**Załącznik nr 12 do SWZ**

***Parametry minimalne sprzętu i oprogramowania***

Spis treści

[1 Rozbudowa serwera aplikacyjnego 3](#_Toc184565442)

[2 Centralny UPS 10kVA 7](#_Toc184565443)

[3 Urządzenie UTM 9](#_Toc184565444)

[4 Serwer NAS klasy korporacyjnej 14](#_Toc184565445)

[5 Dostarczenie i wdrożenie narzędzi klasy EDR 15](#_Toc184565446)

[6 Switch 10Gb 16](#_Toc184565447)

# **Rozbudowa serwera aplikacyjnego**

W ramach dostawy Wykonawca musi rozbudować obecny serwer DELL PowerEdge R640 o numerze ServiceTag 8D2JS63 o kartę 2 portową 10Gb SFP+ wraz z wkładkami, dodatkowe 128GB RAM oraz dostarczyć serwer spełniający poniższe wymagania jako drugi węzeł Klastra.

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

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.

Standard komunikacji to minimum 10Gb wobec czego Wykonawca jest zobowiązany do dostarczenia wszelkich niezbędnych wkładek i patchcordów w celu połączenia do sieciowych urządzeń aktywnych.

|  |  |
| --- | --- |
| **Nazwa** | **Minimalne wymagania dla sprzętu** |
| **Obudowa** | Obudowa Rack 19” o wysokości max 2U z możliwością instalacji min. 8 dysków 2.5” 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. |
| **Procesor** | Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.8GHz z częstotliwości nominalnej, klasy x86, osiągające minimalne wyniki testów w konfiguracji dwuprocesorowej:  SPECrate2017\_int\_base wynik min. 169pkt  SPECrate2017\_int\_peak wynik min. 174pkt  SPECrate2017\_fp\_base wynik min. 246pkt  SPECrate2017\_fp\_peak wynik min. 252pkt  Maksymalny TDP dla procesora 125W  Wynik testu musi być opublikowany na stronie <https://www.spec.org/cpu2017/results/> w dniu złożenia oferty - **dołączyć do oferty wydruk jako przedmiotowy środek dowodowy**. |
| **RAM** | 128GB (w układzie 4x32GB)o częstotliwości taktowania minimum 5400MHz, 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 10/25Gb SFP28 (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) |
| **Kontroler SAS** | Sprzętowy kontroler dyskowy, posiadający minimum:  o 8GB nieulotnej pamięci cache,  o Możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10, 50, 60.  o Wsparcie dla dysków samoszyfrujących |
| **Dyski twarde** | Zainstalowane dyski o minimalnych parametrach:  2 dyski M.2 NVMe SSDs o pojemności 480GB Hot-Plug skonfigurowane w RAID 1 z zainstalowanym systemem operacyjnym opisanym w dalszej cześci  4 dyski 1,92TB SSD SATA typu ReadIntensive DWPD>=1 |
| **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 max. 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 serwerowego systemu operacyjnego (dalej SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego 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. |
| **Licencje dostępowe** | Należy dostarczyć **20** licencji dostępowych na użytkownika tzw. USER CAL |
| **Warunki gwarancji** | 1. Minimum 12 miesięcy 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 – dokumenty potwierdzające należy załączyć do oferty.  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 – dokumenty potwierdzające należy załączyć do oferty.  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. 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 dokument np. certyfikat lub oświadczenie, potwierdzającym autoryzację dla wskazanej firmy serwisującej do świadczenia usług serwisowych w imieniu producenta urządzenia.. Zamawiający dopuszcza Oświadczenie Producenta ze wskazaniem firm(y) serwisującej świadczącej usługi serwisowe dla jej urządzeń na terenie Polski – dokumenty potwierdzające należy załączyć do oferty  **Wymagane dokumenty należy dołączyć do oferty jako przedmiotowy środek dowodowy**  Uwaga! Kryterium punktowane za rozszerzenie gwarancji, wsparcia technicznego i aktualizacyjnego do **60** miesięcy |

# **Centralny UPS 10kVA**

Zamawiający wymaga podłączenia i uruchomienia UPS zgodnie z dobrymi praktykami producenta. Instalacja powinna być wykonana przez osoby autoryzowane lub serwis producenta w celu zachowania ewentualnych świadczeń gwarancyjnych. Zamawiający ze swojej strony zapewni wykonanie kabli zasilających i odbiorczych

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | Projektuje się zasilacz UPS pracujący w topologii on-line VFI-SS-111, wg normy IEC 62040-3, o mocy 10kVA/10kW, pracujący w konfiguracji 3f/3f (wejście 3-fazowe i wyjście 3-fazowe). UPS będzie wyposażony w wewnętrzny, bezprzerwowy bypass elektroniczny. Bypass wewnętrzny będzie posiadał zabezpieczenie przed zwrotnym podawaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040). UPS będzie zasilany dwutorowo – przez tor główny (układ prostownik-falownik) oraz tor rezerwowy (bypass elektroniczny). Dodatkowo będzie wyposażony w zewnętrzny tor obejściowy (serwisowy, mechaniczny). Baterie akumulatorów, zapewniające czas podtrzymania 21 minut dla obciążenia 10kW, będą umieszczone wewnątrz zasilacza UPS oraz w zewnętrznym module bateryjnym. |
| Dane techniczne | * moc wyjściowa: **10 kVA/10 kW** * 3/3 – trzy fazy wejściowe i trzy fazy wyjściowe * sprawność w trybie on-line: **co najmniej 96,1% dla obciążenia w zakresie 75-100%** (do **98,7%** w trybie oszczędzania energii) * tolerancja napięcia wejściowego prostownika, bez przejścia na pracę z baterii: 187-276 V * częstotliwość wejściowa 50 Hz lub 60 Hz z tolerancją 40Hz do 72Hz * wahania napięcia wyjściowego: < 1% * wahania częstotliwości wyjściowej: ±0,1 Hz * cosφ wyjściowy = 1 * cosφ wejściowy > 0,99 * zabezpieczenie przed zwrotnym podaniem energii do sieci zasilającej (backfeed protection, zgodnie z normą IEC 62040) w torze bypassu statycznego UPS * urządzenie powinno być wyposażone w system nieciągłego ładowania baterii. Należy dołączyć opis sposobu zarządzania pracą baterii. W opisie znaleźć się muszą informacje nt. trwania okresów ładowania forsującego, konserwującego i okresu spoczynkowego (tzw. restingu). Okres spoczynkowy w jednym cyklu nie może być krótszy niż 14 dni. Opis powinien być materiałem firmowym producenta * urządzenie powinno posiadać tryb oszczędzania energii, zapewniający automatyczne, bezprzerwowe przełączanie w tryb online (w czasie do 2ms) w przypadku wystąpienia nieprawidłowości w torze bypassu statycznego. Opis technologii powinien być materiałem firmowym producenta * wejściowe zniekształcenia THDi < 5% * wyjściowe THDu:   - dla obciążenia liniowego < 1,5%,  - dla obciążenia nieliniowego < 3,5%.   * Urządzenie musi posiadać panel komunikacyjny, w którym powinny być zainstalowane:   - gniazdo komunikacji RS-232,  - gniazdo wyłącznika awaryjnego p.poż.   * interfejsy komunikacyjne: SNMP – karta sieciowa Gigabit Ethernet, zgodność ze standardem cyberbezpieczeństwa UL 2900-1, UL 2900-2-2 oraz IEC 62443-4-2, szyfrowanie TLS 1.2. Należy przedstawić certyfikaty potwierdzające spełnianie wymaganych norm, wystawione przez niezależną jednostkę badawczą (opcjonalnie: Modbus RTU, Modbus TCP, BACNet IP, styki przekaźnikowe) * graficzny dotykowy wyświetlacz LCD z komunikatami w języku polskim * oświetlenie LED zamontowane w drzwiach UPS, sygnalizujące stany pracy: online, bypass statyczny, tryb bateryjny, awaria UPS |
| Cechy jakościowe | Producent urządzenia musi znajdować się na liście Energy Technology List w zakresie systemów zasilania gwarantowanego UPS  Producent urządzenia musi posiadać ważny certyfikat ISO 9001 w zakresie projektowania, produkcji, sprzedaży i serwisu systemów zasilania gwarantowanego UPS |
| Cechy fizyczne | Wymiary UPS (szer. x gł. x wys.): 350 x 750 x 950 mm  Masa UPS: max 170 kg  Wymiary modułu bateryjnego (szer. x gł. x wys.): 200 x 750 x 950 mm  Masa modułu bateryjnego: max 130 kg  Zyski ciepła z UPS przy 100% obciążenia: maksimum 450W |
| Gwarancja | Minimum **12** miesięcy gwarancji producenta świadczonej w miejscu instalacji UPS, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta lub dedykowany polskojęzyczny portal producenta.  Uwaga! Kryterium punktowane za rozszerzenie gwarancji do **24** miesięcy |

# **Urządzenie UTM**

W ramach dostawy Wykonawca musi dostarczyć system bezpieczeństwa klasy UTM spełniający poniższe wymagania.

Zamawiający informuje, że obecnie użytkuje firewall Fortinet z którego to Wykonawca będzie zobowiązany do przeniesienia obecnej konfiguracji sieci oraz usunięcia ewentualnych błędów/konfliktów konfiguracyjnych w ramach dostawy.

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

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Wymagania ogólne | System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.  System wspiera protokoły IPv4 oraz IPv6 w zakresie:  • Firewall.  • Ochrony w warstwie aplikacji.  • Protokołów routingu dynamicznego. |
| Redundancja, monitoring i wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.  2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.  3. Monitoring stanu realizowanych połączeń VPN.  4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych. |
| Interfejsy i zasilanie | 1. System realizujący funkcję Firewall dysponuje co najmniej 10 portami Gigabit Ethernet RJ-45 i 2 gniazdami SFP 1 Gbps.  2. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.  3. System jest wyposażony w zasilanie AC. |
| Parametry wydajnościowe | 1. W zakresie Firewall’a obsługa nie mniej niż 1.4 mln jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.  2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.  3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.  4. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.  5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions)- minimum 1.3 Gbps.  6. Wydajność skanowania ruchu o charakterystyce typowej dla środowiska przedsiębiorstw (np.: Enterprise Traffic Mix, Enterprise Testing Conditions) z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.  7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps. |
| Funkcje systemu bezpieczeństwa | 1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.  2. Kontrola Aplikacji.  3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.  4. Ochrona przed malware.  5. Ochrona przed atakami - Intrusion Prevention System.  6. Kontrola stron WWW.  7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.  8. Zarządzanie pasmem (QoS, Traffic shaping).  9. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.  10. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.  11. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.  12. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa). |
| Polityki, Firewall | 1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.  2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  • Translację jeden do jeden oraz jeden do wielu.  • Dedykowany ALG (Application Level Gateway) dla protokołu SIP.  3. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.  4. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.  5. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.  6. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.  7. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.  • Amazon Web Services (AWS).  • Microsoft Azure.  • Cisco ACI.  • Google Cloud Platform (GCP).  • OpenStack.  • VMware NSX.  • Kubernetes. |
| Połączenia VPN | 1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:  • Wsparcie dla IKE v1 oraz v2.  • Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).  • Obsługa protokołu Diffie-Hellman grup 19, 20.  • Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.  • Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.  • Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.  • Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.  • Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.  • Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.  • Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.  • Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.  • Mechanizm „Split tunneling” dla połączeń Client-to-Site.  2. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:  • Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.  • Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji. |
| Routing i obsługa łączy WAN | W zakresie routingu rozwiązanie zapewnia obsługę:  1. Routingu statycznego.  2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).  3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.  4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.  5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.  6. BFD (Bidirectional Forwarding Detection).  7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu. |
| Funkcje SD-WAN | 1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.  2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec). |
| Zarządzanie pasmem | 1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.  2. System daje możliwość określania pasma dla poszczególnych aplikacji.  3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.  4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Ochrona przed malware | 1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).  2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.  3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.  4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.  5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).  6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.  8. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.  19. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu. |
| Ochrona przed atakami | 1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.  2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.  3. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.  4. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.  5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).  6. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.  7. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie. |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.  2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.  3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.  4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.  5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.  6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).  7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80). |
| Kontrola WWW | 1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.  2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.  3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.  4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.  5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).  6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.  7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.  8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.  9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji. |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:  • Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.  • Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.  • Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  2. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.  3. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.  4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.  2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.  3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.  4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.  5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.  6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.  7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.  8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).  9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP. |
| Logowanie | 1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.  2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.  3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.  4. Możliwość włączenia logowania per reguła w polityce firewall.  5. System zapewnia możliwość logowania do serwera SYSLOG.  6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS. |
| Szkolenie | Wraz z urządzeniem należy zapewnić autoryzowane szkolenie producenta. Szkolenie musi umożliwiać otrzymanie certyfikatu z akredytacją producenta oferowanego rozwiązania potwierdzający zdobyta wiedzę.. |
| Serwisy, licencje i gwarancja | Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje: Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres minimum **12** miesięcy  Gwarancja sprzętowa: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7  [Uwaga! Kryterium punktowane za rozszerzenie gwarancji, wsparcia technicznego i aktualizacyjnego do **60** miesięcy |

# Serwer NAS klasy korporacyjnej

W ramach dostawy Wykonawca musi dostarczyć serwer NAS spełniający poniższe wymagania.

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 sieci Zamawiającego.

Standard komunikacji to minimum 10Gb wobec czego Wykonawca jest zobowiązany do dostarczenia wszelkich niezbędnych wkładek i patchcordów w celu połączenia do sieciowych urządzeń aktywnych.

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Procesor | Jeden 4-rdzeniowy/4-wątkowy Intel Celeron N5105/N5095 lub równoważny procesor osiągający w testach PassMark - CPU Mark wynik nie gorszy niż 4000 pkt.  W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie <https://www.cpubenchmark.net> - **dołączyć do oferty wydruk jako przedmiotowy środek dowodowy**. |
| Obudowa | Rack 2U o wymiarach nie większych niż, 90× 500 × 430 mm  (wys. x szer. x gł.); w zestawie szyny wysuwane do instalacji w szafie RACK |
| Pamięć RAM | Minimum 8 GB  Urządzenie powinno obsługiwać do 16GB pamięci RAM. |
| Ilość obsługiwanych dysków | 12 dysków 3,5-calowych 3,5/2,5 SATA3 |
| Ilość zainstalowanych dysków | Zainstalowane najmniej 12 dysk HDD o pojemności 4TB znajdujących się na liście zgodności serwera; dyski przeznaczone do pracy 24/7  Dodatkowo należy dostarczyć 1 dysk zapasowy |
| Interfejsy sieciowe | 2 porty 2,5Gigabit sieci Ethernet (RJ45)  2 porty 10GbE SFP+ - zezwala się na użycie 2 portowej karty PCIe z listy zgodności serwera NAS |
| Porty | 2 gniazda typu A USB 2.0  2 gniazda typu A USB 3.2 Gen 2 10 Gb/s  1 gniazdo HDMI 1.4b |
| Porty PCIe | Min. 1 gniazdo Gen3 x2 |
| Wskaźniki LED | Dyski, stan, LAN, stan portów rozszerzenia pamięci masowej |
| Obsługa RAID | RAID 0, 1, 5, 6, 10, 50, 60 |
| Funkcje RAID | Dodanie grupy RAID do puli magazynu, wymiana wszystkich dysków w danej grupie RAID na większe, podłączanie jednostek rozszerzających JBOD. |
| Szyfrowanie | 256-bitowe szyfrowanie AES wolumenów i folderów współdzielonych |
| Stacja monitoringu | Tak, w standardzie 8 darmowych licencji na podłączenie kamer. |
| Protokoły | CIFS, AFP, NFS, FTP, WebDAV, iSCSI, FC, Telnet, SSH, SNMP |
| Usługi | Stacja monitoringu  Windows ACL  Integracja w Windows ADS  Serwer WWW  Serwer plików  Manager plików przez WWW  Replikacja w czasie rzeczywistym  Serwer RADIUS  Klient LDAP  Serwer Syslog  Możliwość uruchomienia kontenerów LXC/LXD  Możliwość uruchomienia maszyn wirtualnych z systemem Windows i Linux |
| Zarządzanie dyskami | SMART, sprawdzanie złych sektorów. |
| Język GUI | Polski |
| System plików | Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+ |
| iSCSI | Obsługa MPIO, MC/S i SPC-3 Persistent Reservation |
| Liczba kont użytkowników | Min. 4096 |
| Liczba grup | Min. 512 |
| Liczba udziałów | Min. 512 |
| Max ilość połączeń (CIFS) | Min. 1500 |
| Zasilanie | Max 2x 300W, 100–240 V |
| Wentylatory | 2 x 80mm, 12VDC |
| UPS | Obsługa sieciowych awaryjnych zasilaczy UPS. |
| Gwarancja i serwis | Minimum **12** miesięcy gwarancji na NAS realizowanej w trybie NBD Onsite przez producenta serwera NAS  [Uwaga! Kryterium punktowane za rozszerzenie gwarancji, wsparcia technicznego i aktualizacyjnego do **36** miesięcy |

# 

# **Dostarczenie i wdrożenie narzędzi klasy EDR**

W ramach dostawy Wykonawca musi dostarczyć oprogramowanie spełniający poniższe wymagania.

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | Obecnie Zamawiający użytkuję oprogramowanie ESET PROTECT Entry na 26 urządzeń o identyfikatorze licencji ………….  Dostarczone oprogramowanie musi zostać podniesione przynajmniej do wersji ESET PROTECT Enterprise dla 26 urządzeń. Obecnie posiadana licencja jest ważna do 21 kwietnia 2025 r., wymaga się również przedłużenia podniesionej licencji o kolejny rok. |

# **Switch 10Gb**

W ramach dostawy Wykonawca musi dostarczyć klaster 2 switchy spełniających poniższe wymagania. Zaoferowane rozwiązanie musi umożliwiać integrację z oferowanym w punkcie 3 urządzeniu „Urządzenie UTM” oraz umożliwiać w przyszłości integracji z systemami klasy NAC.

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

|  |  |
| --- | --- |
| Cecha | Wymagania minimalne |
| Ogólne | W ramach postępowania wymaganym jest dostarczenie elementów systemu niezbędnych do zbudowania bezpiecznej infrastruktury dostępowej. Poszczególne elementy systemu muszą zostać dostarczone w postaci komercyjnych platform sprzętowych lub programowych. W celu realizacji bezpiecznej infrastruktury teleinformatycznej, wymaganym jest dostarczenie przełącznika oraz innych elementów funkcjonalnych, współpracujących oferowanym przez wykonawcę UTM. |
| Parametry fizyczne platformy | 1. Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U. 2. Zasilanie AC 230V. 3. Maksymalny pobór mocy: 30W. |
| Interfejsy sieciowe - wymagania minimalne | 1. Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: 2. 24 porty GE RJ-45 3. 4 porty 10 GE SFP+. |
| Zarządzanie | 1. Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS). 2. Wsparcie dla SNMP w wersjach 1-3 3. Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami. 4. Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI. 5. Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline. 6. Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP). 7. Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+. 8. Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji. 9. Automatycznie wykonywane rewizje konfiguracji. |
| Parametry wydajnościowe | 1. Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps. 2. Tablica adresów MAC o pojemności co najmniej 32k wpisów. 3. Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund. |
| Wymagane funkcje | 1. Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń. 2. Obsługa Jumbo Frames. 3. Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree). 4. Agregacja portów zgodna ze standardem 802.3ad. 5. Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q. 6. Port-mirroring. 7. Uwierzytelnianie 802.1x na poziomie portu. 8. Uwierzytelnianie 802.1x w oparciu o adres MAC. 9. W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN). 10. W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia. 11. W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN. |
| Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC | 1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej: 2. centralne zarządzanie konfiguracją urządzenia 3. aktualizacja oprogramowania realizowana z systemu centralnego zarządzania 4. centralne zarządzanie sieciami vlan. 5. blokowanie ruchu pomiędzy klientami w ramach jednego vlan'u 6. rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp. 7. przenoszenie zidentyfikowanych urządzeń do właściwych stref. w przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej. 8. integrację z systemem kontroli dostępu. urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego. 9. automatyczna detekcja i rekomendacje konfiguracji. 10. przesyłanie logów na zewnętrzny serwer syslog. 11. funkcja uruchomienia captive portalu w celu identyfikacji użytkowników. 12. obsługa białych i czarnych list adresów mac. 13. wykrywanie aplikacji komunikujących się w sieci. 14. Musi być możliwe redundantne połączenie z elementami zarządzającymi. 15. W ramach postępowania koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC. |
| Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa | 1. System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym. 2. System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing. |
| Serwisy, licencje i gwarancja | Sprzęt musi być objęty serwisem gwarancyjnym producenta przez okres **12** miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7  [Uwaga! Kryterium punktowane za rozszerzenie gwarancji, wsparcia technicznego i aktualizacyjnego do **60** miesięcy |