiać tworzenie asymetrycznych sieci VLAN. |
| Funkcjonalność warstwy 3 | Przełącznik musi mieć możliwość utworzenia wielu interfejsów IPv4 na urządzeniu - co najmniej 16 takich interfejsów.  Przełącznik musi posiadać funkcjonalność Gratuitous ARP.  Przełącznik powinien także umożliwiać przekierowanie ruchu UDP na wskazany adres IP w sieci.  Musi być możliwe uruchomienie na urządzeniu serwera DHCP przydzielającego minimum 10 pule adresów IP oraz wspierającego protokół IPv6 przydzielającego minimum 16 pule adresów IP.  Urządzenie powinno posiadać tablicę ARP o wielkości co najmniej 0,5K wpisów oraz umożliwiać wprowadzenie co najmniej 256 wpisów statycznych.  Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 510 tras routingu dla IPv4 do maszyn znajdujących się na bezpośrednio przyłączonych do urządzenia podsieciach oraz 256 takich tras dla IPv6.  Platforma sprzętowa powinna umożliwiać przechowywanie co najmniej 60 tras routingu dla IPv4 do maszyn znajdujących się wewnątrz sieci oraz 32 takich tras dla IPv6.  Urządzenie musi umożliwiać zdefiniowanie statycznych tras routingu dla IPv4 (co najmniej 60 takich tras) oraz dla IPv6 (co najmniej 30 tras).  Urządzenie musi być wyposażone w funkcję Floating Static Route (tworzenie zapasowych domyślnych/statycznych tras routingu dla danej podsieci docelowej) dla IPv4.  Urządzenie powinno wspierać funkcję IPv6 Neighbor Discovery. |
| Quality of Service (QoS) | Przełącznik powinien obsługiwać funkcjonalność QoS i posiadać co najmniej 8 kolejek sprzętowych na każdym porcie fizycznym. Klasyfikacja ruchu do odpowiednich kolejek powinna odbywać się na bazie co najmniej: wejściowego portu fizycznego przełącznika, sieci VLAN, adresu MAC, pola EtherType, adresu IP, pola DSCP, typu protokołu, portu TCP/UDP, klasy ruchu IPv6, etykiety ruchu IPv6.  Urządzenie powinno umożliwiać mapowanie wartości pola DSCP w pakiecie IP do odpowiednich klas obsługi ruchu, WRR, WDRR.  Przełącznik powinien umożliwiać ograniczenie pasma dla ruchu wychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s.  Urządzenie powinno także umożliwiać limitowanie pasma dla ruchu przychodzącego na każdym porcie z granulacją co najwyżej 64 kb/s. |
| Filtrowanie ruchu | Urządzenie powinno posiadać możliwość filtrowania ruchu w oparciu co najmniej o informacje takie, jak: port przełącznika, adres MAC, sieć VLAN, priorytet 802.1p, adres IP, zawartość pola DSCP, typ protokołu, port TCP/UDP, klasę ruchu IPv6, etykietę ruchu IPv6 i mieć możliwość uruchamiania reguł ACL wg kalendarza.  Przełącznik powinien mieć możliwość definiowania reguł ACL na poziomie sieci VLAN. |
| Funkcje bezpieczeństwa | Przełącznik powinien być wyposażony w funkcjonalność umożliwiającą ograniczenie liczby adresów MAC na pojedynczym porcie fizycznym przełącznika oraz "zatrzaśnięcie" na nim określonych adresów MAC i powinien obsługiwać co najmniej 120 takich adresów MAC na pojedynczym porcie fizycznym. Funkcjonalność powinna umożliwiać wyłączenie portu po przekroczeniu zdefiniowanej liczby adresów MAC obecnych na porcie.  Urządzenie powinno umożliwiać uwierzytelnianie przyłączonych użytkowników za pomocą protokołu 802.1X współpracującego z funkcjonalnością umożliwiającą przyznanie dostępu do ograniczonych zasobów w przypadku, gdy użytkownik nie jest uwierzytelniony.  Funkcjonalność 802.1X musi umożliwiać niezależne uwierzytelnianie wielu użytkowników znajdujących się na pojedynczym porcie fizycznym przełącznika.  Urządzenie musi umożliwiać przypisywanie co najmniej następujących atrybutów otrzymanych z serwera RADIUS: VLAN, priorytet 802.1p, przepustowość portu, reguły ACL.  Urządzenie musi wspierać funkcję umożliwiającą zmianę przypisanych z serwera RADIUS uprawnień bez rozłączania ponownego uwierzytelniania przyłączonego klienta.  Przełącznik musi umożliwiać uwierzytelnianie użytkowników w oparciu o portal WWW z możliwością przypisania użytkownika do wskazanej sieci VLAN. Funkcjonalność ta musi działać również dla adresów IPv6.  Urządzenie musi również umożliwiać uwierzytelnianie użytkowników w oparciu o adres MAC z możliwością przypisania użytkownika do wskazanej sieci VLAN.  Musi istnieć możliwość alternatywnego uwierzytelniania za pomocą więcej, niż jednego agenta uwierzytelniania.  Przełącznik musi realizować funkcjonalność filtrowania ruchu od klientów, którzy posiadają nieodpowiednią parę adresów IP-MAC (co najmniej 250 powiązań IP-MAC na urządzenie), jak również z możliwością dynamicznego tworzenia powiązań IP-MAC na bazie informacji pobranych z serwera DHCP i możliwością inspekcji zawartości pakietów ARP. Funkcja IP-MAC binding musi współpracować z protokołem IPv6.  Przełącznik powinien również posiadać funkcjonalność umożliwiającą realizację komunikacji z jednym lub więcej portów wspólnych (np. portów do których podłączony jest router, serwery wydruku itp.).  Urządzenie powinno posiadać funkcjonalność niedopuszczania do sieci nieautoryzowanych przez administratora serwerów DHCP.  Przełącznik powinien mieć możliwość definiowania globalnie dla urządzenia adresów MAC, z/do których ruch nie będzie obsługiwany.  Urządzenie powinno posiadać funkcjonalność zapobiegającą atakom ARP Spoofing przez użytkowników sieci.  Urządzenie powinno posiadać funkcjonalność zapobiegania atakom BPDU.  Urządzenie powinno posiadać funkcjonalność zapobiegania atakom Denial of Service.  Przełącznik powinien posiadać możliwość limitowania Unknown Unicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Multicast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), Broadcast (z krokiem minimalnym co najwyżej 64Kbps i 2pps), a także umożliwiać automatyczne wyłączenie portu w przypadku długotrwałej burzy oraz jego ponowne włączenie po ustalonym czasie.  Przełącznik powinien posiadać mechanizm ochrony procesora przed jego przeciążeniem dużą liczbą pakietów Broadcast/Multicast/Unicast. |
| Zarządzanie | Powinna istnieć możliwość konfiguracji uwierzytelniania dostępu do urządzenia na zewnętrznym serwerze RADIUS i TACACS+.  Grupa urządzeń połączonych w stos powinna być zarządzana poprzez jeden adres IP.  Urządzenie powinno wspierać protokół umożliwiający zdalne wykrywania urządzenia w sieci poprzez dedykowaną do tego celu aplikację producenta przełącznika i umożliwiać co najmniej: zmianę adresu IP urządzenia.  Lokalne zarządzanie urządzeniem powinno odbywać się przez: przeglądarkę internetową - również poprzez adres IPv6, Telnet (co najmniej 4 sesji jednoczesnych) - również poprzez adres IPv6, SSH - również poprzez adres IPv6, konsolę lokalną. Zarządzanie przez interfejs tekstowy musi umożliwiać wprowadzanie poleceń. Niedopuszczalna jest konfiguracja oparta o wybór z menu. Interfejs tekstowy musi zapewniać konfigurację wszystkich funkcjonalności urządzenia.  W przypadku zarządzania przez interfejs WWW musi być możliwość szyfrowania połączenia co najmniej protokołem SSLv3.  Urządzenie powinno posiadać możliwość wykrywania urządzeń zgodnych z protokołem ONVIF oraz prezentować informacje o rzeczywistym stanie tych urządzeń.  Urządzenie musi obsługiwać protokół zarządzania SNMPv2, v3 - również poprzez adres IPv6.  Przełącznik musi umożliwiać monitorowanie zdalne protokołem RMON i obsługiwać protokół sFlow.  Przełącznik musi obsługiwać także cyfrową diagnostykę parametrów pracy modułów światłowodowych, zgodną z SFF-8472, umożliwiającą przynajmniej: pomiar prądu wzmacniacza, pomiar mocy nadajnika i odbiornika, pomiar temperatury modułu oraz pomiar zasilania modułu.  Urządzenie musi posiadać wbudowanego klienta DHCP oraz umożliwiać automatyczne pobieranie konfiguracji z zewnętrznego serwera TFTP podczas uruchamiania urządzenia.  Przełącznik musi posiadać możliwość lokalnego rozwiązywania FQDN na adres IP, co pozwala na wykonywanie poleceń typu ping/traceroute/tftp/telnet dla nazwy FQDN.  Przełącznik musi posiadać możliwość synchronizacji swojego zegara systemowego z zewnętrznym źródłem czasu także przy użyciu protokołu IPv6.  Zapisywanie logów generowanych przez urządzenie musi być możliwe na zewnętrznym serwerze logów - również poprzez adres IPv6.  Urządzenie powinno posiadać możliwość wysyłania i pobierania konfiguracji z serwera TFTP w sieci.  Przełącznik musi umożliwiać wykonywanie polecenia traceroute z poziomu jego interfejsu zarządzającego.  Urządzenie powinno posiadać możliwość wykonywania polecenia ping z poziomu interfejsu zarządzającego - również poprzez adres IPv6, a także umożliwiać przeglądanie tablicy adresów MAC.  Powinna istnieć możliwość uruchomienia diagnostyki okablowania z poziomu interfejsu zarządzającego urządzenia. Test powinien dokonywać co najmniej pomiaru długości kabla oraz ciągłości połączenia.  Interfejs zarządzający musi umożliwiać wprowadzenie tekstowego opisu dla każdego z portów fizycznych urządzenia.  Urządzenie powinno być w stanie wysyłać powiadomienia SNMP (tzw. SNMP Traps) w przypadku pojawienia się w sieci nowego adresu MAC.  Wymagana jest funkcjonalność umożliwiająca logowanie wydanych poleceń konfiguracyjnych wraz z informacją o koncie, z jakiego polecenie zostało wydane.  Urządzenie powinno umożliwiać przechowywanie wielu wersji firmware.  Przełącznik powinien być wyposażony w pamięć Flash umożliwiającą przechowywanie dowolnej liczby plików.  Urządzenie powinno wspierać standard 802.3az (Energy Efficient Ethernet).  Przełącznik powinien umożliwić zmniejszenie pobieranej mocy poprzez wykrywanie aktywności linku na portach, a także administracyjnego wyłączenia wskaźników LED na portach, wyłączenie wskaźników LED na portach w zdefiniowanych interwałach czasowych, wyłączenie portów przełącznika w zdefiniowanych interwałach czasowych oraz wyłączenie wszystkich funkcji sieciowych urządzenia w zdefiniowanych interwałach czasowych. |
| Aktualizacje | Do urządzenia powinny być dostępne bezpłatne aktualizacje oprogramowania. |
| Gwarancja sprzętowa | Wymaga się aby urządzenie było objęte ograniczoną wieczystą gwarancją (do 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie minimum door-to-door przez serwis producenta. Urządzenie powinno być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez okres gwarancji. |

# Zarządzalne urządzenia sieciowe z obsługą VLAN, MACsec, standardu 802.1X typ 3 - Switche przed klastrem UTM – 2szt.

|  |  |
| --- | --- |
| Nazwa parametru | Minimalna wartość parametru |
| Ogólne cechy sprzętowe | Urządzenie musi być wyposażone w min. 16 portów SFP+  Porty SFP+ muszą obsługiwać wkładki o prędkości zarówno 1Gbps jak i 10Gbps  Urządzenie musi być wyposażone w port konsoli umożliwiający zarządzanie urządzeniem z poziomu linii komend  Dopuszczane są jedynie urządzenia w architekturze nieblokującej pracujące w trybie store-and-forward  Rozmiar tablicy adresów MAC urządzenia min. 32K  Min. przepustowość urządzenia – 320 Gbps  Min. szybkość przekierowań pakietów - 238 Mpps  Pobór mocy urządzenia nie może przekraczać 50W  Przełącznik musi być w formacie 1U umożliwiającym jego montaż w standardowej szafie 19” oraz posiadać w zestawie odpowiednie uchwyty montażowe  Głębokość urządzenia nie może przekraczać 250 mm |
| Standardy | Urządzenie musi spełniać następujące standardy:   * 802.3z * 802.3ae * 802.3x * 802.3ad * 802.1ab * 802.1D * 802.1w * 802.1s * 802.1p * 802.1q |
| Funkcjonalności | Wymaga się, aby urządzenie posiadało następujące funkcjonalności:   * Zarządzanie za pomocą przeglądarki poprzez interfejs http/https * Z poziomu CLI (Telnet, SSH, port konsoli) musi być możliwa pełna konfiguracja urządzenia * Urządzenie musi mieć obsługiwać możliwość adopcji przez zewnętrzny kontroler w celu scentralizowanego zarządzania * Obsługę stosu IPv4 i IPv6 * Funkcję wykrywania pętli * Funkcję izolacji portów * Funkcję agregacji portów z wykorzystaniem protokołu LACP * Obsługę protokołu LLDP/LLDP-MED * Funkcję DHCP Snooping zarówno dla IPv4 jak i IPv6 * Funkcję umożliwiającą powiązanie adresu IP z adresem MAC (zarówno dla IPv4 jak i IPv6) * Obsługę protokołu drzewa rozpinającego (STP/RSTP/MSTP) * Obsługę 4K identyfikatorów VLAN * Funkcję umożliwiającą automatyczne przypisywanie wyznaczonych urządzeń do konkretnej sieci VLAN (MAC VLAN) * IGMP Snooping oraz MLD Snooping * Obsługę min. 900 grup multicastowych jednocześnie * MVR * Obsługę routingu statycznego i/lub dynamicznego * Możliwość konfiguracji co najmniej 16 interfejsów IP * Obsługę min 40 tras statycznych dla funkcji routingu statycznego * Obsługę AAA z wykorzystaniem mechanizmów Radius oraz TACACS+ * Uwierzytelnianie użytkowników z wykorzystaniem 802.1X w oparciu o adres MAC urządzenia * Obsługę list kontroli dostępu (ACL) * Obsługę SNMP w wersjach v1/v2c/v3 * Obsługę grup RMON 1,2,3,9) |
| Dodatkowe wymagania | Urządzenia maja być wyposażone niezbędne do realizacji połączeń wkładki 1/10Gb SFP+ MM jak i ewentualnie 1/10Gb BaseT (Rj-45) niezbędne do realizacji redundantnych połączeń |
| Gwarancje i certyfikaty | Urządzenie musi posiadać certyfikację CE  Gwarancja na urządzenie musi wynosić min. 5 lat  Urządzenie musi pochodzić z polskiego autoryzowanego kanału dystrybucyjnego producenta |

# Oprogramowanie antywirusowe - Antywirus z XDR dla 50 stanowisk z szyfrowaniem i modułem aktualizacji

Zamawiający oczekuje rozszerzenia wsparcia technicznego i aktualizacyjnego na kolejny okres do posiadanych rozwiązań Bitdefender zgodnie z opisanymi poniżej wymaganiami. Obecne licencję kończą się 2025-05-11.

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | Wymaga się przedłużenia i rozszerzenia aktualnego kontraktu Bitdefender GravityZone Business Security o numerze seryjnym: A9WZTTVSDUB4 o funkcjonalności:  - EDR, czyli podniesienie do produktu Bitdefender GravityZone Business Security Enterprise (Ultra)  - Bitdefender GravityZone Patch Management, - Bitdefender GravityZone Full Disk Encryption Dodatkowo zamawiający wymaga przedłużenia rozszerzonego kontraktu o okres minimum 12 miesięcy od daty końca aktualnej licencji z ochroną na minimum 50 urządzeń. Dopuszcza się dostawę nowych kluczy z zachowaniem minimalnych dat końca licencji. |

# Szkolenia typ 1 - Certyfikowane szkolenie producenta z obsługi programu antywirusowego – 2szt.

Zamawiający wymaga przeszkolenia z obsługi programu antywirusowego w języku polskim przez minimum 4h. Szkolenie musi zakończyć się certyfikatem wystawionym przez oficjalnego dystrybutora marki Bitdefender na rynek Polski.  
**Szkolenie musi obejmować:**

* Omówienie systemu Bitdefender GravityZone
* Omówienie licencjonowania oraz różnic pomiędzy wersjami
* Tworzenie dostępu do konsoli w wersji cloud
* Instalacja wersji on-premise i rejestracja klucza licencyjnego
* Instalacja serwera bezpieczeństwa
* Tworzenie pakietów instalacyjnych i ich wdrożenie ręczne oraz zdalne na systemach Windows oraz ręczne na systemach Linux
* Tworzenie paczek .msi
* Konfiguracja szablonów polityk bezpieczeństwa wraz z omówieniem występujących opcji, zwróceniem uwagi na najważniejsze ustawienia pod kątem stacji roboczych i serwerów
* Konfiguracja modułu Antymalware
* Konfiguracja reguł Zapory sieciowej
* Konfiguracja blokowania stron internetowych
* Konfiguracja i blokowanie urządzeń podłączanych do komputerów
* Obsługa systemu EDR
* Obsługa Analizatora Sandbox
* Wyjaśnienie działania funkcji Zarządzanie Ryzykiem
* Konfiguracja powiadomień i raportów
* Rozwiązywanie podstawowych problemów przy administracji

# Szkolenia typ 2 - Certyfikowane szkolenie producenta dla administratorów z obsługi firewalla – 2szt.

1. Szkolenie z dostarczonego systemu kopii zapasowej:
2. Szkolenie musi zostać przeprowadzone w formie zdalnej lub na miejscu w wyznaczonym centrum szkoleniowym w języku polskim.
3. Szkolenie musi zostać przeprowadzone przez certyfikowanego trenera oferowanego rozwiązania klasy firewall
4. Szkolenie musi zakończyć się imiennym certyfikatem akredytowanym przez producenta oficjalnego rozwiązania
5. Szkolenie musi trwać minimum 3 dni
6. Zakres szkolenia:

· Rozpoznawania najważniejszych funkcjonalności i wykorzystanie ich do obrony przed zagrożeniami   
· Wykonywania typowych zadań konfiguracyjnych

· Wykonywania kopii i odzyskiwanie konfiguracji   
· Codziennej pracy z urządzeniem   
· Wyświetlania, zarządzania i analizowania logów i raportów   
· Podstawowej diagnostyki i metod rozwiązywania problemów

# Szkolenia typ 3 - Certyfikowane szkolenie producenta z obsługi rozwiązania do backupu – 2szt.

1. Szkolenie z dostarczonego systemu kopii zapasowej:
2. Szkolenie musi zostać przeprowadzone w formie zdalnej w języku polskim.
3. Szkolenie jest realizowane bezpośrednio przez producenta oferowanego systemu backupowego.
4. Szkolenie musi zostać przeprowadzone przez dedykowanego inżyniera producenta systemu backupowego.
5. Szkolenie musi zakończyć się imiennym certyfikatem
6. Szkolenie musi trwać minimum 8 godzin.

# Usługi informatyczne - Wdrożenie serwerów z migracją oraz z postawieniem systemu logów

Dostarczone rozwiązania należy odpowiednio skonfigurować i dokonać jego integracji z posiadanym przez Zamawiającego środowiskiem sieciowo-serwerowym.

Dostarczone rozwiązania musi zostać zainstalowane w infrastrukturze Zamawiającego zgodnie z najlepszymi praktykami i wszystkimi niezbędnymi do wykonania konfiguracjami które to wynikną w czasie jego implementacji na infrastrukturze Zamawiającego.

W ramach dostawy Wykonawca jest zobowiązany do migracji obecnego środowiska Zamawiającego na dostarczony klaster z punktu 2 oraz migracji ustawień sieciowych na klaster UTM z pkt 1.

Dodatkowo na dostarczonym klastrze serwerów należy zainstalować i skonfigurować opisane rozwiązanie do zbierania LOGów

|  |  |
| --- | --- |
| Nazwa parametru | **Minimalne wymagania dla systemu logów** |
| Ogólne | 1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:    1. System operacyjny powinien być na licencji Open Source.    2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego fizyczny serwer będący na wyposażeniu Zamawiającego wirtualna maszyna w środowisku Hyper-V.    3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source    4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach min. 8 vCPU, pamięć RAM 16 GB oraz przestrzeń dyskową 4TB.    5. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.    6. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.    7. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów oraz ich import jak i eksport.    8. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trypie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.    9. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.    10. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów). 2. W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:    1. Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualnej.    2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca zaproponuje rozwiązanie pozwalające na uspójnienie zegarów czasów sieci Zamawiającego.    3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.    4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.    5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły integrację z dostarczonymi rozwiązaniami oraz stacjami roboczymi i serwerami w środowisku zamawiającego    6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.    7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.    8. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.    9. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.    10. Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami. |