Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Serwery do klastra HA – 2 szt.

Obudowa: • Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. • Możliwość wyposażenia w panel LCD umieszczony na froncie obudowy • Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna: • Płyta główna z możliwością zainstalowania do dwóch procesorów. • Obsługa procesorów 32 rdzeniowych. • Płyta główna musi być zaprojektowana przez producenta serwera • Na płycie głównej powinno znajdować się minimum 16 sloty przeznaczone do instalacji pamięci. • Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Chipset: • Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor: • Zainstalowane dwa procesory min. 8-rdzeniowe, min. 2.6GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 169 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
Pamięć RAM: • Minimum 256GB DDR5 RDIMM 5600MT/s,
Gniazda PCI: • minimum jeden slot PCIe x16 Gen 4 • minimum dwa sloty PCIe x8 Gen 4
Interfejsy sieciowe / FC / SAS: • Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie Base-T • Dodatkowe min. 4 interfejsy sieciowe 1Gb Ethernet w standardzie Base- (porty nie mogą być osiągnięte poprzez karty w slotach PCIe) • 4 interfejsy SAS 12Gb/s wyprowadzone na zewnątrz obudowy w celu połączenia z zamawianą macierzą dyskową
Dyski twarde: • Zainstalowane 2 dyski SSD M.2 o pojemności min. 480GB Hot-Plug skonfigurowane w RAID 1
Wbudowane porty:

- 3x USB, w tym min. 1 porty USB 3.0
- 2x port VGA (jeden na panelu przednim)

Video:

- Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200

Zasilacze:

- Redundantne, Hot-Plug min. 700W klasy Titanium każdy.

Bezpieczeństwo:

- Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych.
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania.
- BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła
- Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
- Moduł TPM 2.0
- Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem

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.

- 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.
- 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
- Wykonawca musi posiadać certyfikat nadany przez uprawniony podmiot potwierdzający realizację usług serwisowych zgodnie z normą PN-EN ISO 27001:2017 lub certyfikat równoważny

Wdrożenie:

Zamawiający wymaga montażu fizycznych serwerów 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.

Macierz do klastra HA – 1 szt.

Obudowa: • Do instalacji w standardowej szafie RACK 19”, macierz musi zajmować maksymalnie 2U i pozwalać na instalacje min. 24 dysków 2.5”.
Kontrolery: • Dwa kontrolery RAID pracujące w układzie active-active posiadające łącznie minimum osiem portów SAS z przepustowością minimum 12 Gb/s wraz z 4 kablami o długości min. 2m. • Komunikacja kontrolerów z podłączanymi półkami dyskowymi musi być realizowana przez połączenia SAS o przepustowości minimum 12 Gb/s • Możliwość konfiguracji RAID 1, 5, 6, 10.
Cache: • Minimum 16GB na kontroler, pamięć cache zapisu mirrorowana między kontrolerami, podtrzymywana bateryjnie przez min. 72h w razie awarii.
Zainstalowane dyski: • Min. 3 dyski SSD SAS o pojemności min. 1.6TB przeznaczone do mieszanych zastosowań, • Min. 9 dysków SAS o pojemności min. 2.4TB 10k. Zaproponowane rozwiązanie musi wspierać instalację minimum 220 dysków w ramach jednego rozwiązania. Rozwiązanie musi mieć możliwość rozbudowy do minimum 2.3PB przestrzeni surowej.
Oprogramowanie/Funkcjonalności: • Zarządzanie macierzą poprzez minimum przeglądarkę internetową, GUI oparte o HTML5. • Wbudowany system powiadamiania drogą mailową o awarii. • Macierz musi umożliwiać utworzenie minimum 512 LUN’ów oraz 1024 kopii migawkowych na całą macierz. • Wbudowana funkcjonalność automatycznego (bez interwencji człowieka) rozkładania danych między dyskami poszczególnych typów (tzw. auto-tiering). Dane muszą być automatycznie przemieszczane między rożnymi typami dysków. • Rozwiązanie musi wspierać obsługę samoszyfrujących się dysków Jeżeli którakolwiek z powyższych funkcjonalności wymaga dostarczenia dodatkowej licencji to należy ją zapewnić na całe oferowane rozwiązanie rozumiane w szczególności w zakresie przestrzeni dyskowej
Wsparcie dla systemów operacyjnych: • Windows Server 2019, Windows Server 2022,
Bezpieczeństwo: • Ciągła praca obu kontrolerów nawet w przypadku zaniku jednej z faz zasilania. Zasilacze, wentylatory, kontrolery RAID redundantne.
Warunki gwarancji dla macierzy: • 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 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 macierzy.
- Wszystkie naprawy gwarancyjne powinny być możliwe na miejscu.
- Dostawca ponosi koszty napraw gwarancyjnych, włączając w to koszt części i transportu.
- W czasie obowiązywania gwarancji dostawca zobowiązany jest do udostępnienia Zamawiającemu nowych wersji BIOS, firmware i sterowników (na płytach CD lub stronach internetowych).

Dokumentacja użytkownika:

- Zamawiający wymaga dokumentacji w języku polskim lub angielskim.

Certyfikaty:

- Macierz musi być wyprodukowana zgodnie z normą ISO 9001:2015.
- Wykonawca musi posiadać certyfikat nadany przez uprawniony podmiot potwierdzający realizację usług zgodnie z normą ISO 27001:20017 lub certyfikat równoważny.

Wdrożenie:

- Zamawiający wymaga, aby wykonawca wykonał następujące prace wdrożeniowe: Instalacja fizyczna sprzętu w serwerowi.
- Ustawienie adresacji i podłączenie urządzeń zgodnie z wymaganiami Zamawiającego.
- Aktualizacja oprogramowania systemowego oraz układowego wdrażanych rozwiązań do najnowszego na dzień wdrożenia
- Przygotowanie dokumentacji powdrożeniowej.

Urządzenie magazynujące dane – 1 szt.

Sprzęt musi być fabrycznie nowy, rok produkcji nie starszy niż 2024 r.
Rozwiązanie musi spełniać minimalne poniższe wymagania sprzętowe:
Obudowa rack rozmiar: 2U
Procesor: min. 8 rdzeni, min. 16 wątków. Minimalna częstotliwość bazowa procesora 2.8GHz
Pamięć RAM: 32GB DDR4
Przestrzeń dostępna na przechowywanie danych:
Min. 40TB po RAID 6
Osobne dyski SSD M.2 nVME działające w RAID1 w celu instalacji warstwy oprogramowania i systemu operacyjnego,
Urządzenie musi pozwalać na zbudowanie magazyny obiektowego S3
Urządzenie musi pozwalać na włączenie funkcji Imutable Storage
Urządzenie powinno być odporne przed atakami szyfrującymi
Urządzenie po zintegrowaniu z systemem backupowym, powinno być w pełni hermetyczne (brak możliwości skasowania danych zapisywanych przez system backupowi z poziomu urządzenia)
urządzenie musi pozwać na ingracjację z systemami backupowymi z wykorzystaniem technologię AirGap
Redundantne zasilanie,
Interfejsy sieciowe
Min. 2szt. Ethernet 1Gb, Dual SFP + 10 Gb
Gwarancja NBD on-premise o czasie trwania analogicznym do trwania wsparcia technicznego dla oprogramowania.

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.
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. • Wykonawca musi posiadać certyfikat nadany przez uprawniony podmiot potwierdzający realizację usług serwisowych zgodnie z normą PN-EN ISO 27001:2017 lub certyfikat równoważny

Zakup dysków do serwera do wykonywania kopii bezpieczeństwa dla Urzędu Gminy Santok – 1 kpl.

Zamawiający wymaga dostarczenia 8 szt. dysków o parametrach min.: Typ dysku: HDD Format szerokości: 3,5'' (LFF) Typ napędu: Wewnętrzny Pojemność dysku: min. 8 TB Interfejs dysku: SATA Prędkość obrotowa: min.5640 obr/min Bufor: min. 256 MB TBW: min. 180 TB

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

Licencje

Serwerowy System Operacyjny

Oprogramowanie Microsoft Windows Server Standard 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.
Licencje dla Serwerowego Systemu Operacyjnego muszą być dostarczone zgodnie z polityką producenta oprogramowania i uwzględniać wszystkie dostarczane serwery fizyczne

Licencje dostępowe do SSO

Dostarczone licencje dostępowe muszą być zgodne z dostarczanym Serwerowym Systemem Operacyjnym.

Dostarczone licencje muszą pracować w trybie na użytkownika.
Dostarczone licecnje muszą uwzględniać min.: - Urząd Gminy – 35 nazwanych użytkowników - OPS – 15 nazwanych użytkowników

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: • 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

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.

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 24 porty 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.

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

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.

Zakup urządzenia Access Point dla Ośrodka Pomocy Społecznej w Santoku – 1 szt.

Ilość portów RJ-45: min. 3
Ilość portów USB: min. 1
Klient DHCP: Tak
Liczba rdzeni procesora: min. 4
Pobór mocy: 13W
Prędkość transferu danych przez Ethernet LAN: 10,100,1000
Protokoły zarządzające: UNMS, CLI, SNMP, NetFlow, LLDP, NTP
Obsługa jakość serwisu (QoS): Tak
Obsługa sieci VLAN: Tak

Zakup licencji na oprogramowanie antywirusowe

Wymagane jest dostarczenie oprogramowania posiadającego poniższą funkcjonalność
Zamawiający posiada aktywną licencje ESET Protect Entry ON-PREM dla 30 użytkowników.
Zamawiający wymaga przedłużenie tej licencji na okres do 30 czerwca 2026 roku dla 40 użytkowników lub dostarczyć rozwiązanie równoważne.

OPIS RÓWNOWAŻNOŚCI

Administracja zdalna w chmurze:

1. Rozwiązanie musi być dostępne w chmurze producenta oprogramowania antywirusowego.
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu SSL.

4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
6. Rozwiązanie musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
7. Rozwiązanie musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.
9. rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
10. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
11. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.

Ochrona stacji roboczych:

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
3. Rozwiązanie musi wspierać architekturę ARM64.
4. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
6. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
7. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
8. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
9. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
11. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
12. Rozwiązanie musi zapewniać skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
13. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
14. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

15. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
16. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
17. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
- tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

18. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
19. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
20. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
21. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
22. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
23. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
24. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:

- tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
- tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
- tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
- tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.

25. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
26. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
27. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
28. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
29. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
30. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.

31. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

Ochrona serwera:

1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu
2. Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise
3. Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
5. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
6. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
7. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Rozwiązanie musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
8. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
9. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
10. Rozwiązanie musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
11. Dodatkowe wymagania dla ochrony serwerów Windows:
12. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
13. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
14. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
15. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
16. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
17. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
18. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
19. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
20. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
21. Dodatkowe wymagania dla ochrony serwerów Linux:
22. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
23. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
24. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.

Zakup licencji do aplikacji umożliwiającej połączenie się z innym komputerem – 8 szt.

Typ: Zakup licencji do aplikacji umożliwiającej połączenie się z innym komputerem
Zamawiający wymaga dostarczenia licencji oprogramowania do zdalnego dostępu na okres do 30.06.2026 o parametrach minimalnych: Oprogramowanie umożliwia interakcję administratora z użytkownikiem, polegającą na podłączeniu do stanowiska (przejęcie pulpitu) administratora bez konieczności uprzedniego wylogowania użytkownika. Funkcjonalność zdalnego pulpit nie może wymagać instalacji aplikacji firm trzecich, wymagane jest obsłużenie przejęcia zdalnego pulpitu przez mechanizm wbudowany w agencie (ten sam proces systemowy). Oprogramo*wanie umożliwia wybór monitora, kt*órego ekran ma zostać przejęty podczas połączenia zdalnego. Podczas aktywnego połączenia zdalnego, użytkownik jest informowany o trwaniu sesji zdalnej poprzez wyświetlanie na aktywnym monitorze kontrastowego obramowania ekranu. Oprogramowanie umożliwia zdalne zarządzanie (bez użycia RDP/VNC itp.) lokalnymi kontami użytkowników w zakresie (tworzenie, usuwanie, edycja, zmiana hasła oraz typ konta). Oprogramowanie umożliwia wysyłanie polecenia Wake-on LAN. Oprogramowanie umożliwia zdalną dwukierunkową linię poleceń. Oprogramowanie umożliwia przesyłanie plików/katalogów od zdalnego użytkownika do administratora i/lub od administratora do zdalnego użytkownika bez względu na lokalizację sieciową komputera (LAN, WAN, Internet). Oprogramowanie umożliwia konfigurację przez administratora parametrów połączenia z użytkownikiem w zakresie: ilość kolorów, ilość klatek/sekundę, skalowanie okna użytkownika, jeżeli jest ono większe niż rozdzielczość stacji administratora. Oprogramowanie umożliwia wybór aktywnych sesji terminalowych, do których chcemy się podłączyć. Oprogramowanie umożliwia zbiorczy podgląd zdalnych pulpitów stacji. Oprogramowanie posiada zarządzanie technologią iAMT, vPro w zakresie uwzględniającym min.: Serial Over Lan (SOL), IDE Redirection (IDER), Hardware KVM, Assets. Oprogramowanie zapewnia zdalną konfigurację technologii iAMT w trybie Client Control Configuration Mode. Oprogramowanie umożliwia zarządzanie stacjami komputerowymi poza siecią LAN/WAN, wymagane jest tylko dowolne połączenie internetowe Oprogramowanie umożliwia zdalne wykonywanie zapytań WQL Oprogramowanie umożliwia zdalny odczyt oraz modyfikację rejestru Windows Oprogramowanie umożliwia pełne wykorzystanie funkcji zawartych w sekcji zdalne zarządzanie dla stacji posiadających dowolne połączenie do sieci INTERNET bez konieczności zestawiania połączenia VPN Oprogramowanie umożliwia przejęcie pulpitu zdalnego z poziomu konsoli zarządzającej znajdującej się poza siecią LAN organizacji poprzez połącznie konsoli ze wskazanym serwerem aplikacji. Oprogramowanie umożliwia prowadzenie w czasie rzeczywistym dwukierunkowej komunikacji tekstowej (chat) pomiędzy użytkownikiem a administratorem.

Zakup oprogramowania do zabezpieczania danych wraz ze wsparciem

Zarządzanie i magazyny:

1. Produkt dostępny w polskiej wersji językowej.
2. Konsola zarządzająca dostępna z poziomu przeglądarki internetowej
3. System musi umożliwiać tworzenie kopii zapasowych na poziomie dysków
4. System musi umożliwiać tworzenie kopii zapasowych na poziomie plików i folderów
5. System musi umożliwiać replikację kopii zapasowych do wielu lokalizacji docelowych

6. System musi umożliwiać tworzenie kopii zapasowych i przywracanie systemów wykorzystujących UEFI/GPT
7. System musi umożliwiać współpracę z usługą kopiowania woluminów w tle (VSS) firmy Microsoft
8. Możliwość zdefiniowania limitu przepustowości sieciowej z jakiej ma korzystać oprogramowanie backupowe
9. System zarządzania nie może być oparty o relacyjne bazy danych.
10. Rozwiązanie działa w architekturze wykluczającej pojedynczy punkt awarii (awaria jednego z komponentów nie spowoduje przestoju w procesie tworzenia kopii zapasowej).
11. Rozwiązanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera (urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz browsera (urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów).
12. Aplikacje klienckie powinny wysyłać dane z kopii zapasowej bezpośrednio na wskazany magazyn – serwer backupu/usługa zarządzania ani żaden inny element Systemu, nie powinien brać udziału w przesyłaniu danych.
13. Rozwiązanie musi być systemem multi-storage-owym i umożliwia tworzenie wielu repozytoriów danych jednocześnie również na innych środowiskach jako przestrzeń do replikacji danych.
14. System musi oferować mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
15. Rozwiązanie w warstwie sprzętowej powinno bazować na standardowych komponentach architektury x86, bez powiązania i poleganiu na komponentach wyłącznie jednego dostawy (tzw. "no propietary vendor lock").
16. System pozwala administratorowi na ustawienie dowolnego harmonogramu replikacji danych pomiędzy dowolnymi wspieranymi magazynami.
17. System musi umożliwiać wykonywanie kopii obrazu dysku, kopii plików i katalogów oraz kopii maszyn wirtualnych bez ich zatrzymywania z zachowaniem stuprocentowej integralności i spójności danych wewnątrz wykonanej kopii zapasowej.
18. Rozwiązanie musi realizować funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie.
19. Rozwiązanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia.
20. System musi umożliwiać automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku wystąpienia błędu.
21. Rozwiązanie powinno umożliwiać klonowanie planów kopii zapasowych, planów replikacji oraz planów testowego odtwarzania maszyn wirtualnych
22. Rozwiązanie powinno umożliwiać uruchamianie przy zadaniach backupu dowolnych skryptów PRE/POST oraz po wykonaniu migawki VSS.
23. System powinien umożliwiać definiowanie tzw. okna backupowego dla każdego z zadań w celu umożliwienia zarządzania obciążeniem sieci i uwzględnienia okien serwisowych występujących u Zamawiającego.
24. System musi automatycznie dodawać do polityki i harmonogramu tworzenia backupów nowe źródła / maszyny wirtualnych, dodane do bieżącego środowiska (automatyzacja oparta na polityce tworzenia kopii).

25. Rozwiązanie musi udostępniać możliwość podglądu postępu działania dowolnego zadania, w tym zadania wykonywania kopii zapasowych, odtwarzania danych, testowego odtwarzania danych, usuwania danych oraz zadania odświeżania zajętości magazynu na dane.
26. Rozwiązanie musi posiadać system powiadamiania poprzez e-mail oraz Slack o zdarzeniach w następujących przypadkach: zadanie zostało zakończone pomyślnie, zadanie zostało zakończone z ostrzeżeniami, zadanie zostało zakończone z błędem, zadanie zostało anulowane, zadanie nie zostało uruchomione.
27. System powinien umożliwiać wysyłanie powiadomień o statusie wykonanych zadań na dowolne adresy webhook, podawane przez użytkownika,
28. Oferowane rozwiązanie musi być dobrane pod względem wydajności w oparciu o najlepsze praktyki producenta.
29. Rozwiązanie musi być wyskalowane, dobrane pod względem wymaganej funkcjonalności i wydajności stosownie do ilości zabezpieczanych danych i obiektów z uwzględnieniem przyrostu danych (serwery, maszyny wirtualne, bazy danych itp.) zgodnie z opisem w zapytaniu ofertowym.
30. Wydajność oferowanej konfiguracji musi być taka, aby wszystkie funkcje systemu były dostępne w chwili wdrożenia (np. deduplikacja, kompresja, instancja workerów i browserów, replikacja, testowe odtwarzanie maszyn wirtualnych).
31. System pozwala na zmniejszenie rozmiaru przechowywanych i przesyłanych danych poprzez usuwanie zduplikowanych bloków danych ze źródła kopii pomiędzy wszystkimi źródłami w obrębie wszystkich kopii na magazynie danych.
32. Proces deduplikacji musi być możliwy dla każdego z typów obsługiwanych magazynów.
33. Proces deduplikacji nie może wymagać instalacji żadnych dodatkowych komponentów, które będą pośredniczyły w zapisie danych z deduplikowanych
34. Proces deduplikacji nie może posiadać pojedynczego punktu awarii, tym samym musi być dostępny jednocześnie na każdym wspieranym magazynie na dane - również replikacyjnych. Awaria jednego z magazynów na dane nie może wpłynąć na integralność deduplikatów, jak i tablicy deduplikatów na innym magazynie.
35. Proces deduplikacji realizowany jest blokiem o stałej wielkości, którego wielkość może zostać ustalona na etapie wdrożenia rozwiązania zgodnie z najlepszymi praktykami producenta.
36. Proces szyfrowania kopii zapasowych nie może ograniczać procesu deduplikacji w ramach tego samego klucza szyfrującego.
37. Kompresja kopii zapasowych musi obsługiwać jeden z wymienionych algorytmów: LZ4, ZStandard. Dodatkowo, musi umożliwiać określenie szczegółowego poziomu kompresji, w tym: niski, średni, wysoki.
38. Instalacja, modyfikacja ustawień, polityki tworzenia kopii zapasowej systemu nie może wymagać przerwania pracy lub restartu systemu.
39. System musi pozwalać na automatyczne aktualizacje oprogramowania.
40. System musi być w stanie kompresować i szyfrować zabezpieczone dane w systemach NAS.
41. System musi pozwalać na uruchomienie kontenerów Docker w dowolnych urządzeniach NAS w celu ich zabezpieczenia.

42. System tworzenia kopii zapasowej musi przechowywać dane w sposób zapewniający ich niezmienność (tzw. "resilience"), dzięki czemu kopie zapasowe nie będą mogły zostać nadpisane lub zmodyfikowane przez cały okres ich przechowywania, retencji.
43. System zarówno będzie przechowywać dane w kopii zapasowej w postaci zaszyfrowanej jak też ruch wewnątrz systemu również musi być szyfrowany.
44. Archiwum długoterminowych kopii zapasowych musi być szyfrowane, a odzyskiwanie z archiwum obsługiwane z tego samego interfejsu użytkownika, co inne przywracanie dane.
45. System musi mieć mechanizmy chroniące przejęcie konta administratora oraz umożliwiać definiowanie dodatkowych uprawnień dla każdej z predefiniowanych ról użytkowników.
46. System musi pozwalać na gradację uprawnień administratorów - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: system operator, backup operator, restore operator, viewer. Dla każdej z tych ról system musi umożliwiać przypisywanie dodatkowych uprawnień, w tym możliwość zablokowania usuwania danych.
47. Rozwiązanie musi posiadać możliwość nieodwracalnego usuwania danych z magazynu na dane w momencie spełnienia dodatkowych wymogów.
48. W sytuacji, gdyby podstawowe urządzenie tworzenia kopii zapasowej było niedostępne, system musi posiadać możliwość przywrócenia z archiwum za pomocą innej instancji systemu dostarczonej przez tego samego producenta. tzn. archiwum musi zawierać wszystkie informacje konieczne do odzyskania.
49. Rozwiązanie musi umożliwiać uruchomienie konsoli w chmurze producenta zlokalizowanej na terenie Polski, w celu umożliwienia dostępu do środowiska zarządzania kopiami zapasowymi w przypadku czasowej niedostępności środowiska lokalnego.
50. System kopii zapasowej musi umożliwiać dostęp do konsoli administracyjnej z wielu stacji roboczych.
51. System kopii zapasowej musi wykorzystywać mechanizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
52. System powinien posiadać predefiniowane schemat tworzenia kopii zapasowych: Custom, Basic, G-F-S, Forever incremental,
53. Rozwiązanie musi obsługiwać kontrolę dostępu opartą na rolach (RBAC).
54. Możliwość składowania utworzonych kopii zapasowych na magazynach chmurowych Amazon AWS, Azure, Wasabi, Google Cloud Storage, Backblaze B2, magazyny zgodne z S3.
55. Możliwość składowania utworzonych kopii zapasowych na udziałach sieciowych po protokole smb, nfs, iscsi, katalog lokalny
56. Zarządzanie i odzyskiwanie danych z kopii musi odbywać się z tego samego interfejsu użytkownika (konsoli), niezależnie od tego, gdzie znajduje się kopia zapasowa (w chmurze AWS, Azure, GCP, w Data Center czy w usłudze typu SaaS).
57. Czas przechowywania kopii zapasowej (retention time) systemu backupu nie może być zmieniony np. poprzez manipulowanie wskazaniami zegara serwera NTP w celu szybszego ich wyekspirowania - tzn. czasy przechowywania kopii zapasowych nie będą zależne od wskazań zegara czasu serwera NTP, ale będą wykorzystywać technologię, która mierzy upływ czasu.
58. Możliwość generowania raportów dobowych w oparciu o harmonogram

59. Produkt musi posiadać możliwość zapisu kopii zapasowych do magazynu chmurowego dostarczanego bezpośrednio przez producenta oprogramowania (datacenter musi być zlokalizowane na terenie Polski)
60. Produkt musi posiadać możliwość zdefiniowania maksymalnej liczby równocześnie backupowanych urządzeń w ramach jednego planu backupowego, niezależnie od typu urządzenia (np. stacja robocza, serwer, maszyna wirtualna)
61. Możliwość wyświetlenia szczegółowych informacji o chronionym urządzeniu takich jak: CPU, RAM, System operacyjny, Adres IP.
62. Produkt musi posiadać możliwość zdefiniowania poziomu obciążenia magazynu, po osiągnięciu którego zostanie wysłane powiadomienia e-mail. (poziom definiowany indywidualnie dla każdego magazynu)

Wspierane systemy:

Możliwość instalacji oraz uruchomienia agenta backupowego na hostach fizycznych,maszynach wirtualnych czy też kontenerach docker opartych o systemy:
Alpine 3.10+,
Debian: 9+,
Ubuntu: 16.04+,
Fedora: 29+,
centOS: 7+,
RHEL: 6+,
openSUSE: 15+,
SUSE Enterprise Linux (SLES): 12 SP2+,
macOS: 10.13+,
Windows: 7, 8.1, 10(1607+),
Windows Server: 2008 R2+,
Środowisk wirtualnych:
Hyper-V 2016+,
VMware: 6.7+.

Możliwość instalacji oraz uruchomienia serwera zarządzania na hostach fizycznych, maszynach wirtualnych czy też kontenerach docker opartych o systemy:
Debian: 9+
Ubuntu: 16.04+
Fedora: 29+
centOS: 7+
RHEL: 6+
openSUSE: 15+
SUSE Enterprise Linux (SLES): 12 SP2+
Windows Client: 7, 8.1, 10 (1607+)
Windows Server: 2012 R2+,

Środowiska fizyczne i bazy danych:

1. Rozwiązanie powinno umożliwiać tworzenie grup urządzeń w celu automatyzacji procesów podczas pracy z urządzeniami.
2. Produkt musi posiadać możliwość tworzenia zadań dla grupy urządzeń oraz dla wybranych urządzeń.

3. Rozwiązanie musi pozwalać na automatyczne wyłączenie stacji roboczej po wykonaniu kopii zapasowej.
4. Rozwiązanie backupowe musi pozwalać na zabezpieczanie zaszyfrowanych partycji min. BitLocker, Veracrypt, TrueCrypt, Eset Endpoint Encryption.
5. System jest niezależny od wersji Microsoft SQL i musi umożliwiać przywracanie danych SQL dla tej samej lub nowszej wersji.
6. System musi obsługiwać również narzędzia RMAN firmy Oracle do tworzenia kopii zapasowych i odzyskiwania. Dodatkowo system musi obsługiwać funkcję przyrostowego scalania danych.
7. System kopii zapasowej musi wspierać odtwarzanie pojedynczych plików z systemów Windows oraz Linux.
8. W przypadku niedostępności źródła danych, system musi oczekiwać na powrót dostępności źródła danych przez określony przez administratora okres. W przypadku braku powrotu dostępności źródła, system musi podjąć ustaloną przez administratora liczbę prób kontynuacji kopii. W przypadku powrotu źródła danych system musi kontynuować zadanie backupu od momentu, w którym wystąpiła niedostępność źródła - system nie może rozpoczynać zadania od punktu początkowego i rozpoczynać przesyłania kopii od zera. W przypadku braku powrotu źródła danych system powinien zakończyć zadanie błędem.
9. Odtwarzanie Bare Metal Restore w Systemie może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika.
10. Rozwiązanie powinno umożliwiać uruchamianie procesu Bare Metal Restore z dowolnego bootowalnego nośnika danych.
11. Rozwiązanie powinno wspierać odtwarzanie danych w scenariuszach P2P, P2V, V2P, V2V.
12. Rozwiązanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie (RAW, VHD, VHDX, VMDK).
13. Rozwiązanie musi umożliwiać odtwarzanie zasobów plikowych bez praw dostępu (tzw. ACL) oraz z prawami dostępu. Funkcjonalność ta musi być możliwa do skonfigurowania przez administratora na etapie konfiguracji procesu przywracania danych.
14. Rozwiązanie musi umożliwiać przywracanie plików pomiędzy różnymi systemami operacyjnymi i systemami plików (np. odtwarzanie danych plikowych Linux na systemie Windows).

Środowiska wirtualne

1. System musi wspierać kopię w trybie application-aware dla wszystkich wspieranych wirtualizatorów.
2. System musi umożliwiać wykonywanie kopii maszyn wirtualnych z zastosowanie zaawansowanych metod transportu (HotAdd, SAN, LAN), w tym metodami LAN-Free, tj. takimi, które podczas wykonywania backupu nie obciążają interfejsów sieciowych maszyn wirtualnych.
3. System kopii zapasowej musi wykorzystywać mechanizmy Change Block Tracking oraz Replica Change Tracking dla wspieranych przez producenta platformach wirtualizacyjnych.
4. Rozwiązanie producenta musi być certyfikowane przez dostawcę platformy wirtualizacyjnej, tj. producent musi uczestniczyć w programie Technology Alliance Partner.

5. System kopii zapasowej musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage-u użytego do przechowywania kopii zapasowych.
6. Dla środowiska vSphere i Hyper-V rozwiązanie powinno umożliwiać uruchomienie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna).
7. System kopii zapasowej musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSphere.
8. System kopii zapasowej musi umożliwiać weryfikację odtwarzalności wirtualnych maszyn według własnego harmonogramu w dowolnym środowisku.

Licencjonowanie i wsparcie techniczne:

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk.
7. Licencje powinny być dostępne w opcji wieczystej.
8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. 24 miesięcy
9. Sposób licencjonowania opiera się na:
    a. ilości serwerów/endpointów - dla fizycznych urządzeń,
    b. ilości socketów w hostach - dla środowisk wirtualnych lub ilości maszyn wirtualnych,
    c. ilość repozytoriów - dla GIT.
10. Licencje powinny umożliwiać zabezpieczenie w wersji wieczystej:
    a. ilości serwerów/endpointów - dla fizycznych urządzeń,
    b. ilości socketów w hostach - dla środowisk wirtualnych lub ilości maszyn wirtualnych,

Anty-ransomware i bezpieczeństwo:

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.

4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu ani żaden inny komponent, którego awaria sparaliżowałyby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.
5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.

Zakup systemu ochrony poczty – 1szt.

1. System do ochrony poczty powinien spełniać wszystkie wymagania funkcjonalne dotyczące ochorny serwerów fizycznych przedstawione w sekcji „Zakup oprogramowania do zabezpieczania danych wraz ze wsparciem”
2. Powinien pozwalać na wdrożenie na jednym fizycznym serwerze

Licencjonowanie i wsparcie techniczne:

1. Wszystkie linie supportu muszą być obsługiwane w języku polskim.
2. Wsparcie techniczne musi być świadczone bezpośrednio przez główną siedzibę producenta.
3. Możliwość zgłaszania ticketów supportowych bezpośrednio z poziomu interfejsu zarządzania w formie czatu.
4. Producent wraz z rozwiązaniem musi udostępnić materiały samopomocowe w j. polskim (minimum dostęp do bazy wiedzy, materiałów wideo oraz kart produktów)
5. Wsparcie techniczne musi umożliwiać korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego.
6. Licencje w ramach rozwiązania powinny pozwalać na zabezpieczenie określonej przez Zamawiającego ilości hostów w obrębie wspieranych przez System środowisk.
7. Licencje powinny być dostępne w opcji wieczystej.
8. Dostęp do wsparcia technicznego producenta powinno obowiązywać przez okres min. 24 miesięcy
9. Sposób licencjonowania opiera się na:
    a. ilości serwerów/endpointów - dla fizycznych urządzeń

Anty-ransomware i bezpieczeństwo:

1. System plików rozwiązania musi być odporny na ataki Ransomware (zapewnić ochronę przed szyfrowaniem end-to-end, kopie zapasowe nie mogą być nadpisywane - "niezmienny system plików").
2. System powinien umożliwiać wykorzystanie wbudowanego menedżera haseł do przechowywania wszelkich sekretów (haseł, danych dostępowych, kluczy szyfrujących) wykorzystywanych przez System
3. System powinien umożliwiać przywrócenie hasła głównego administratora w przypadku jego utraty.
4. W ramach systemu, komunikacja pomiędzy hostem źródłowym, a magazynem powinna odbywać się tylko i wyłącznie bezpośrednio pomiędzy agentem backupu, a magazynem. Komunikacja nie może przechodzić przez serwer backupu ani żaden inny komponent, którego awaria sparaliżowałyby działanie Systemu. System nie może posiadać pojedynczego punktu awarii.

5. System musi działać w zgodzie z regułą Zero-knowledge Encryption. Oznacza to, że wszelkie sekrety muszą być przechowywane w centralnym Managerze Haseł w postaci zaszyfrowanej algorytmem AES i być udostępniane agentowi dopiero w momencie rozpoczęcia wykonywania kopii zapasowej. Sekrety nie mogą być przechowywane w konfiguracji agenta na zabezpieczonym urządzeniu.

Zakup routera do zapewnienia stabilnego połączenia internetowego dla Ośrodka Pomocy Społecznej w Santoku

Ilość portów Ethernet LAN (RJ-45): min. 1
Liczba użytkowników: min. 300
Maksymalna szybkość przesyłania danych: min. 3000
Maksymalna szybkość przesyłania danych (2.4 GHz): min. 600
Maksymalna szybkość przesyłania danych (5 GHz): min. 2400
Maksymalne zużycie mocy: min. 16,5
Obsługa PoE: Tak
Obsługa sieci VLAN: Tak
Obsługiwane protokoły sieciowe: 802.11?x, 802.11?c, 802.11n, 802.11g, 802.11b, 802.11?, 802.3at, 802.1Q
Poziom wzmocnienia anteny: max. 5,5

Zakup systemu do zarządzania infrastrukturą IT

Zamawiający wymaga dostarczenia licencji na okres do 30.06.2026 o poniższych parametrach dla 40 użytkowników:

- Oprogramowanie musi umożliwiać okresowe skanowanie sieci LAN (wg. zadanych kryteriów, na wybranych serwerach lokalnych) z wykorzystaniem protokołu SNMP, celem prezentacji aktywnych urządzeń IP w zakresie co najmniej komputery, drukarki, routery, smartphony
- Oprogramowanie musi umożliwiać monitorowanie poprzez wykorzystanie protokołu SNMP stanu drukarek tj. poziomy tonerów, liczba wydrukowanych stron oraz informować błędach takich jak brak papieru, zacięcie papieru.
- Oprogramowanie musi umożliwiać wizualizację ruchu sieciowego na poszczególnych portach urządzeń sieciowych wraz z wizualizacją w postaci mapy sieci dla wskazanego urządzenia typu switch, router.
- Oprogramowanie musi umożliwiać z zdalną instalację agenta systemu z poziomu wykrytej struktury sieciowej z wykorzystaniem poświadczeń administracyjnych, w tym również stanowisk poza usługą katalogową.
- Oprogramowanie musi umożliwiać monitorowanie stanu dowolnej usługi sieciowej TCP.
- Oprogramowanie musi umożliwiać monitorowanie dowolnego licznika SNMP(v1/2/3) urządzenia.
- Oprogramowanie musi umożliwiać monitorowanie stanu dowolnego urządzenia sieciowego poprzez odpytywanie typu PING.
- Oprogramowanie musi umożliwiać tworzenie konfigurowalnych zdarzeń sieciowych powodujących wysyłanie komunikatów informacyjnych i/lub ostrzegawczych poprzez SMS i/lub Email.
- Oprogramowanie musi umożliwiać inwentaryzację Systemów Informatycznych oraz Zbiorów danych

- Oprogramowanie musi umożliwiać określanie powiązań pomiędzy pracownikami z Systemami Informatycznymi oraz Zbiorami danych
- Oprogramowanie musi umożliwiać budowanie powiązanych zestawów atrybutów dla Systemów Informatycznych oraz Zbiorów danych (np. termin ważności dostępu, poziom dostępu, przetwarzanie danych wrażliwych)
- Oprogramowanie musi umożliwiać tworzenie ścieżek decyzyjnych dla dowolnych wniosków o uprawnienia do Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać akceptację poszczególnych etapów przez dedykowane osoby decyzyjne zdefiniowane w konfiguracji ścieżek
- Oprogramowanie musi umożliwiać akceptację etapów ścieżki przez automatyczny wybór powiązanych opiekunów merytorycznych oraz technicznych
- Oprogramowanie musi umożliwiać definiowanie dowolnych akcji dla poszczególnych kroków (np. zmiana opiekuna, statusu)
- Oprogramowanie musi umożliwiać automatyczne tworzenie powiązań pracownika z Systemem informatycznym lub Zbiorem danych po akceptacji wniosku
- Oprogramowanie musi umożliwiać obsługę procesu (wniosku) o odebranie uprawnień (koniec terminu dostępu, zwolnienie pracownika)
- Oprogramowanie musi umożliwiać raportowanie uprawnień wg Systemów Informatycznych oraz Zbiorów danych dla poszczególnych osób
- Oprogramowanie musi umożliwiać raportowanie uprawnień w pracowników do Systemów Informatycznych oraz Zbiorów danych
- Oprogramowanie musi umożliwiać generowanie edytowalnej Karty Uprawnień Pracownika
-

Zakup akumulatorów do centralnego UPS dla Urzędu Gminy Santok

Zamawiający posiada UPS APC 15kW, wyposażony w dwa moduły akumulatorów SYBT4.
Zamawiający wymaga wymiany akumulatorów, min. 2 moduły. Zastosowane baterie nie mogą być gorsze niż:
Napięcie na jednostkę: 12V
Pojemność: min. 7.2 Ah
Max. prąd rozładowania 5 sec. :100/130 A
Limit - zalecany maksymalny prąd ładowania:
Gwarancja: min. 12 miesięcy
Zamawiający wymaga, aby wykonawca dokonał montażu, tj. Wymiany pakietów bateryjnych w siedzibie Zamawiającego oraz rekonfiguracji urządzenia UPS.

Doradztwo informatyczno -technologiczne w zakresie wsparcia realizacji projektu

W ramach dostawy przedmiotu zamówienia wymagane jest przeprowadzenie szkolenia dla administratora w zakresie dostarczanego sprzętu, serwerowego oraz sieciowego w zakresie minimum 8 godzin. Dodatkowo, w ramach realizacji szkoleń wymagane jest świadczeniu opieki serwisowej nad posiadaną przez Zamawiającego infrastrukturą serwerową, infrastrukturą sieciową pra urządzeniami do backupu w zakresie minimum 20 godzin, przez okres do 30 czerwca 2026.

Szkolenie osoby odpowiedzialnej za bezpieczeństwo obszaru IT - Oprogramowanie antywirusowe

Wykonawca zapewni certyfikowane szkolenie (minimum 2 dni) dla administratora Zamawiającego (1 osoba) z posiadanego rozwiązania antywirusowego ESET.
Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie powinno zostać dostarczone w formie vouchera.

Wymagania szczegółowe:

- Program szkolenia będzie obejmować w zakresie minimum:
- Omówienie dostępnych produktów,
- Różnice pomiędzy konsolą ON-PREM a chmurową,
- Różnice pomiędzy ochroną na poziomie antywirus i security,
- Przydatne strony WWW,
- Konto administratora -zarządzanie licencjami (ćwiczenie),
- Konsola do zarządzania - architektura i omówienie komponentów,
- Instalacja i aktualizacja serwera z konsolą do zarządzania (ćwiczenie),
- konsola - omówienie funkcji serwera,
- Zarządzanie administratorami i ich uprawnieniami (ćwiczenie),
- Zarządzanie agentami- zdalna instalacja i omówienie możliwości (ćwiczenie),
- Grupy statyczne i dynamiczne,
- Zadania klienta, serwera oraz wyzwalacze,
- Zdalna instalacja klienta antywirusa,
- Typowe scenariusze (ćwiczenia),
- Omówienie funkcji podstawowych i zaawansowanych klienta,
- Ochrona antywirusowa,
- Zarządzanie aktualizacją,
- Polityki i dziedziczenie (ćwiczenie),
- Zapora osobista (ćwiczenie),
- Typowe scenariusze (ćwiczenia),
- Moduł antyspamowy,
- Powiadomienia,
- Raportowanie (ćwiczenie),
- Kontrola dostępu do stron internetowych (ćwiczenie),
- Kontrola dostępu do urządzeń (ćwiczenie),
- Migracja konsoli lokalnej do konsoli chmurowej (ćwiczenie),
- Wdrożenie klienta antywirusa na urządzenia z systemem Android (ćwiczenie),
- Rozwiązywanie problemów.
- Administrator po kursie otrzymuje zaświadczenia ukończenia szkolenia.

Szkolenie osoby odpowiedzialnej za bezpieczeństwo obszaru IT – szkolenie dotyczące rozwiązania UTM

Wykonawca zapewni certyfikowane szkolenie (minimum 3 dni po 8 h dziennie tj. razem minimum 24h) dla administratora Zamawiającego (1 osoba) z posiadanego przez Zamawiającego rozwiązania klasy UTM.
Szkolenie w formie online, zorganizowane w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie powinno zostać dostarczone w formie vouchera

Wymagania szczegółowe:

1. Omówienie programu szkolenia i certyfikacje
2. Rozpoczęcie pracy z urządzeniem UTM
   - Rejestracja w strefie klienta i dostęp zasobów
   - Rozpoczęcie pracy z urządzeniem i wprowadzenie do interfejsu administracyjnego
   - Ustawienia systemowe i uprawnienia administratorów
   - Instalacja licencji i aktualizacja systemu
   - Tworzenie kopii zapasowej i przywracanie konfiguracji
3. Zbieranie logów i monitorowanie
   - Przedstawienie kategorii zbieranych logów
   - Wykresy historyczne i monitorowanie
4. Obiekty
   - Typy obiektów oraz ich wykorzystanie
   - Obiekty sieciowe i obiekt typu „router”
5. Konfiguracja sieci
   - Tryby pracy urządzenia
   - Typy interfejsów (Ethernet, modem, bridge, VLAN, GRETAP)
   - Typy routingu oraz ich priorytety
6. Translacja adresów sieciowych (NAT)
7. Translacja połączeń wychodzących (maskarada)
8. Translacja połączeń przychodzących (przekierowanie)
9. Translacja dwukierunkowa (jeden do jeden)
10. Filtrowanie ruchu sieciowego (Firewall)
11. Ogólne informacje dot. filtrowania ruchu i koncepcji śledzenia połączeń (Stateful inspection)
    - Szczegółowy opis parametrów reguły Firewall
    - Kolejność przetwarzania reguł Firewall i NAT
12. Ochrona aplikacji
13. Implementacja filtrowania URL dla ruchu http i https
14. Konfigurowanie skanowania antywirusowego i modułu Breach Fighter
15. Moduł IPS i stosowanie profili inspekcji
16. Użytkownicy i uwierzytelnianie
17. Konfiguracja usługi katalogowej
18. Wprowadzenie do różnych metod uwierzytelniania (LDAP, Kerberos, Radius, certyfikat SSL, SPNEGO, SSO)
19. Rejestracja użytkowników
20. Uwierzytelnianie użytkowników za pomocą portalu uwierzytelniania
21. Wirtualne sieci prywatne (VPN)

22. Koncepcje i ogólne informacje dotyczące protokołu IPSec VPN (IKEv1 i IKEv2)
23. Tunele Site-to-Site z wykorzystaniem klucza współdzielonego (PSK)
24. Tunele VTI
25. SSL VPN
26. Zasada działania
27. Konfiguracja