1. Serwer dla OPS – 1 szt.

Obudowa: • Obudowa Rack o wysokości max 1U z możliwością instalacji 4 dysków 3.5” wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Obudowa z możliwością wyposażenia w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS’u, zasilaniu oraz temperaturze.
Płyta główna: • Płyta główna z możliwością zainstalowania jednego procesora. Płyta główna musi być zaprojektowana przez producenta serwera. • Płyta powinna obsługiwać do min. 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci.
Chipset: • Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych.
Procesor: • Jeden procesor 8-rdzeniowy, min. 2.6GHz, umożliwiający osiągnięcie wyniku min. 84 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org w konfiguracji jednoprocesorowej.
Pamięć RAM: • 2x32GB pamięci RAM DDR5 UDIMM o częstotliwości pracy 4800MT/s.
Gniazda PCI: • Min. dwa sloty PCIe x8 Gen 4
Interfejsy sieciowe/FC/SAS: • Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T
Kontroler RAID: • Sprzętowy kontroler dyskowy, posiadający możliwość konfiguracji poziomów RAID: 0, 1, 5, 6, 10 wyposażony w 8GB cache
Dyski twarde: • Zainstalowane: 4x dysk SATA o pojemności min. 8TB, Hot-Plug. • Zainstalowane: 2x dysk M.2 NVMe SSD o pojemności min. 480GB z możliwością konfiguracji RAID 1.
Wbudowane porty: • min. 3 porty USB w tym 1 port USB 3.0 z tyłu obudowy, • Min.1 port VGA na tylnym panelu, • Min. 1 port RS232
Video: • Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze: • Redundantne, o mocy maks. 700W klasy Titanium.
System operacyjny: Oprogramowanie Microsoft Windows Server Standard 2022 oraz min. 10 licencji dostępowych Microsoft Users CAL’s 2019/2022 lub równoważne spełniające poniższe warunki zgodności:

- Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji
- Możliwość wykorzystywania 240 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
- Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
- Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy
- Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
- Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
- Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading;
- Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
- Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
- Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
- Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
- Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
- Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
- Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 2 języków poprzez wybór z listy dostępnych lokalizacji.
- Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
- Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
- Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
- Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.

Bezpieczeństwo:

- Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0
- Serwer musi być wyposażony w rozwiązanie zapewniające ochronę oprogramowania układowego przed manipulacją złośliwego oprogramowania. Ochrona taka musi być zgodna z zaleceniami NIST SP 800-147B i NIST SP 800-155. Jednocześnie Zamawiający wymaga, aby

dostarczony serwer posiadał zaimplementowane sprzętowo mechanizmy kryptograficzne poświadczające integralność oprogramowania BIOS (Root of Trust).
Karta zarządzania: Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera oraz z możliwością rozszerzenia funkcjonalności o: • Wirtualny schowek ułatwiający korzystanie z konsoli zdalnej • Przesyłanie danych telemetrycznych w czasie rzeczywistym • Dostosowanie zarządzania temperaturą i przepływem powietrza w serwerze • Automatyczna rejestracja certyfikatów (ACE)
Certyfikaty: • Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015, ISO-50001 oraz ISO-14001 • Serwer musi posiadać deklaracja CE. • Serwer musi spełniać wymagania normy NIST SP 800-193 ochrony przed cyberatakami. • Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows Server 2019, Microsoft Windows Server 2022.
Dokumentacja użytkownika: • Zamawiający wymaga dokumentacji w języku polskim lub angielskim. • Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Warunki gwarancji: • Zamawiający wymaga zapewnienia przez wykonawcę usługi wsparcia technicznego z zakresu wdrażanej technologii na okres min. 36 miesięcy z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. • Zamawiający oczekuje możliwości zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.

- Zamawiający wymaga dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.
- Wymagane dołączenie do oferty oświadczenia potwierdzającego, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.
- Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
- Zamawiający oczekuje nieodpłatnego udostępnienia narzędzi serwisowych i procesów wsparcia umożliwiających: Wykrywanie usterek sprzętowych z predykcją awarii.
- Automatyczną diagnostykę i zdalne otwieranie zgłoszeń serwisowych.
- Firma serwisująca musi posiadać ISO 9001:2015 oraz ISO-27001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

Wdrożenie:

Zamawiający wymaga montażu fizycznego serwera wraz z pełną aktualizacją systemu operacyjnego hosta i maszyn wirtualnych/oprogramowania układowego serwera na dzień wdrożenia. Wymagane jest zaadresowanie interfejsu niskopoziomowego zarządzania, oraz serwera fizycznego i 2 maszyn wirtualnych które to Wykonawca musi uruchomić na w/w serwerze. Parametry minimalne w/w maszyn wirtualnych zostaną podane na etapie realizacji wdrożenia.
W ramach wdrożenia należy podłączyć oba dostarczane serwery do dostarczanej macierzy za pomocą dedykowanych przewodów. Zezwala się na połączenie direct między macierzą i serwerem bez wykorzystania dedykowanego przełącznika.
W ramach wdrożenia należy wykonać testy redundancji sieci SAN za pomocą fizycznego odpięcia każdej ścieżki.
Wdrożenie musi być zakończone dokumentacją powdrożeniową opisującą wszelkie istotne w punktu działania klastra rekonfigurację, w tym opis konfiguracji konsoli niskopoziomowego zarządzania serwerem.
Wymaga się, aby Wykonawca w ramach dostawy serwera zapewnił dostęp do urządzenia kryptograficznego spełniającego wymagania FIPS-140 Level minimum 3. Urządzenie to może być dostępne dla Zamawiającego jako urządzenie w Cloud z gwarancją przechowywania kluczy kryptograficznych na terenie Polski, lub jako osobne urządzenie w formie karty PCIe lub osobnego urządzenia dostępnego z poziomu sieci LAN.
Na potrzeby udostępnienia takiej usługi Wykonawca musi zapewnić osobny slot urządzenia kryptograficznego na wyłączne potrzeby Zamawiającego. Wymagane interfejsy komunikacji z urządzeniem kryptograficznym PKCS#11, CSP/CNG. Komunikacja sieciowa pomiędzy siedzibą Zamawiającego a urządzeniem kryptograficznym musi być zaszyfrowana za pomocą połączenia IPSEC z kluczem szyfrującym o długości minimum 256bitów typu AES. Dopuszczalne jest użycie algorytmu ECC o długości 192bitów.

2. Serwer NAS dla OPS – 1 szt.

Procesor:

- procesor w architekturze x86 4rdzeniowy o taktowaniu min. 2GHz

Pamięć RAM:

- min. 4 GB DDR4

• min. 2 sloty przeznaczone do instalacji pamięci • możliwość rozbudowy do 16GB
Pamięć FLASH: • min. 4 GB
Obsługiwane dyski twarde: • min. 8 dysków • obsługa dysków 3,5” SATA oraz 2,5” SATA lub SSD SATA
Zainstalowane dyski twarde: • 8 dysków o pojemności min. 8TB
Możliwość rozbudowy: • rozbudowa za pomocą modułów rozszerzających • ilość obsługiwanych modułów rozszerzających: 2
Porty sieciowe: • min. 2 porty 2,5GbE Base-T
Obudowa: • do montażu w szafie RACK 19” o wysokości max. 2U • wyposażona w diody sygnalizujące: stan urządzenia, działanie portów sieciowych, stan dysków twardych • wyposażona w przyciski: Zasilanie, Reset
Porty USB: • min. 2 porty USB 3.2 Gen 2 Typ A • min. 2 porty USB 2.0
Zasilanie: • redundantne zasilacze o mocy 300W
Obsługiwane systemy plików: • dyski wewnętrzne: EXT4 • dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+
Szyfrowanie: • szyfrowanie wolumenów za pomocą protokołu AES256
Zarządzanie dyskami: • pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, • obsługa Hot Spare per grupa RAID oraz global hot spare • rozszerzanie pojemności Online RAID • migracja poziomów Online RAID • HDD S.M.A.R.T. • skanowanie uszkodzonych bloków (pliku) • przywracanie macierzy RAID • obsługa map bitowych • pula pamięci masowej • obsługa migawek • obsługa replikacji migawek
Wbudowana obsługa iSCSI: • obsługa LUN Mapping & Masking • obsługa MPIO • migawka LUN • kopia zapasowa iSCSI LUN

Zarządzanie prawami dostępu: • ograniczenie dostępnej pojemności dysku dla użytkownika • importowanie listy użytkowników • zarządzanie kontami użytkowników • zarządzanie grupą użytkowników • zarządzanie współdzieleniem w sieci • tworzenie użytkowników za pomocą makr • obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL
Obsługa Windows AD: • logowanie użytkowników domenowych poprzez protokoły CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web • funkcja serwera i klienta LDAP
Funkcje backup: • oprogramowanie do tworzenia kopii plików, opracowane przez producenta urządzenia dla systemów Windows, • backup na zewnętrzne dyski twarde,
Darmowe aplikacje na urządzenia mobilne: • Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki • dostępne na systemy iOS oraz Android
Minimum obsługiwane aplikacje: • serwer plików • serwer FTP • serwer WEB • serwer kopii zapasowych • serwer multimediów UPnP • serwer pobierania (Bittorrent / HTTP / FTP) • serwer Monitoringu
VPN: • VPN client / VPN server • obsługa PPTP, OpenVPN
Administracja systemu: • połączenia HTTP/HTTPS • powiadamianie przez e-mail (uwierzytelnianie SMTP) • powiadamianie przez SMS • ustawienia inteligentnego chłodzenia • DDNS oraz zdalny dostęp w chmurze • SNMP (v2 & v3) • obsługa UPS z zarządzaniem SNMP (USB) • obsługa sieciowej jednostki UPS • monitor zasobów • kosz sieciowy dla CIFS/SMB oraz AFP • monitor zasobów systemu w czasie rzeczywistym • rejestr zdarzeń • system plików dziennika • całkowity rejestr systemowy (poziom pliku) • zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line

• aktualizacja oprogramowania • kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu
Wirtualizacja: • wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. • dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 • funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.
Konteneryzacja: • możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker
Zabezpieczenia: • filtracja IP • ochrona dostępu do sieci z automatycznym blokowaniem • połączenie HTTPS • FTP z SSL/TLS (Explicit) • obsługa SFTP • szyfrowanie AES 256-bit • szyfrowana zdalna replikacja (Rsync poprzez SSH) • import certyfikatu SSL • powiadomienia o zdarzeniach za pośrednictwem Email i SMS
Możliwość instalacji dodatkowego oprogramowania: • tak, sklep z aplikacjami; możliwość instalacji z paczek
Gwarancja: • min. 36 miesięcy gwarancji Producenta

3. Urządzenie UTM – 1 szt.

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 z oferowanym UTM, o następujących parametrach:
Obsługa sieci: • Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewall, systemu IPS oraz usług sieciowych takich jak np. DHCP.
Zapora korporacyjna: • Wymaganym jest, aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości: • Urządzenie ma być wyposażone w Firewall klasy Stateful Inspection. • Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. • Urządzenie ma umożliwiać ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). • Interface (GUI) do konfiguracji firewall ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy, port docelowy, etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie.

- Administrator ma mieć możliwość budowania reguł firewall na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, usług internetowych (web services), użytkownika bądź grupy z bazy LDAP, pola DSCP nagłówka pakietu, przypisania kolejki QoS, określenia limitu połączeń na sekundę, godziny oraz dnia nawiązywania połączenia.
- Urządzenie ma umożliwiać filtrowanie jedynie na poziomie warstwy 2 modelu OSI tj. na podstawie adresów mac.
- Administrator ma mieć możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł firewall.
- Edytor reguł firewall ma posiadać wbudowany analizator reguł, który wskazuje błędy i sprzeczności w konfiguracji reguł.
- Urządzenie ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę LDAP (wewnętrzną oraz zewnętrzną), zewnętrzny serwer RADIUS, zewnętrzny serwer Kerberos.
- Urządzenie ma umożliwiać wskazanie trasy routingu dla wybranej reguły niezależnie od innych tras routingu (np. routingu domyślnego).
- System musi umożliwiać budowanie reguł bezpieczeństwa w oparciu o definiowane przez administratora harmonogramy czasowe.

Intrusion Prevention System (IPS):

- System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalie w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe.
- Moduł IPS ma być opracowany przez producenta urządzenia. Nie dopuszcza się, aby moduł IPS pochodził od zewnętrznego dostawcy.
- Moduł IPS ma zabezpieczać przed co najmniej 10 000 ataków i zagrożeń.
- Administrator ma mieć możliwość tworzenia własnych sygnatur dla systemu IPS.
- Moduł IPS ma nie tylko wykrywać, ale również usuwać szkodliwą zawartość w kodzie HTML oraz JavaScript żądanej przez użytkownika strony internetowej nie blokując dostępu do tej strony po usunięciu zagrożenia.
- Urządzenie ma umożliwiać inspekcję ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, POP3S oraz SMTPS.
- Administrator ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
- Urządzenie ma umożliwiać ochronę między innymi przed atakami typu SQL Injection, Cross Site Scripting (XSS) oraz złośliwym kodem Web2.0.
- Po zakupie stosownej licencji moduł IPS ma zapewniać analizę protokołów przemysłowych co najmniej takich jak: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS/LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose
- Urządzenie musi zapewniać automatyczną aktualizację sygnatur kontekstowych.

Kształtowanie pasma:

- Urządzenie ma umożliwiać kształtowanie pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma.
- Ograniczenie pasma lub priorytetyzacja reguły firewall ma być możliwe względem pojedynczego połączenia, adresu IP, zautoryzowanego użytkownika, pola DSCP.

- Urządzenie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma, a jedynie na śledzenie konkretnego typu ruchu (monitoring).
- Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch.

Ochrona antywirusowa:

- Urządzenie ma umożliwiać zastosowanie jednego z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania).
- Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji.
- Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym.
- Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu wykrycia infekcji.

Ochrona antyspam:

- Urządzenie ma posiadać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM).
- Ochrona antyspam ma działać w oparciu o:
  - białe/czarne listy,
  - DNS RBL,
  - Skaner heurystyczny.
- W przypadku ochrony w oparciu o DNS RBL administrator ma mieć możliwość modyfikowania listy serwerów RBL znajdujących się w domyślnej konfiguracji urządzenia.
- Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
- Urządzenie ma umożliwiać stworzenie sieci VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja).
- Urządzenie ma wspierać co najmniej następujące typy sieci VPN:
  - PPTP VPN,
  - IPSec VPN,
  - SSL VPN.
- SSL VPN ma działać co najmniej w trybach tunelu i portalu.
- Producent urządzenia ma umożliwiać pobranie klienta VPN współpracującego z oferowanym rozwiązaniem.
- Klient SSL VPN ma być dostępny z poziomu portalu uwierzytelniania (captive portal)
- Urządzenie ma umożliwiać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover).
- Urządzenie ma umożliwiać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf.
- Urządzenie ma umożliwiać tworzenie tuneli IPSec Policy Based oraz Route Based.

Filtr dostępu do stron www:

- Urządzenie ma posiadać wbudowany filtr URL.
- Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych.
- Administrator ma mieć możliwość dodawania własnych kategorii URL.
- Administrator ma mieć możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru ma być przynajmniej:
  - blokowanie dostępu do adresu URL,

- zezwolenie na dostęp do adresu URL,
- blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora.
- Administrator ma mieć możliwość skonfigurowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony.
- Strona blokady ma umożliwiać wykorzystanie zmiennych środowiskowych.
- Filtr URL musi uwzględniać komunikację po protokole HTTPS.
- Urządzenie ma umożliwiać identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME.
- Urządzenie ma umożliwiać stworzenie listy stron dostępnych po protokole HTTPS, które nie będą deszyfrowane.
- Urządzenie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch

Uwierzytelnianie:

- Urządzenie ma umożliwiać uwierzytelnianie użytkowników co najmniej w oparciu o:
- lokalną bazę użytkowników (wewnętrzny LDAP),
- zewnętrzną bazę użytkowników (zewnętrzny LDAP),
- usługę katalogową Microsoft Active Directory.
- Urządzenie ma umożliwiać równoczesne użycie co najmniej 5 różnych baz LDAP.
- Urządzenie ma umożliwiać uruchomienie specjalnego portalu (captive portal), który ma zezwalać na autoryzację użytkowników co najmniej w oparciu o protokoły:
- SSL,
- Radius,
- Kerberos.
- Urządzenie ma umożliwiać transparentną autoryzację użytkowników w usłudze katalogowej Microsoft Active Directory w oparciu o co najmniej dwa mechanizmy.
- Co najmniej jedna z metod transparentnej autoryzacji nie może wymagać instalacji dedykowanego agenta.
- Autoryzacja użytkowników z Microsoft Active Directory nie może wymagać modyfikacji schematu domeny.
- Rozwiązanie musi mieć możliwość transparentnego uwierzytelniania użytkowników w ramach infrastruktury VDI (Virtual Desktop Infrastructure) poprzez dedykowanego agenta. Metoda ta musi wspierać co najmniej technologie Citrix Virtual Apps i Microsoft Remote Desktop Services (RDS).
- Urządzenie musi posiadać wbudowany moduł zapewniający podwójne uwierzytelnianie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP).
- Wbudowany moduł 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec,

Administracja łączami do Internetu:

- Urządzenie ma umożliwiać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. Load Balancing).
- Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy:
- równoważenie względem adresu źródłowego,
- równoważenie względem połączenia.
- Mechanizm równoważenia obciążenia ma uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu.

- Urządzenie ma umożliwiać przełączenie na łącze zapasowe w przypadku awarii łącza podstawowego (tzw. Failover).
- Urządzenie ma wspierać mechanizm SD-WAN zapewniając automatyczną optymalizację i wybór najkorzystniejszego łącza.
- W zakresie SD-WAN urządzenie ma zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów).
- Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP.

Routing:

- Urządzenie ma umożliwiać statyczne trasowanie pakietów.
- Urządzenie ma umożliwiać trasowanie połączeń IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego.
- Urządzenie ma umożliwiać trasowanie pakietów z poziomu wybranej reguły firewall (tzw. Policy Based Routing).
- Urządzenie ma umożliwiać dynamiczne trasowanie pakietów w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP.

Administracja urządzeniem:

- Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego.
- Interfejs konfiguracyjny ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być możliwa zarówno poprzez niezaszyfrowany protokół HTTP, jak zaszyfrowany protokół HTTPS.
- Administrator ma mieć możliwość wskazania do komunikacji innego portu niż 443 TCP.
- Urządzenie ma umożliwiać zarządzanie przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami.
- Urządzenie musi oferować możliwość wykorzystania wbudowanych profili administracyjnych określających dostęp do poszczególnych modułów systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.
- Urządzenie ma umożliwiać zarządzenia z poziomu konsoli (SSH)
- Urządzenie ma umożliwiać zarządzanie poprzez dedykowaną platformę centralnego zarządzania.
- Interfejs konfiguracyjny platformy centralnego zarządzania ma być dostępny poprzez przeglądarkę internetową, a komunikacja ma być zabezpieczona za pomocą protokołu HTTPS.
- Wbudowany webowy, graficzny interfejs administracyjny urządzenia musi oferować narzędzia diagnostyczne, co najmniej ping, traceroute, nslookup.
- Wbudowany webowy, graficzny interfejs administracyjny musi oferować narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych.
- Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość zdefiniowania polityki haseł stosowanych w całym systemie w zakresie minimalnej ilości znaków czy złożoności hasła.
- Wbudowany webowy, graficzny interfejs administracyjny musi oferować możliwość generowania skryptów z czynności wykonywanych przez administratora (script recording).
- System musi oferować możliwość zdefiniowania własnych obiektów sieciowych, obiektów URL, certyfikatów, usług internetowych (web services).
- Urządzenie musi oferować portal uwierzytelniania (captive portal) dla użytkowników.

- Urządzenie ma umożliwiać zapisywanie logów na wbudowanym dysku.
- Urządzenie ma umożliwiać eksportowanie logów na zewnętrzny serwer (syslog) z wykorzystaniem transmisji nieszyfrowanej jak i szyfrowanej (TLS).
- Urządzenie ma umożliwiać eksportowanie logów za pomocą protokołu IPFIX.
- Urządzenie ma umożliwiać eksportowanie backupu konfiguracji (kopia zapasowa) co najmniej w zakresie:
  - manualnego eksportu do pliku w dowolnym momencie czasu,
  - automatycznego eksportu do serwerów producenta lub na dedykowany serwer zarządzany przez administratora, z możliwością wyboru częstotliwości co najmniej: raz dziennie, raz w tygodniu, raz w miesiącu
- Urządzenie ma umożliwiać odtworzenie backupu konfiguracji pochodzącego bezpośrednio z serwerów producenta lub z dedykowanego serwera zarządzanego przez administratora.
- Urządzenie ma umożliwiać anonimizację logów co najmniej w zakresie adresu źródłowego oraz nazwy użytkownika.
- Rozwiązanie musi dawać możliwość ręcznej aktualizacji baz zabezpieczeń poprzez wskazanie pliku aktualizacji w trybie offline z poziomu interfejsu graficznego.

- **Raportowanie:**
- Urządzenie ma posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu.
- System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania.
- System raportowania ma posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego, skanera Antyspamowego.
- System raportowania ma umożliwiać wygenerowanie co najmniej 25 różnych raportów.
- System raportowania ma umożliwiać edycję konfiguracji bezpośrednio z poziomu raportu.
- System raportowania ma umożliwiać eksport wyników raportu do formatu CSV.
- Urządzenie musi posiadać możliwość rozbudowy o dedykowany system zbierania logów i tworzenia raportów w postaci wirtualnej maszyny pochodzący od tego samego producenta.
- Urządzenie ma umożliwiać monitorowanie swojego stanu w wykorzystanie protokołu SNMP w wersji 1, 2 i 3.
- Urządzenie ma umożliwiać monitorowanie ruchu sieciowego bezpośrednio w konsoli GUI, a także z poziomu konsoli (SSH).

Pozostałe usługi i funkcje:

- Urządzenie ma umożliwiać stworzenie interfejsu zagregowanego w oparciu o protokół LACP.
- Urządzenie ma posiadać wbudowany serwer DHCP z możliwością dynamicznego przypisywania adresów jak i statycznego przypisywania adresu IP do adresu MAC karty sieciowej.
- Urządzenie ma pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP (tzw. DHCP Relay).
- Konfiguracja serwera DHCP ma być niezależna dla IPv4 i IPv6.
- Urządzenie ma umożliwiać stworzenia różnych konfiguracji DHCP dla różnych podsieci skonfigurowanych zarówno na interfejsach fizycznych jak i wirtualnych (VLAN) w zakresie określenia bramy, serwerów DNS, nazwy domeny).
- Urządzenie ma posiadać usługę DNS Proxy.
- Urządzenie ma posiadać wsparcie dla Spanning-tree protocol (RSTP/MSTP).

- Urządzenie musi oferować wsparcie dla IEEE 802.1Q VLAN.
- Urządzenie musi mieć zaimplementowane Open API
- 1Urządzenie ma posiadać dwie niezależne partycje np. w celu zapewnienia działania na wypadek awarii podczas aktualizacji oprogramowania układowego (firmware). W tym celu ma być możliwe zsynchronizowanie aktywnej partycji z zapasową przed aktualizacją firmware lub w dowolnym innym momencie.

Gwarancja i serwis:

- Urządzenie ma być objęte min. 60-miesięczną gwarancją producenta na dostarczone elementy systemu oraz licencję dla wszystkich funkcji bezpieczeństwa.
- W okresie obowiązywania gwarancji ma być zapewnione wsparcie techniczne świadczone co najmniej drogą e-mail lub przez dedykowany do tego portal.
- Urządzenie ma być objęte gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od potwierdzenia awarii.

Parametry sprzętowe:

- Urządzenie ma być wyposażone w dysk SSD o pojemności co najmniej 200 GB.
- Urządzenie wyposażone jest w redundantne zasilanie z sygnalizacją pracy poszczególnych zasilaczy.
- Liczba portów Ethernet 2,5Gbps – min. 8 z możliwością rozszerzenia do 16.
- Liczba portów światłowodowych 1Gbps – min. 2 z możliwością rozszerzenia do 10.
- Urządzenie ma pozwalać na instalację modułu rozszerzeń z poniższej listy:
  - Moduł z 8 interfejsami miedzianymi 2,5Gbps
  - Moduł z 4 interfejsami miedzianymi 10Gbps.
  - Moduł z 4 interfejsami światłowodowymi 1Gbps.
  - Moduł z 8 interfejsami światłowodowymi 1Gbps.
  - Moduł z 4 interfejsami światłowodowymi 10Gbps.
- Urządzenie ma umożliwiać dostęp do Internetu za pomocą modemu 3G oraz 4G pochodzącego od dowolnego producenta.
- Urządzenie ma być wyposażone w min. 2, różniące się typem, porty konsolowe. Przynajmniej jeden port konsolowy ma być typu RJ45.
- Przepustowość Firewall (1518 bajtów UDP) – minimum 10Gbps.
- Przepustowość Firewall wraz z włączonym systemem IPS (1518 bajtów UDP) – minimum 5Gbps.
- Przepustowość filtrowania Antywirusowego – minimum 1.3 Gbps.
- Przepustowość tunelu VPN przy szyfrowaniu AES – minimum 2.5Gbps.
- Maksymalna liczba tuneli VPN IPSec – minimum 1000.
- Maksymalna liczba tuneli typu SSL VPN (tryb tunelu) – minimum 150.
- Maksymalna liczba tuneli typu SSL VPN (tryb portalu) – minimum 150.
- Obsługa interfejsów 802.11q (VLAN) – minimum 256.
- Liczba równoczesnych sesji – minimum 600 000 i nie mniej niż 30 000 nowych sesji/sekundę.
- Urządzenie ma umożliwiać budowanie klastrów wysokiej dostępności HA co najmniej w trybie Active-Passive.
- Urządzenie nie ma limitu na liczbę użytkowników.
- Liczba reguł filtrowania – minimum 16 384.
- Liczba tras statycznego routingu – minimum 5 120.
- Liczba tras dynamicznego routingu – minimum 10 000.

• Możliwość instalacji w szafie RACK 19”, wysokość urządzenia 1U. • Urządzenie musi być wyposażone w moduł TPM.
Wdrożenie: Zamawiający wymaga przeprowadzenie wdrożenia dostarczonego urządzenia UTM w zakresie minimum: • Wstępna konfiguracja urządzenia UTM/NGFW - dostępy administracyjne, synchronizacja czasu • Przeniesienie konfiguracji z obecnie posiadanego rozwiązania (Reguły firewall/NAT, konfiguracja interfejsów, routing statyczny, DHCP, IPSec VPN do 10 tuneli) • Uruchomienie SSL VPN (wewnętrzna baza użytkowników lub Active Directory/LDAP) • Integracja z Active Directory + Agent SSO • Dostosowanie wyjątków dla alarmów lub zaawansowanej konfiguracji systemu IPS. • Uruchomienie funkcji automatycznego backupu konfiguracji. • Uruchomienie funkcji DNS proxy. • Uruchomienie wbudowanego systemu raportowania. • Uruchomienie powiadomień mailowych – jeśli klient dostarczy dane serwera SMTP. • Konfiguracja zbierania logów • Uruchomienie agenta SNMP • Przygotowanie Dokumentacji powdrożeniowej Wymagane jest, aby wdrożenie przeprowadzone było przez Inżyniera Wykonawcy, posiadającego certyfikat producenta dostarczanego rozwiązania, który będzie potwierdzeniem posiadania umiejętności min: (Certyfikat należy załączyć do oferty) • Sieci i routingu w dostarczonym rozwiązaniu • Przechwytywania i analizy ruchu sieciowego • Konfiguracji i diagnostyki połączeń IPSec VPN oraz SSL VPN • Konfiguracji systemu IPS oraz dostosowywania jego konfiguracji • Konfiguracji i analizy polityk bezpieczeństwa • Konfiguracji mechanizmu NAT • Konfiguracji uwierzytelniania użytkowników • Kontroli dostępu do stron WWW oraz deszyfrowania ruchu sieciowego w celu analizy przez systemy bezpieczeństwa • Konfiguracji i diagnostyki mechanizmów zapewniania wysokiej dostępności • Konfiguracji mechanizmów PKI w dostarczonym rozwiązaniu • Przeszukiwania logów dotyczących ruchu sieciowego oraz pracy urządzenia • Wsparcia technicznego i rozwiązywania problemów z dostarczonym rozwiązaniem

4. Przełącznik 48-portowy – 2 szt.

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.
Obudowa: • Do montażu w szafie rack 19”, wysokość 1U wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona aktywnie
Porty:

• Minimum 48 portów 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at, minimum 4 porty SFP/SFP+ 1/10GbE, • Budżet mocy PoE min. 400 W • Min. 1 port typu out-of-band management • Min. 1 port konsolowy RS232 RJ45 • Min 1 port typu USB A do transferu plików
Wydajność przełącznika: • Minimum 16000 adresów MAC Switch fabric capacity min. 176 Gbps • Forwarding rate min. 120 Mpps • Pamięć flash min. 128 MB • Pamięć RAM min. 512 MB
Funkcjonalność warstwy II: • Minimum 16000 adresów MAC Switch fabric capacity min. 176 Gbps Forwarding rate min. 120 Mpps • Pamięć flash min. 128 MB • Pamięć RAM min. 512 MB
Funkcjonalność warstwy III: • Obsługa routingu statycznego oraz dynamicznego RIPv2 oraz OSPFv2 Obsługa minimum 64 wpisów routingu statycznego • Obsługa minimum 512 wpisów routingu dynamicznego
Inne Funkcjonalności: • Obsługa list kontroli dostępu opartych o adresy MAC i IP Ochrona DoS • Storm Control Broadcast/Multicast/Unknown Unicast • DHCP Snooping • DHCP Relay • DHCP Server • IGMP Snooping Querier • IGMP Proxy • PVST/PVRST • BPDU Guard, BPDU filtering, Root Guard • Authentication, Authorization, and Accounting (AAA) • Private VLAN • Port Mirroring • Port Security/MAC Locking • DiffServ support • DSCP and 802.1p (CoS) • Traffic shaping/metering • OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority (SP) • Narzędzia diagnostyczne PING, TRACEROUTE, ICMPv6 • TFTP, FTP, Telnet, SSH v2 • SNMP v1/v2/v3 • Zarządzanie IPv6 • Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych

• Zero-touch deployment • Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS) oraz kontroler w wersji on-premise lub chmurowej
Zgodność z protokołami: • 802.1ab LLDP • ANSI/TIA-1057- LLDP-MED • 802.1D Bridging, Spanning Tree • 802.1p Ethernet Priority • 802.1Q VLAN Tagging • 802.1S Multiple Spanning Tree (MSTP) • 802.1W Rapid Spanning Tree (RSTP) • 802.1X Network Access Control, Auto VLAN • 802.2 Logical Link Control • 802.3 10BASE-T • 802.3ab Gigabit Ethernet (1000BASE-T) • 802.3ac Frame Extensions for VLAN Tagging • 802.3ad Link Aggregation with LACP • 802.3u Fast Ethernet (100BASE-TX) • 802.3x Flow Control • RFC 768 UDP • RFC 791 IP • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 2030 SNTP • RFC 2132 DHCP options and BOOTP vendor extensions • RFC 2865 RADIUS Client • RFC 3579 RADIUS Support for EAP • RFC 3164 Syslog
Gwarancja oraz wsparcie: Minimum 60 miesięcy gwarancji producenta.

5. Przełącznik 24-portowy – 2 szt.

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.
Obudowa: • Do montażu w szafie Rack 19", o wysokości nie więcej niż 1U, wraz z kompletem uchwytów montażowych, wyposażona w zintegrowany zasilacz, chłodzona pasywnie (bez użycia wentylatorów).
Porty: • Minimum 48 portów 10/100/1000 Mbps RJ45 z obsługą PoE+ 802.3af/at, minimum 4 porty SFP/SFP+ 1/10GbE, • Budżet mocy PoE min. 400 W • 1 port typu out-of-band management • 1 port konsolowy RS232 RJ45

• 1 port typu USB A do transferu plików
Wydajność przełącznika: • Minimum 16000 adresów MAC • Switch fabric capacity min. 128 Gbps • Forwarding rate min. 120 Mpps • Pamięć flash min. 128 MB • Pamięć RAM min. 512 MB
Funkcjonalność warstwy II: • Obsługa minimum 4000 wirtualnych sieci • Wsparcie dla agregacji statycznej oraz LACP (802.3ad) • Obsługa 8 grup LACP i 8 portów fizycznych per grupa • Obsługa ramek Ethernet typu Jumbo min. 9k
Funkcjonalność warstwy III: • Obsługa routingu statycznego oraz dynamicznego RIPv2 oraz OSPFv2 • Obsługa minimum 64 wpisów routingu statycznego • Obsługa minimum 512 wpisów routingu dynamicznego
Inne Funkcjonalności: • Obsługa list kontroli dostępu opartych o adresy MAC i IP • Ochrona DoS • Storm Control Broadcast/Multicast/Unknown Unicast • DHCP Snooping • DHCP Relay • DHCP Server • IGMP Snooping Querier • IGMP Proxy • PVST/PVRST • BPDU Guard, BPDU filtering, Root Guard • Authentication, Authorization, and Accounting (AAA) • Private VLAN • Port Mirroring • Port Security/MAC Locking • DiffServ support • DSCP and 802.1p (CoS) • Traffic shaping/metering • OoS – kolejki priorytetowe oraz Weighted Round Robin (WRR), Strict Priority (SP) • Narzędzia diagnostyczne PING, TRACEROUTE, ICMPv6 • TFTP, FTP, Telnet, SSH v2 • SNMP v1/v2/v3 • Zarządzanie IPv6 • Funkcjonalność typu autoinstall/autodeployment dla oprogramowania układowego oraz plików konfiguracyjnych • Zero-touch deployment • Zarządzanie przez CLI, wbudowane WebGUI (HTTP/HTTPS) oraz kontroler w wersji on-premise lub chmurowej
Zgodność z protokołami: • 802.1ab LLDP

• ANSI/TIA-1057- LLDP-MED • 802.1D Bridging, Spanning Tree • 802.1p Ethernet Priority • 802.1Q VLAN Tagging • 802.1S Multiple Spanning Tree (MSTP) • 802.1W Rapid Spanning Tree (RSTP) • 802.1X Network Access Control, Auto VLAN • 802.2 Logical Link Control • 802.3 10BASE-T • 802.3ab Gigabit Ethernet (1000BASE-T) • 802.3ac Frame Extensions for VLAN Tagging • 802.3ad Link Aggregation with LACP • 802.3u Fast Ethernet (100BASE-TX) • 802.3x Flow Control • RFC 768 UDP • RFC 791 IP • RFC 792 ICMP • RFC 793 TCP • RFC 826 ARP • RFC 2030 SNTP • RFC 2132 DHCP options and BOOTP vendor extensions • RFC 2865 RADIUS Client • RFC 3579 RADIUS Support for EAP • RFC 3164 Syslog
Gwarancja oraz wsparcie: Minimum 60 miesięcy gwarancji producenta.

6. Access Point – 1 szt.

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera.
Porty: • Min. 1 x 10/100/1000/2500 RJ-45 port PoE
Pasmo: • 2,4 GHz • 5 GHz • 6 GHz
Standardy: • 802.11a • 802.11b • 802.11g • 802.11n • 802.11ax • 802.11ac • 802.1Q
Antena:

• Wewnętrzna
Bezpieczeństwo: • WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)
Funkcje dodatkowe: • BSSID 8 per radio • VLAN 802.1Q • Advanced QoS Per-user rate limiting • Guest traffic isolation Supported • Concurrent clients 600+ • Zero wait DFS
Gwarancja: min. 12 miesięcy gwarancji Producenta

7. Zakup platformy do zarządzania logami

Wymagane jest dostarczenie oprogramowania posiadającego poniższą funkcjonalność
Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń: • Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna. • Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (usługą katalogową) lub ręcznie przez definiowanie kont w samym rozwiązaniu. • 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. • 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. • 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 dowolną przeglądarką WWW. • 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. • 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). W zakresie wdrożenie proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń: • Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualne.

- 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.
- Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
- Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
- Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:
  - Urządzenie klasy UTM
  - Przełączniki zarządzalne
  - Serwery fizyczne
  - Serwery wirtualizacji
  - stacje roboczych
  - aplikację centralnego zarządzania posiadanego antywirusa
  - aplikację do monitorowania infrastruktury informatycznej dla Zamawiającego

- Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
- Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
- Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
- Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
- Konfiguracja wysyłania powiadomień poprzez maila w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
- Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.

Zamawiający wymaga, aby Wykonawca w czasie do 30.06.2026 od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
Zamawiający wymaga, aby Wykonawca w okresie do 30.06.2026 od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.