

OPIS PRZEDMIOTU ZAMÓWIENIA

„Dostawa wraz z wdrożeniem sprzętu informatycznego w celu modernizacji systemów bezpieczeństwa, sieci LAN, systemów Datacenter, infrastruktury IT szpitala”

Zakres przedmiotu zamówienia obejmuje:

1. Zintegrowana zapora sieciowa UTM – ochrona środowiska wirtualnego i systemów szpitala przed zagrożeniami z sieci publicznej, zarządzanie politykami bezpieczeństwa
2. System ochrony poczty elektronicznej zapewniający zaawansowane filtrowanie spamu, ochronę przed phishingiem, malware oraz złośliwymi załącznikami, archiwizacja
3. Repozytorium danych dla środowiska wirtualnego – macierz dyskowa jako magazyn dla maszyn wirtualnych
4. Serwery klastra wysokiej dostępności (2 szt.)
5. Niezależny system backupu - serwer wraz z biblioteką taśmową, oprogramowaniem backupowym oraz urządzeniem typu NAS
6. Segmentacja sieci i zwiększenie przepustowości – dostosowanie sieci LAN do wymagań środowiska wirtualnego, podział na strefy bezpieczeństwa, podniesienie przepustowości łącza, rewitalizacja punktów dystrybucyjnych
7. Switche dostępne – rozbudowa infrastruktury LAN, zapewniająca bezpieczny dostęp do środowiska wirtualnego i usług IT dla użytkowników (10 szt.)
8. Switch warstwy rdzeniowej (2 szt.)
9. Zakup małych switchy dostępowych w celu eliminacji obecnie pracujących urządzeń bez wsparcia (mini switchy) (10 szt.)
10. Pakiet ochrony antywirusowej – zabezpieczenie serwerów, maszyn wirtualnych oraz urządzeń końcowych przed zagrożeniami malware, ransomware i innymi atakami
11. System zarządzania urządzeniami końcowymi – centralna kontrola nad infrastrukturą IT, monitoring stacji roboczych i serwerów, wsparcie dla bezpieczeństwa środowiska IT
12. 7 System NAC (kontrola dostępu do sieci) – zapewnienie bezpieczeństwa sieci poprzez segmentację, autoryzację urządzeń i użytkowników, ochrona przed nieautoryzowanym dostępem
13. Oprogramowanie do monitoringu infrastruktury
14. Oprogramowanie do przechowywania logów z urządzeń sieciowo/serwerowych
15. Komputery dla administracji i obsługi środowiska wirtualnego – stacje robocze dla personelu odpowiedzialnego za zarządzanie i utrzymanie infrastruktury IT szpitala, UPS do komputera (20szt.)

16. Szkolenia w zakresie dostarczonego sprzętu oraz technologii
17. Wdrożenie infrastruktury IT – instalacja i konfiguracja klastra wirtualnego, usług katalogowych (AD), backupu, systemów bezpieczeństwa i segmentacji sieci
18. UPS rackowy do podtrzymania i wygaszenia maszyn w momencie awarii (3 szt.)

W ramach zamówienia Wykonawca przedstawi Zamawiającemu Analizę Przedwdrożeniową (AP) oraz Projekt Techniczny (PT) planowanego rozwiązania.

Zamawiający przystąpi do realizacji zadania zgodnie z PT po zatwierdzeniu dokumentów : AP i PT.

Zamawiający może wezwać Wykonawcę do wyjaśnień i poprawy dokumentów AP i PT. Wykonawca w przeciągu trzech dni roboczych od wezwania musi przedstawić Zamawiającemu wyjaśnienia i poprawione dokumenty.

Po wykonaniu zamówienia Wykonawca przedstawi Zamawiającemu Dokumentację Powdrożeniową (DP). DP zawierać musi opis wdrożonych rozwiązań oraz instrukcje konfiguracji wdrożonych rozwiązań.

Kolejnym etapem realizacji zamówienia są szkolenia /instruktaże dla administratorów Zamawiającego z wdrożonego rozwiązania. Szkolenia /instruktarze prowadzone będą dla 3 osób. Ilość godzinowa oraz forma szkolenia (on-line/ stacjonarnie) zostanie ustalona wspólnie przez Zamawiającego i Wykonawcę . Zamawiający zastrzega wymóg przeprowadzenia co najmniej 16 godzin instruktażu w ramach realizacji zamówienia.

1. Zintegrowana zaporą sieciową UTM- ochrona środowiska wirtualnego i systemów szpitala przed zagrożeniami z sieci publicznej, zarządzanie politykami bezpieczeństwa

W ramach zadania Wykonawca dostarczy nowe urządzenia (Co najmniej dwa urządzenia pracujące w klastrze HA, spełniające poniższe wymagania z okresem licencji i wsparcia serwisowego na minimum 36 miesięcy.

Wymagania funkcjonalne:

1. Zaporą sieciową typu Next Generation Firewall (NGFW),
2. Mechanizm pozwalający na dwustronną analizę ruchu bez proxy oraz ograniczeń na rozmiar skanowanego pliku.
3. Minimalna ilość interfejsów:
 - a) 10 interfejsów 10 GbE SFP+,
 - b) 24 interfejsy RJ-45 Ethernet 10/100/1000 – każdy z interfejsów musi mieć możliwość konfiguracji osobnej podsieci i strefy bezpieczeństwa.
 - c) 2 interfejsy USB 3.0 dla przyszłych potrzeb i do podłączenia modemu 3G,
 - d) 1 interfejs konsoli do zarządzania zaporą,

- e) 1 interfejs RJ-45 Ethernet 10/100/1000 do zarządzania zaporą,
4. Zapora powinna posiadać dysk M.2 o pojemności przynajmniej 256 GB z możliwością wymiany na większy.
5. Możliwość przypisania wielu interfejsów fizycznych do pojedynczej strefy bezpieczeństwa
6. Możliwość powiązania wielu interfejsów fizycznych w jeden port logiczny (agregacja portów) celem podniesienia wydajności połączeń oraz zapewnienia redundancji,
7. Możliwość utworzenia przynajmniej 256 interfejsów logicznych VLAN, wsparcie dla standardu 802.1q,
8. Obsługa nielimitowanej ilości hostów podłączonych w sieci chronionej,
9. Minimalna ilość jednocześnie obsługiwanych połączeń: 3 000 000,
10. Możliwość obsłużenia przynajmniej 90 000 nowych połączeń w ciągu 1 sekundy.
11. Przepustowość urządzenia pracującego w trybie stateful firewall: 12 Gbps – dla ramki 1518B zgodnie z RFC 2544,
12. Przepustowość urządzenia pracującego z włączonym mechanizmem IPS: 8 Gbps,
13. Przepustowość urządzenia pracującego jako koncentrator VPN: 8 Gbps dla szyfrowania AES bez aktywnych usług UTM, zgodnie z RFC 2544,
14. Przepustowość urządzenia DPI/NGFW (z włączonymi wszystkimi usługami bezpieczeństwa – antivirus, antyspyware, IPS, bez buforowania i proxy i bez ograniczeń jeśli chodzi o wielkość skanowanych plików) – 8,0 Gbps,
15. Minimalna ilość jednocześnie zestawionych tuneli site-site VPN (urządzenie – urządzenie): 3 000,
16. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site SSL VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 2 z możliwością rozszerzenia do przynajmniej 500
17. Minimalna ilość licencji umożliwiających zestawienie połączeń client-site IPSec VPN (komputer – urządzenie), dostępnych w pakiecie z urządzeniem: 50 z możliwością rozszerzenia do przynajmniej 1 000.
18. Urządzenie powinno umożliwiać poddanie inspekcji zawartości ruchu szyfrowanego SSL/TLS poprzez jego odszyfrowanie i ponowne zaszyfrowanie zmienionym certyfikatem. Administrator powinien mieć możliwość tworzenia wyjątków do inspekcji ruchu SSL poprzez wykorzystanie kategorii stron np. wyłączenie z inspekcji kategorii zawierających strony bankowe i medyczne.
19. Wydajność urządzenia z włączoną funkcją inspekcji ruchu SSL/TLS powinna wynosić minimum 3 Gbps oraz obsłużyć 300 000 połączeń.
20. Obsługa IPSec, ISAKMP/IKE, Radius, L2TP, PPPoE, PPTP,

21. Zintegrowany serwer DHCP, umożliwiający przydzielanie adresów IP dla hostów znajdujących się w sieci chronionej, a także dla hostów połączonych poprzez VPN (dla tuneli nawiązanych w trybie site-site oraz client-site),
22. Wsparcie funkcjonalności IP Helper, lub IP Relay (przekazywanie komunikacji DHCP pomiędzy strefami bezpieczeństwa),
23. Uwierzytelnianie użytkowników w oparciu o wewnętrzną bazę użytkowników, oraz z wykorzystaniem zewnętrznych mechanizmów RADIUS/XAUTH, Active Directory, SSO, LDAP,
24. Wsparcie dla Dynamicznego DNS tzw. DDNS,
25. Zintegrowany mechanizm kontroli zawartości witryn pogrupowanych na kategorie tematyczne.
26. Mechanizm kontroli treści powinien mieć możliwość filtrowania stron tłumaczonych przez google translate (strony takie również powinny być poddane inspekcji, na takich samych zasadach jak strony na które użytkownik wchodzi bezpośrednio).
27. Administrator powinien mieć możliwość tworzenia różnych akcji dla stron które zostały wychwycone przez filtr treści. Powinny być dostępne takie akcje jak:
 - a) wyświetlenie strony blokady (z możliwością tworzenia kilku różnych stron),
 - b) wyświetlenie strony blokady z możliwością podania hasła odblokowującego dostęp do zablokowanej strony,
 - c) wyświetlenie informacji z polityką bezpieczeństwa organizacji podczas wchodzenia na strony z danej kategorii. Użytkownik może wejść na stronę po akceptacji polityki.
28. Administrator powinien mieć możliwość stworzenia polityki kontroli treści obejmującego np. strony z kategorii Multimedia i przydzielenia ograniczonego pasma dla stron w tej kategorii np. 5 Mbps,
29. Zintegrowany mechanizm kontroli transmisji poczty elektronicznej w oparciu o zewnętrzne serwery RBL.
30. Zintegrowany mechanizm zabezpieczający bezprzewodową sieć LAN, umożliwiający szyfrowanie transmisji w połączeniach bezprzewodowych realizowanych pomiędzy dodatkowymi urządzeniami Access Point a stacjami roboczymi za pomocą IPSec VPN. System wspomagania uwierzytelniania bezprzewodowych stacji roboczych, oraz użytkowników, pozwalający na wdrożenie polityki dostępowej dla sieci.
31. Możliwość uruchomienia minimum dwóch łączy WAN - Zintegrowane funkcje Load-Balancing, oraz Failover. Funkcja Failover oparta o badanie stanu łącza i badanie dostępności hosta zewnętrznego.
32. Możliwość ograniczenia ruchu na zewnętrznej stacji roboczej podczas pracy zdalnej VPN (dostęp tylko do udostępnionych zasobów lub dostęp do udostępnionych zasobów oraz

zasobów sieci Internet z uwzględnieniem filtrowania treści, mechanizmu IPS oraz ochrony przed wirusami i wszelkim innym oprogramowaniem złośliwym dla komputerów połączonych przez VPN),

33. Kontrola dostępności zestawionych tuneli VPN,
34. Możliwość zarządzania urządzeniem z wykorzystaniem protokołów http, https, SSH i SNMP.
35. Konfiguracja oparta na pracy grupowej/obiektowej. Polityka bezpieczeństwa pozwalająca na całkowitą kontrolę nad dostępem do Internetu powinna być tworzona według reguł opartych o grupy i obiekty.
36. Przy tworzeniu reguł dostępowych zapewniona możliwość konfiguracji trzech typów reakcji: allow, deny, discard (zezwolić, zabronić, odrzucić),
37. Funkcja NAT oparta o reguły bezpieczeństwa.
38. NAT w wersji jeden-do-jeden, jeden-do-wielu, PAT, wiele-do-wielu, wiele-do-jednego. Funkcje oparte o zaawansowaną konfigurację według reguł bezpieczeństwa (m.in. możliwość ograniczenia działania funkcji do niektórych hostów, możliwość translacji portów wyjściowych na inne docelowe),
39. Zintegrowany system skanowania antywirusowego na poziomie bramy internetowej – skanowanie protokołów http, ftp, pop3, smtp, imap4, tcpstream. Możliwość filtrowania załączników poczty. Skanowanie również plików skompresowanych.
40. Zintegrowany system skanowania antyspyware,
41. Zintegrowany system IPS (system wykrywania i blokowania wtargnięć) oparty o sygnatury ataków uwzględniające zagrożenia typu worm, Trojan, dziury systemowe, peer-to-peer, bufferoverflow, komunikatory, niebezpieczne kody zawarte na stronach www.
42. System IPS musi używać algorytmu szeregowego przetwarzania.
43. Zintegrowany system zapory działającej w warstwie aplikacji, umożliwiający definiowanie własnych sygnatur aplikacji z wykorzystaniem ciągu znaków lub wyrażeń regularnych (regex).
44. Systemy skanowania IPS/Antywirus/Antyspyware muszą umożliwiać skanowanie ruchu w warstwie aplikacji,
 - a) Bazy w/w systemów muszą być aktualizowane co najmniej raz dziennie.
 - b) Administrator systemu musi mieć możliwość ręcznej aktualizacji sygnatur (online lub offline poprzez manualne zaimportowanie sygnatur,
 - c) Administrator systemu musi mieć możliwość skonfigurowania, którym portem i łączem urządzenie będzie się kontaktowało z serwerami backend w celu aktualizacji sygnatur.
45. System IPS/Antywirus/Antyspyware nie może posiadać ograniczeń związanych z rozmiarem skanowanych plików.

46. Skanowanie IPS/Antywirus/Antyspyware musi być możliwe między strefami bezpieczeństwa,
47. Możliwość pełnej kontroli nad programami typu P2P, IM oraz aplikacjami multimedialnymi,
48. Wsparcie mechanizmów QoS – Priorytet pasma, maksymalizacja pasma, gwarancja pasma, DSCP, 802.1p,
49. Wsparcie dla komunikacji VoIP - Pełne wsparcie dla SIP, H323v.1-5, zarządzanie pasmem (ruch wychodzący), VoIP over WLAN, śledzenie i monitorowanie połączeń, Urządzenie powinno mieć możliwość analizy behawioralnej (sandbox) minimum plików wykonywalnych PE, PDF, Office i aplikacji mobilnych. Sandbox powinien działać z wykorzystaniem minimum 4 silników pochodzących od różnych producentów w celu zwiększenia skuteczności analizy sandbox. Analiza powinna być wykonywana równolegle na wszystkich silnikach. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
50. Urządzenie umożliwia bezpieczne uwierzytelnianie i autoryzację między dostawcami tożsamości (IdP) a dostawcami usług (SP) z użyciem protokołu SAML
51. Urządzenie umożliwia rozpoznanie zalogowanej osoby na końcówce na podstawie event logów w AD, WMI, NetApi.
52. Urządzenie powinno posiadać możliwość realizacji funkcjonalności SD-WAN bazując minimum na poniższych parametrach: Jitter, Latency, Packet Loss. Funkcjonalność nie może wymagać zakupu dodatkowych licencji.
53. Urządzenie powinno posiadać zintegrowany kontroler sieci bezprzewodowej kompatybilny z punktami dostępowymi pochodzącymi od tego samego producenta i pozwalający na obsługę do 512 takich punktów dostępowych sieci bezprzewodowej.
54. Wymagane jest dostarczenie dodatkowego urządzenia pełniące funkcję standby w klastrze wysokiej dostępności (HA) z urządzeniem podstawowym. Urządzenie standby powinno mieć identyczne parametry wydajnościowe jak podstawowa jednostka. Urządzenia powinny synchronizować pomiędzy sobą stany sesji połączeń.
55. Gwarancja: Min. 36 mc, wsparcie w trybie 24x7.
56. Wymagane licencje:
 - Subskrypcje pozwalające na aktualizację sygnatur aplikacji, IPS i wirusów oraz dostęp do bazy URL dla modułu kontroli aplikacji, sandboxing na okres 3 lat.
 - Licencja na centralne zarządzanie DNS z funkcjami takimi jak filtrowanie zapytań DNS. Usługa bazując na 19 predefiniowanych kategoriach, umożliwia utworzenie polityk pozwalających podjęcie 4 działań w oparciu o skonfigurowane profile. Licencje ważne 3 lat.
 - Licencja na usługę przechowywania logów z systemu firewall i generowania na ich podstawie raportów oraz oprogramowanie do zarządzania systemami firewall. Obydwie

funkcjonalności muszą być obsługiwane z tej samej konsoli zainstalowanej lokalnie w siedzibie klienta. Licencja powinna umożliwiać przechowywanie logów przez okres jednego roku. Eksport danych z zapory sieciowej powinien odbywać się za pomocą protokołu IPFIX. W celach zapewnienia kompatybilności oprogramowanie powinno pochodzić od tego samego producenta co system firewall. Wymagana jest licencja, która pozwoli na korzystanie z oprogramowania przez okres 3 lat. Licencja powinna umożliwiać wygenerowanie co najmniej 40 rodzajów raportów. Rodzaje raportów dostępnych w ramach licencji, m.in.:

- Raporty zagrożeń (Threat Reports)
- Wykryte ataki (IPS, malware, botnety)
- Źródła zagrożeń (IP, geolokalizacja)
- Typy zablokowanych zagrożeń
- Analityka aplikacji

System do zarządzania powinien umożliwiać m.in.:

wykonywania szablonów konfiguracyjnych i zarządzania nimi, tworzenia sieci VPN oraz konfiguracji SD-WAN za pomocą kreatora, zastosowania konfiguracji o wybranej porze dnia, znajdowania różnic pomiędzy konfiguracją zapisaną na urządzeniu a nową tworzoną przez administratora.

2. System ochrony poczty elektronicznej zapewniający zaawansowane filtrowanie spamu, ochronę przed phishingiem, malware oraz złośliwymi załącznikami, archiwizacja

W ramach zadania Wykonawca wdroży rozwiązanie do ochrony poczty elektronicznej Zamawiającego wraz z licencjami na okres 36 miesięcy obejmującymi wymienione poniżej funkcjonalności spełniające poniższe wymagania z okresem licencji i wsparcia serwisowego 36 miesięcy.

Zamawiający wymaga aby wdrożone rozwiązanie zostało zintegrowane z systemem pocztowym wykorzystywanym przez Zamawiającego tj. hosting zewnętrzny – obecnie cyberfolks.pl

Zamawiający wymaga systemu ochrony poczty:

1. System ochrony poczty musi być dostarczony w formie dwóch identycznych specjalizowanych maszyn wirtualnych oraz centralnego systemu zarządzania w formie maszyny wirtualnej.
2. Centralny system zarządzania umożliwia rozbudowanie klastra wysokiej dostępności do 15 urządzeń w postaci maszyn wirtualnych lub fizycznych. Klaster wysokiej dostępności obsługuje środowisko mieszane, tzn. działanie maszyn wirtualnych i fizycznych jednocześnie.
3. System musi wspierać platformę ESXi co najmniej w wersji 5.5 oraz Hyper-V.

4. Dla zapewnienia wysokiej wydajności maszyny wirtualne powinny obsługiwać co najmniej:
 - 64 GB pamięci RAM
 - Dysk 160 GB
 - 8 CPU
5. System powinien umożliwiać funkcjonowanie jako MTA (Mail Transfer Agent) ze wsparciem dla protokołu SMTP oraz pracę w trybie PROXY.
6. System powinien posiadać własne filtry reputacji oraz mechanizmy antyphishingowe oraz antyspamowe.
7. System musi umożliwiać weryfikację maili przychodzących oraz wychodzących.
8. Możliwość wykorzystania rekordów SPF oraz mechanizmu DKIM oraz DMARC
9. Dla maili wychodzących system umożliwia wstawienie podpisu cyfrowego do nagłówka wiadomości.
10. System musi umieć analizować raporty DMARC i generować na ich podstawie statystyki oparte na gotowych szablonach dostarczonych przez producenta rozwiązania.
11. Automatyczna aktualizacja filtrów bez przerywania pracy.
12. Musi posiadać wewnętrzną konsolę do administrowania (Web), bez potrzeby instalowania klientów
13. Możliwość stworzenia kwarantanny per użytkownik. Umożliwianie użytkownikowi zarządzania własną kwarantanną, usuwanie wiadomości lub zwolnienie tych, które nie uważają za SPAM, a także możliwość blokowania e-maili. Kwarantanna może być implementowana z bezpośrednią integracją z aplikacji poczty e-mail lub przez interfejs WWW (HTTPS)
14. Możliwość uruchomienia konsoli web, dzięki której użytkownicy mogą sprawdzać wiadomości, które są poddawane kwarantannie ze względu na spam
15. Możliwość, aby użytkownicy sami tworzyli listy wyjątków dla nadawców w konsoli web
16. Umożliwianie użytkownikom na przeglądanie podejrzanych wiadomości w kwarantannie i zaakceptowanie nadawców bez interwencji administratora;
17. Umożliwianie użytkownikowi na utworzenie osobistych, białych list (zaufanych adresów), niezależnie od administratora, tak aby te białe listy nie kolidowały z filtrami innych użytkowników;
18. Moduł kwarantanny powinien znajdować się w samym systemie antyspamowym i być w stanie wysłać okresowe powiadomienie do użytkowników, informując o wiadomościach traktowanych jako SPAM, które zostały wstawione do kwarantanny.

19. Użytkownik powinien być w stanie automatycznie usunąć wiadomości poddane kwarantannie zgodnie z ustawieniami określonymi przez administratora;
20. System powinien dawać możliwość powiadomienia administratora pocztą e-mail, jeśli filtry antyspamowe nie otrzymują aktualizacji przez pewien czas. Przyjmuje się alternatywnie, że administrator zostanie powiadomiony w przypadku błędów aktualizacji.
21. Rozwiązanie powinno być w stanie tworzyć i zarządzać wieloma grupami użytkowników i definiować zróżnicowane reguły i polityki dla każdej z tych grup. System powinien integrować się z bazą LDAP.
22. Rozwiązanie umożliwia stosowanie filtrów, które aplikowane są przed wejściem wiadomości do systemu. Filtry te muszą mieć możliwość klasyfikacji różnych typów zachowań (takich jak białe i czarne listy). Filtry połączeń muszą być konfigurowane przynajmniej przez:
 - a. Adres IP
 - b. Zakres adresów IP
 - c. Muszą wspierać RBL (listy oparte o DNS)
 - d. Muszą posiadać i mieć możliwość używania filtrów reputacji
 - e. Muszą być w stanie definiować następujące polityki:
 - a. Limit ilości odbiorców na wiadomość
 - b. Limit wielkości wiadomości
 - f. Pozwalać lub zabraniać używania SSL/ TLS dla połączeń
 - g. Używać antyspam
 - h. Musi wspierać SSL / TLS dla połączeń przychodzących i wychodzących
 - i. Musi mieć możliwość używania odwrotnej translacji adresów DNS (revDNS)
23. Urządzenie powinno wspierać wiele domen (rekordów MX) oraz obsługiwać routing wiadomości w oparciu o każdą z tych domen.
24. Kolejki dostarczania w oprogramowaniu MTA muszą być na tyle duże, aby wspierać przeładowanie wiadomościami w sytuacji awarii albo problemów w innych punktach infrastruktury pocztowej.
25. Powinna być możliwość zarządzania kolejkami, oraz posiadać opcja wstrzymania i uruchomienia kolejki oraz kasowania wiadomości z kolejki
26. Rozwiązanie powinno wspierać unikalne profile, które obsługują zachowanie wiadomości odbijanych bazując na domenach lub na docelowych adresach IP.
27. Rozwiązanie musi wspierać kilka kwarantann znajdujących się na urządzeniu fizycznym lub wirtualnym, gdzie wiadomości muszą być przechowywane przez okres wskazany przez administratora.

28. Moduł kwarantanny powinien być w stanie wysłać okresowe powiadomienie dla użytkowników, informując o wiadomościach traktowanych jako spam, które zostały przeniesione do kwarantanny.
29. Directory Collection Protection: rozwiązanie musi posiadać ochronę przed tego typu atakami dzięki skanowaniu odbiorcy wiadomości w LDAP, Active Directory.
30. DoS: system operacyjny urządzenia fizycznego lub wirtualnego powinien mieć możliwość identyfikacji i ochrony MTA przed atakami typu DoS.
31. System uwierzytelniania powinien mieć ochronę przed atakami (np. atak słownikowy).
32. Posiadać funkcję zapory e-mail, chronić serwer poczty przed atakiem typu Directory Harvest Attack (DHA)
33. Posiadać funkcję zapory e-mail zdolną do odroczenia połączenia SMTP, jeśli źródło wysyłania wysłało w określonym czasie procentową liczbę wiadomości traktowanych jako spam, obie wartości konfigurowane przez administratora
34. Filtry ochrony przed spamem powinny skanować wszystkie części wiadomości, w tym:
 - a. Nadawcy (komenda SMTP MAIL FROM)
 - b. Odbiorcy (komenda SMTP RCPT TO)
 - c. Nagłówek wiadomości
 - d. Treść wiadomości e-mail
 - e. Załączniki wiadomości e-mail
35. Filtry bezpieczeństwa:
 - A. Urządzenie musi posiadać mechanizm identyfikacji treści wiadomości takich elementów jak: numer karty kredytowej, RG i / lub CPF.
 - B. Musi posiadać mechanizmy tworzenia katalogów słów należących do konkretnych tematów, takich jak przestępstwa.
 - C. Musi zezwalać na heurystyczną weryfikację nowo wprowadzonych wirusów, nawet bez dostępnej szczepionki;
 - D. Musi pozwalać na weryfikację rzeczywistego typu pliku nawet po zmianie nazwy;
 - E. Umożliwiać skanowanie plików wykonywalnych skompresowanych;
 - F. Posiadać ochronę przed oprogramowaniem szpiegującym bez potrzeby dodatkowego oprogramowania lub agenta;
 - G. Ochrona przed Dialerami bez potrzeby dodatkowego oprogramowania lub agenta;
36. Rozwiązanie umożliwia archiwizowanie maili przychodzących oraz wychodzących za pomocą dwóch metod: zapisywanie ich na zasobie dyskowym, przekazywanie do zewnętrznego serwera SMTP.

37. Rozwiązanie analizuje pliki przesyłane za pomocą trzech zewnętrznych silników antywirusowych.
38. Rozwiązanie powinno umożliwiać wysyłanie plików do dodatkowej analizy w systemie sandbox przy czym system sandbox powinien posiadać co najmniej cztery równoległe działające silniki w tym dwa pochodzące od innego producenta.
39. Rozwiązanie umożliwia analizę przesyłanych linków w treści maila w trybie ciągłym, tzn. poprzez podmianę oryginalnego linku na system ochrony poczty.

Licencje:

System powinien zostać dostarczony z licencjami do ochrony **100 skrzynek pocztowych**.

Licencje powinny zapewniać ochronę antyspam, antyphishing, antywirus, sandboxing oraz wsparcie techniczne **24x7 na okres 3 lat**

Dodatkowo, Zamawiający wymaga dostarczenia narzędzia do wykonywania kopii zapasowej poczty o parametrach niegorszych niż:

Wymaganie	Opis
Okres dostępu do oprogramowania w przypadku oprogramowania typu SaaS	36 miesięcy
Obsługa nieograniczonej liczby skrzynek	Możliwość wykonywania backupu dla dowolnej liczby kont e-mail w zakresie określonego limitu pojemności (500GB).
Limit pojemności	Łączna pojemność przechowywanej kopii zapasowej e-mail wynosi 500GB, niezależnie od liczby obsługiwanych skrzynek.
Automatyczne i przyrostowe kopie zapasowe	Automatyczne tworzenie kopii zapasowych nawet do 12 razy dziennie, każda kopia jest przyrostowa, umożliwiając szybkie odzyskiwanie danych bez zajmowania zbędnego miejsca.
Obsługa wielu technologii	Backup e-mail z IMAP/POP3, Microsoft Exchange, Google Workspace (Gmail).
Granularne odzyskiwanie danych	Możliwość przywracania całych skrzynek, wybranych folderów, pojedynczych wiadomości lub załączników jednym kliknięciem.
Bezpieczne szyfrowanie danych	Szyfrowanie danych na poziomie AES-256 (w spoczynku i podczas transmisji).
Wsparcie dla RODO i standardów bezpieczeństwa	Usługa zgodna z wymaganiami RODO/GDPR oraz licznymi normami bezpieczeństwa (SOC2, ISO 27001 itd.).
Intuicyjny panel administracyjny	Dostęp do panelu zarządzania kontami użytkowników, monitorowania stanu kopii i powiadomień.

Zaawansowane wyszukiwanie	Możliwość szybkiego wyszukiwania z użyciem ponad 20 kryteriów w backupowanych wiadomościach
---------------------------	---

3. Repozytorium danych dla środowiska wirtualnego – macierz dyskowa jako magazyn dla maszyn wirtualnych

Macierz dyskowa w konfiguracji:		
Lp.	Nazwa parametru	Minimalna wartość parametru
	Obudowa i komponenty	System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19". Podzespoły macierzy tj. wentylatory, zasilacze muszą być w pełni redundantne żeby zapewnić odpowiedni poziom bezpieczeństwa.
2.	Pojemność:	<p>System musi zostać dostarczony w konfiguracji zawierającej minimum:</p> <p>10 dysków 15.3TB NVME na pętli 100GbE</p> <p>oraz posiadać możliwość rozbudowy o kolejne dyski w obudowie do minimum 72 dysków w ramach klastra dwóch kontrolerów.</p> <p>System wielo-kontrolerowy musi wspierać dyski o wielkościach:</p> <ul style="list-style-type: none"> NVME: od 1900GB do co najmniej 60 000GB
3.	Kontroler	<p>Dwa kontrolery wyposażone w przynajmniej 64GB cache każdy.</p> <p>W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania baterijnego przez minimum 72 godziny lub za pomocą zrzutu danych na pamięć nie ulotną.</p> <p>Procesory macierzy powinny być wykonane w technologii INTEL lub AMD wielordzeniowej z przynajmniej 20 rdzeniami na klastery. Zamawiający dopuszcza alternatywne procesory z min 96 rdzeniami.</p> <p>Macierz musi pozwalać na rozbudowę do przynajmniej 480 dysków w obrębie pary kontrolerów lub klastra w szczególności rozbudowę w technologii NVMe z obsługą min 480 dysków min 30TB w technologii NVME.</p>
4.	Interfejsy	<p>Oferowana macierz musi posiadać minimum:</p> <p>8 portów 10GbE z wkładkami SFP+</p> <p>4 porty 100GbE</p>

		<p>2 porty 1Gb RJ45</p> <p>Macierz musi pozwalać na rozbudowę lub wymianę na dodatkowe porty:</p> <p>8 portów 64Gb FC</p> <p>8 portów 25GbE</p> <p>4 porty 100GbE</p> <p>Jeśli korzystanie z któregoś z wyżej wymienionych portów wymaga zastosowania wkładek (np. SFP+), zamawiający wymaga ich dostarczenia wraz z urządzeniem. Dla portów 100GbE zamawiający wymaga dostarczenia kabli DAC.</p>
5.	RAID	System RAID musi zapewniać taki poziom zabezpieczania danych, aby był możliwy do nich dostęp w sytuacji awarii minimum dwóch dysków w grupie RAID
6.	Kopie Migawkowe	Macierz musi być wyposażona w system kopii migawkowych, dostępny dla wszystkich rodzajów danych przechowywanych na macierzy. System kopii migawkowych nie może powodować spadku wydajności przy odczycie więcej niż 5%.
7.	Obsługiwane protokoły	Macierz musi obsługiwać jednocześnie protokoły FC; iSCSI; NFS; CIFS/SMB, S3 , NVME over FC, NVME over IP. Zamawiający w tym postępowaniu wymaga dostarczenia licencji na wszystkie protokoły.
8.	Inne wymagania	<p>Macierz musi posiadać funkcjonalność eliminacji (deduplikacji) identycznych bloków danych in-line. Macierz musi posiadać także funkcjonalność kompresji danych in-line.</p> <p>Jeżeli oferowane rozwiązanie nie pozwala na deduplikację i kompresję w locie lub nie posiada możliwości deduplikacji i kompresji zamawiający wymaga dostarczenia 4-krotnej pojemności wyspecyfikowanej w punkcie 2. Zamawiający wymaga by dostarczona licencja nie miała żadnych ograniczeń pojemnościowych a także została dostarczona na najwyższy możliwy stopień deduplikacji/kompresji, jeżeli istnieje takie licencjownowanie.</p> <p>Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów Win 2018 i nowszych, Linux, Vmware, Unix</p> <p>Macierz musi posiadać funkcjonalność priorytetyzacji zadań w tym ustawienie max parametrów (I/Ops i Mbps) dla poszczególnych LUN.</p> <p>Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów</p>

		<p>logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.</p> <p>Macierz musi posiadać funkcjonalność replikacji danych z inna macierzą tego samego producenta w trybie synchronicznym i asynchronicznym. Funkcjonalność replikacji danych musi być natywnym narzędziem macierzy. Przed procesem replikacji macierz musi umożliwiać włączenie procesu deduplikacji danych i kompresji danych w celu optymalizacji wykorzystania łącza dla replikowanych zasobów lub zamawiający wymaga dostarczenia zewnętrznego narzędzia do deduplikowania replikowanych danych lub dwukrotnego zwiększenia pojemności ze względu na rozważaną w przyszłości replikację całości zasobów.</p> <p>Macierz musi posiadać licencję na tworzenie zasobów typu WORM, Zamawiający wymaga dostarczenia tej licencji.</p> <p>System posiadać specjalny moduł do zabezpieczenia przez atakiem Ransomware w szczególności:</p> <ul style="list-style-type: none"> - musi informować administratora w przypadku nie standardowego zachowania systemu oraz danych - wykonywać automatyczną prewencyjną kopię migawkową „snapshot” w przypadku zagrożenia atakiem ransomware i wystąpienia ataku zarówno dla zasobów blokowych jak i plikowych. <p>Macierz musi posiadać funkcjonalność klonowania danych bez potrzeby fizycznego kopiowania danych na nośnikach.</p> <p>Macierz musi posiadać funkcjonalność wykonania spójnego snapshotu dla następujących aplikacji:</p> <ul style="list-style-type: none"> - VMware - SAP - MS SQL - MS Exchange - MS HyperV <p>W celach bezpieczeństwa macierz musi posiadać funkcjonalność wieloetapowej akceptacji wybranych operacji tj. operacje takie jak: Skasowanie LUN/Wolumeny, skasowanie Snapshotu, wyłączenie replikacji. System musi pozwalać by wykonanie w/w operacji było akceptowane przez przynajmniej dwóch administratorów w celu zwiększenia bezpieczeństwa i uniknięcia błędów ludzkich.</p> <p>Macierz musi posiadać funkcjonalność klastra geograficznego</p>
--	--	---

		<p>pozwalającego na automatyczne przełączanie zasobów pomiędzy macierzami dla zasobów SAN w szczególności wspierający minimum następujące systemy:</p> <ul style="list-style-type: none"> • VMware • VMFS • Windows • Windows Server Failover Cluster (WSFC) • Hyper-V • Oracle, Oracle RAC, MS SQL, SAP HANA • Linux <p>Automatyczne przełączanie zasobów z jednej macierzy dwukontrolerowej na inną macierz dwukontrolerową musi się odbywać w trybie:</p> <ul style="list-style-type: none"> - bez ingerencji inżyniera - z ingerencją inżyniera <p>Macierz musi posiadać pakiet oprogramowania do backupu zasobów plikowych pomiędzy macierzami tego samego producenta.</p> <p>Oferowana konfiguracja macierzy musi pozwalać na osiągnięcie wydajności do 380 000IOPS przy 8Kb bloku i stosunku 70/30% odczyt/zapis. Zamawiający wraz z ofertą wymaga dostarczenia oficjalnego dokumentu producenta z wymiarowaniem wydajności oraz dopuszcza możliwość sprawdzenia wydajności macierzy przy odbiorze.</p> <p>Macierz musi posiadać narzędzie umożliwiające generowanie raportu o konfiguracji, utworzonych dyskach logicznych i woluminach oraz ich zajętości wraz z podziałem na rzeczywiste dane, kopie migawkowe oraz dane wewnętrzne macierzy.</p> <p>Macierz musi być wyposażona oprogramowanie do audytu zasobów plikowych w szczególności pozwalać na:</p> <ul style="list-style-type: none"> - blokowanie zapisywania plików z określonym (do zdefiniowania przez administratora) rozszerzeniem - monitorowaniu operacji wykonywanych na plikach <p>Macierz musi posiadać funkcjonalność „Tieringu” zimnych danych na:</p> <ul style="list-style-type: none"> ○ inną macierz tego samego producenta (z wolnymi dyskami np. NL-SAS) ○ inną macierz dowolnego producenta z protokołem S3 ○ Tiering musi być natywnym narzędziem macierzy i wykonywać się automatycznie. ○ Tiering do chmury na zasób S3 ○ Replikację asynchroniczną na dowolny zasób S3 dowolnego producenta <p>Wszystkie funkcjonalności muszą być dostarczone na maksymalną</p>
--	--	--

		<p>pojemność macierzy. Z macierzą zamawiający wymaga dostarczenia oprogramowania które pozwala na:</p> <ul style="list-style-type: none"> - monitoring wykorzystania przestrzeni na macierzy - monitoring grup RAIDowych - monitoring wykonywanych backupów/replikacji danych między macierzami - monitoring wydajności macierzy - analizę i diagnozę spadku wydajności <p>Zamawiający dopuszcza zastosowanie oprogramowania zewnętrznego, na pełną max pojemność systemu. Wszystkie funkcjonalności muszą być dostarczone na maksymalną pojemność urządzenia i pozwalać na wspólne działanie (żadna funkcjonalność nie może wykluczać działania innej funkcjonalności).</p>
9.	Gwarancja i serwis	<p>3 lata serwisu z 2 godzinnym czasem odpowiedzi i wymianą części na następny dzień roboczy po diagnozie problemu. Dostarczony serwis musi umożliwiać zgłaszanie awarii w trybie 24x7.</p> <p>Dostarczony system musi posiadać również 3 lata subskrypcji dla dostarczonego wraz z macierzą oprogramowania, dostęp do portalu serwisowego producenta, dostęp do wiedzy i informacji technicznych dotyczących oferowanego urządzenia.</p> <p>Zepsute nośniki pozostają u zamawiającego</p>
10.	Inne	<p>System musi posiadać moduł do audytu zasobów plikowych na wyspecyfikowanej macierzy po kątem przechowywanych danych wrażliwych/osobowych. W szczególności moduł mu posiadać:</p> <ul style="list-style-type: none"> • Możliwość przeszukiwania zasobów plikowych <ul style="list-style-type: none"> ○ na wyspecyfikowanej macierzy/serwerze plików ○ innych serwerach plików jak Google drive, Onedrive, Azurefiles, ○ baz danych: Oracle, MySQL, MS SQL, PostgreSQL, Mongo DB, SAP HANA - system musi pozwalać na utworzenie kategorii przeszukanych plików na: <ul style="list-style-type: none"> ○ nie wrażliwe (ogólne informacje o pracowniku) ○ dane osobiste (numer NIP, Pesel) ○ dane wrażliwe (dane zdrowotne, informacje o wynagrodzeniu) - System musi być zgodny z europejskimi przepisami GDPR (Rodo) w tym móc przeszukiwać i kategoryzować dane po: <ul style="list-style-type: none"> ○ NIP/Regon ○ Pesel ○ Adresie Email ○ Kontach bankowych <p>Zamawiający wymaga, aby zaoferowane urządzenia były uznanymi rozwiązaniami na świecie – producent zaoferowanego rozwiązania musi być notowany w raportach Gartnera dla rozwiązań "Primary</p>

		Storage" nie starszych niż 2 lata przed złożeniem oferty i być wymieniony w grupie liderów (ang. Leaders). Jako równoważny dla raportu Gartnera Zamawiający dopuści również inny raport udostępniany publicznie, powszechnie akceptowany, mający charakter zewnętrznego i obiektywnego raportu standaryzacyjnego, który zapewnia analizę, wgląd w kierunek oraz dojrzałość uczestników rynku w rozwiązaniach
--	--	--

4. Serwery klastra wysokiej dostępności (2 szt.)

Obudowa

- Typu RACK, wysokość nie więcej niż 1U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable;
- Obudowa musi umożliwiać zainstalowania 10 dysków twardych hot plug 2,5" SATA/SAS;
- Możliwość rozbudowy o panel diagnostyczny z wyświetlaczem LCD umożliwiającym detekcję usterek umożliwiający wyświetlenie następujących informacji:
 - aktywne ostrzeżenia;
 - status serwera;
 - typ oraz model serwera, numer seryjny;
 - wersje oprogramowania UEFI oraz modułu zarządzania;
 - informacje nt modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS;
 - dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii;
 - aktywne sesje połączeniowe do interfejsu zarządzania;
- Zainstalowane 2 szt. dysków Hot-Swap SSD NVMe 480GB, dyski skonfigurowane w RAID-1 podłączone do sprzętowego kontrolera RAID;

Płyta główna

- Dwuprocessorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 86-rdzeniowych;
- Moduł TPM 2.0;
- 2 złącza PCI Express Gen5 x16 w tym minimum 1 złącze FH;
- Opcjonalnie możliwość 3 złącz PCIe;
- 32 gniazda pamięci RAM;
- Obsługa pamięci CXL 2.0
- Obsługa 8 TB pamięci operacyjnej RAM DDR5;
- Wsparcie dla technologii:
 - BoundedFault;
 - SDDC;
 - ECC;
 - Memory Mirroring;
 - ADDDC;
- Wewnętrzny slot na kartę Micro SD

Procesory

- Dwa procesory 16-rdzeniowe, taktowanie bazowe 2,3 GHz, architektura x86_64;

• osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017_int_base 372 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org> dla oferowanego serwera.

Pamięć RAM

- 256GB pamięci RAM;
- DDR5 Registered 6400MT/s;

Kontrolery LAN

- Interfejsy LAN, nie zajmujące slotów PCI Express (OCP):
- Dwie dwuportowe karty 25Gbit SFP28, wszystkie porty obsadzone dualnymi wkładkami 10/25G MMF LC;
- 1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB;;

Porty

- Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera, możliwość zainstalowania portu cyfrowego (DP lub HDMI)
- 2 porty USB 5Gb/s dostępne z tyłu serwera;
- Opcjonalny port USB 5Gbp/s wewnętrzny;
- Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera;
- Opcjonalny port serial;
- Ilość dostępnych złączy USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1300W;
- Redundantne wentylatory hotplug dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni celsjusza;

Bezpieczeństwo

- Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji;
- Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej;
- Zainstalowany czujnik otwarcia obudowy zintegrowany z modułem zarządzania serwerem;
- Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem;
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania;
- Możliwość ustawienia hasła włączania serwera;
- Możliwość ustawienia hasła administratora;
- Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID;

Zarządzanie

- Wymaga się aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
- Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ówPCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych;

- Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.
- Funkcjonalność kontrolera zdalnego zarządzania:
- Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna)
- Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja
- Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
- Logowanie zdarzeń związanych z utrzymaniem systemu jak upgrade firmware, zmiana/installacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.
- Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3
- Update systemowego firmware
- Monitoring i możliwość ograniczenia poboru prądu
- Zdalne włączanie/wyłączanie/restart
- Zapis video zdalnych sesji
- Podmontowanie lokalnych mediów z wykorzystaniem Java client
- Przekierowanie konsoli szeregowej przez IPMI
- Zrzut ekranu w momencie zawieszenia systemu
- Możliwość przejęcia zdalnego ekranu
- Możliwość zdalnej instalacji systemu operacyjnego
- Alerty Syslog
- Przekierowanie konsoli szeregowej przez SSH
- Wsparcie dla dynamic DNS
- Wyświetlanie danych aktualnych i historycznych dla zużycia energii oraz temperatury serwera
- Wirtualna konsola z dostępem do myszy, klawiatury;
- Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy ActiveX (musi działać w oparciu o HTML5)
- Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
- Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
- wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API
- Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą zarządzającą) bez możliwości uzyskania jakiejkolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
- Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.
- Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.
- Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.
- Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
- Możliwość, w okresie obowiązywania wsparcia, wykupienia opcjonalnej licencji/subskrypcji na oprogramowanie producenta serwera do zarządzania, spełniające poniższe wymagania:

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- Integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym
- Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP
- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu danych min do formatu CSV
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK
- Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych
- Możliwość przejęcia zdalnego pulpitu
- Możliwość zamontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta
- Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)
- Automatyczna polityka aktualizacji „Najnowsze dostępne”
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI
- Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:
- wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów
- wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji

- z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
- inwentaryzacja komponentów w serwerze i ich mikrokodów
- historia min 24h poboru mocy i temperatury serwera
- zbieranie danych diagnostycznych serwera do paczki
- Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin:
- wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze do zdefiniowanej polityki poziomu mikrokodów
- z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
- aktualizacja sterowników systemowych Windows
- inwentaryzacja komponentów w serwerze i ich mikrokodów
- historia min 24h poboru mocy i temperatury serwera
- zbieranie danych diagnostycznych serwera do paczki
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Certyfikowane systemy operacyjne

- Microsoft Windows Server 2025, 2022;
- VMWare ESXi 8.0, 9.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9.x, 10.x;
- Ubuntu 22.04 LTS, 24.04 LTS,
- Oracle Linux 9.x;
- Xen Server 8,8.2

Gwarancja

- 3 lata gwarancji producenta serwera w trybie on-site z czasem reakcji następnego dnia roboczego. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
- Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera w 24h od zgłoszenia usterki

Dodatkowo, zamawiający wymaga dostarczenia licencji Serwerowego Systemu Operacyjnego (SSO) do każdego serwera, o poniższych funkcjonalnościach:

L.p.	Element, parametr lub warunek	Opis minimalnych wymagań
1.	Cechy licencji	<p>Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i nieograniczonej liczby wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</p> <p>Wraz z licencjami SSO należy dostarczyć 170 licencji dostępowych dla użytkowników, jeżeli model licencjonowania oferowanego SSO wymaga takich licencji. Oprogramowanie musi być dostarczone w najnowszej wersji.</p>

2.	Cechy SSO	<p>Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy.</p> <ol style="list-style-type: none"> 1. Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych z możliwością kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: <ol style="list-style-type: none"> a. pozwalają na zmianę rozmiaru w czasie pracy systemu, b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d. umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST
----	-----------	---

	lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
	12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
	13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
	14. Wbudowana zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
	15. Graficzny interfejs użytkownika.
	16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
	17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu.
	18. Wsparcie dla urządzeń peryferyjnych tj. drukarek, urządzeń sieciowych itp.
	19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
	20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
	21. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach.
	22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
	i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
	iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,

		iv. Ustanawianie praw dostępu do określonych zasobów dla użytkowników nie dołączonych do domeny.
		c. Zdalna dystrybucja oprogramowania na stacje robocze.
		d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
		e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
		- Dystrybucję certyfikatów poprzez http,
		- Konsolidację CA dla wielu lasów domeny,
		- Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
		f. Szyfrowanie plików i folderów.
		g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
		h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
		i. Serwis udostępniania stron WWW.
		j. Wsparcie dla protokołu IP w wersji 6 (IPv6).
		k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.
		l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
		- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		- Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
		- Obsługi 4-KB sektorów dysków,
		- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
		- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego

		funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
		- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunkmode).
		23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
		24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
		25. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
		26. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
		27. Sterowniki i dokumentacja od producenta sprzętu.
		28. Materiały edukacyjne w języku polskim.
3	Dokumentacja, inne	Wykonawca dostarcza oprogramowanie wraz z licencjami oraz nośnikami instalacyjnymi.

5. Niezależny system backupu - serwer wraz z biblioteką taśmową, oprogramowaniem backupowym oraz urządzeniem typu NAS

Zadaniem niezależnego systemu backupu jest stworzenie odseparowanego środowiska wyposażonego w serwer backupu, bibliotekę taśmową, serwer plików oraz system do wykonywania kopii zapasowych o poniższych parametrach:

Serwer:

Obudowa

- Typu RACK, wysokość nie więcej niż 1U;
- Szyny umożliwiające wysunięcie serwera z szafy stelażowej wraz z ramieniem porządkującym kable;
- Obudowa musi umożliwiać zainstalowania 10 dysków twardych hot plug 2,5" SATA/SAS;

- Możliwość rozbudowy o panel diagnostyczny z wyświetlaczem LCD umożliwiającym detekcję usterek umożliwiający wyświetlenie następujących informacji:
- aktywne ostrzeżenia;
- status serwera;
- typ oraz model serwera, numer seryjny;
- wersje oprogramowania UEFI oraz modułu zarządzania;
- informacje nt modułu zarządzania: nazwa hosta, adres MAC, adres IP, adres DNS;
- dane środowiskowe: temperaturę procesora, poziom napięcia wejściowego, poziom zużycia energii;
- aktywne sesje połączeniowe do interfejsu zarządzania;
- Zainstalowane 2 szt. dysków Hot-Swap SSD NVMe 960GB, dyski skonfigurowane w RAID-1 podłączone do sprzętowego kontrolera RAID;

Płyta główna

- Dwuprocessorowa;
- Wyprodukowana i zaprojektowana przez producenta serwera;
- Możliwość instalacji procesorów 86-rdzeniowych;
- Moduł TPM 2.0;
- 2 złącza PCI Express Gen5 x16 w tym minimum 1 złącze FH;
- Opcjonalnie możliwość 3 złącz PCIe;
- 32 gniazda pamięci RAM;
- Obsługa pamięci CXL 2.0
- Obsługa 8 TB pamięci operacyjnej RAM DDR5;
- Wsparcie dla technologii:
- BoundedFault;
- SDDC;
- ECC;
- Memory Mirroring;
- ADDDC;
- Wewnętrzny slot na kartę Micro SD

Procesory

- Jeden procesor 12-rdzeniowy, taktowanie bazowe 2,2 GHz, architektura x86_64;

- osiągający w teście SPEC CPU2017 Floating Point wynik SPECrate2017_int_base 286 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany na stronie <http://spec.org> dla oferowanego serwera.

Pamięć RAM

- 64GB pamięci RAM;
- DDR5 Registered 6400MT/s;

Kontrolery LAN

- Interfejsy LAN, nie zajmujące slotów PCI Express (OCP):
- Dwuportowa karta 25Gbit SFP28, wszystkie porty obsadzone dualnymi wkładkami 10/25G MMF LC;
- 1x 1G Base-T dedykowany do zarządzania serwerem w trybie OOB;;

Porty

- Zintegrowana karta graficzna posiadająca 16MB pamięci rozdzielczość 1920x1200 przy 60 Hz, ze złączem VGA z tyłu serwera, możliwość zainstalowania portu cyfrowego (DP lub HDMI)
- 2 porty USB 5Gb/s dostępne z tyłu serwera;
- Opcjonalny port USB 5Gbp/s wewnętrzny;
- Dedykowany port do zarządzania i diagnostyki dostępny z przodu serwera;
- Opcjonalny port serial;
- Ilość dostępnych złączy USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express i/lub USB serwera.
- Karta SAS HBA 4-portowa dedykowana do podłączenia biblioteki taśmowej;

Zasilanie, chłodzenie

- Redundantne zasilacze hotplug o sprawności 96% (tzw. klasa Titanium) o mocy 1300W;
- Redundantne wentylatory hotplug dające gwarancję poprawnego działania serwera w temperaturze otoczenia nie przekraczającej 30 stopni celsjusza;

Bezpieczeństwo

- Możliwość automatycznego przywrócenia BIOS do wspieranej wersji w przypadku wykrycia nieautoryzowanej modyfikacji;
- Wbudowany w BIOS mechanizm umożliwiający usunięcie konfiguracji kart zarządzających, BIOS oraz danych ze wszystkich wewnętrznych urządzeń pamięci masowej;
- Zainstalowany czujnik otwarcia obudowy zintegrowany z modulem zarządzania serwerem;
- Fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;

- Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z systemu zarządzania serwerem;
- Możliwość wyłączenia w BIOS funkcji przycisku zasilania;
- Możliwość ustawienia hasła włączania serwera;
- Możliwość ustawienia hasła administratora;
- Możliwość przewidywania awarii dla procesorów, regulatorów napięcia, pamięci, dysków wewnętrznych, wentylatorów, zasilaczy, kontrolerów RAID;

Zarządzanie

- Wymaga się aby serwer posiadał diody sygnalizujące awarię przy każdej kości pamięci RAM, każdej zatoce dyskowej, każdym zasilaczu.
- Możliwość instalacji serwera oraz serwisowania (instalacji oraz deinstalacji) komponentów takich jak: riser'ówPCIe, backplane'ów dysków twardych, kart rozszerzeń, wentylatorów, bez użycia dodatkowych narzędzi mechanicznych;
- Możliwość użycia aplikacji mobilnej na telefonie (iOS lub Android), do przeglądania awarii, konfigurowania ustawień i włączenia/wyłączenia serwera. Podłączenie telefonu odbywa się poprzez dedykowany port USB na froncie serwera.
- Funkcjonalność kontrolera zdalnego zarządzania:
- Monitoring stanu systemu (komponenty objęte monitoringiem to przynajmniej: CPU, pamięć RAM, dyski, karty PCI, zasilacze, wentylatory, płyta główna
- Uzyskanie następujących informacji o serwerze: nazwa, typ i model, numer seryjny, nazwa systemu, wersja UEFI oraz BMC, adres ip karty zarządzającej, użycie cpu, użycie pamięci oraz komponentów I/O, lokalizacja
- Logowanie zdarzeń systemowych oraz związanych z działaniami użytkownika. Każdy dziennik zdarzeń powinien mieć możliwość zapisu co najmniej 1024 rekordów.
- Logowanie zdarzeń związanych z utrzymaniem systemu jak upgradefirmware, zmiana/instalacja sprzętu. System powinien umożliwiać zapisanie minimum 250 zdarzeń.
- Wysyłanie określonych zdarzeń poprzez SMTP oraz SNMPv3
- Update systemowego firmware
- Monitoring i możliwość ograniczenia poboru prądu
- Zdalne włączanie/wyłączanie/restart
- Zapis video zdalnych sesji
- Podmontowanie lokalnych mediów z wykorzystaniem Java client
- Przekierowanie konsoli szeregowej przez IPMI
- Zrzut ekranu w momencie zawieszenia systemu
- Możliwość przejęcia zdalnego ekranu

- Możliwość zdalnej instalacji systemu operacyjnego
- Alerty Syslog
- Przekierowanie konsoli szeregowej przez SSH
- Wsparcie dla dynamic DNS
- Wyświetlanie danych aktualnych i historycznych dla zużycia energii oraz temperatury serwera
- Wirtualna konsola z dostępem do myszy, klawiatury;
- Montowanie obrazów ISO bez instalacji dodatkowych komponentów Java czy ActiveX (musi działać w oparciu o HTML5)
- Możliwość mapowania obrazów ISO przez HTTPS, SFTP, CIFS oraz NFS
- Możliwość jednoczesnej pracy do 6 użytkowników przez wirtualną konsolę
- wspierane protokoły/interfejsy: IPMI v2.0, SNMP v3, CIM, DCMI v1.5, REST API
- Możliwość wykorzystania frontowego portu USB do celów serwisowych (komunikacja portu z kartą zarządzającą) bez możliwości uzyskania jakiegokolwiek funkcjonalności na poziomie zainstalowanego systemu operacyjnego. Funkcjonalność ta musi być realizowana na poziomie sprzętowym i musi być niezależna od zainstalowanego systemu operacyjnego.
- Kontroler zarządzania musi posiadać 4GB wewnętrznej pamięci (dopuszcza się zastosowanie karty Micro SD w celu uzyskania tej pojemności). Pamięć kontrolera zarządzania musi pełnić funkcję RDOC (Remote Disc on Card) oraz musi umożliwiać przechowywanie plików firmware.
- Monitorowanie zmian sprzętowych w celu wykrycia nieoczekiwanych zmian. Po wykryciu zmiany zapis w logu serwera lub uniemożliwienie boot'u.
- Możliwość synchronizacji konfiguracji i poziomów firmware pomiędzy serwerami.
- Możliwość monitorowania i zarządzania grupą serwerów z poziomu kontrolera zarządzania pojedynczego serwera. Ilość serwerów możliwych do zarządzania – minimum 200.
- Możliwość, w okresie obowiązywania wsparcia, wykupienia opcjonalnej licencji/subskrypcji na oprogramowanie producenta serwera do zarządzania, spełniające poniższe wymagania:
- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- Integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta w systemie operacyjnym
- Automatyczne rozpoznawanie nowych serwerów poprzez protokół SLP oraz SSDP
- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu danych min do formatu CSV
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Możliwość wizualizacji rozmieszczenia serwerów i zarządzanych urządzeń w szafach RACK

- Tworzenie automatycznie grup urządzeń w oparciu o elementy konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji czy stanu np. firmware czy BIOS
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej, pozwalając min weryfikację statusu i wysyłanie paczek diagnostycznych
- Możliwość przejęcia zdalnego pulpitu
- Możliwość zamontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o repozytorium aktualizacji – budowanie repozytorium w sposób automatyczny ze stron producenta
- Możliwość definiowania polityk aktualizacji (konkretne wersje firmware)
- Automatyczna polityka aktualizacji „Najnowsze dostępne”
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta na systemie operacyjnym
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności czy powielania konfiguracji na inne serwery czy backup aktualnej konfiguracji.
- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Wykonanie restartu serwera i automatyczne wejście do BIOSu/UEFI
- Zdalne bezpieczne usunięcie danych na dyskach SSD/HDD w serwerach
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Integracja z środowiskiem VMware vCenter pozwalająca z konsoli/plugin:

- wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze Vmware do zdefiniowanej polityki poziomu mikrokodów
- wykonać/zweryfikować konfigurację serwera zgodną ze zdefiniowaną polityką konfiguracji
- z konsoli vCenter uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
- inwentaryzacja komponentów w serwerze i ich mikrokodów
- historia min 24h poboru mocy i temperatury serwera
- zbieranie danych diagnostycznych serwera do paczki
- Integracja z środowiskiem Microsoft Admin Center pozwalająca z konsoli/plugin:
- wykonać zautomatyzowaną aktualizację firmware serwerów w klastrze do zdefiniowanej polityki poziomu mikrokodów
- z konsoli Admin Center uruchomić zdalną konsolę graficzną serwera (nawet gdy nie jest uruchomiony na serwerze system operacyjny)
- aktualizacja sterowników systemowych Windows
- inwentaryzacja komponentów w serwerze i ich mikrokodów
- historia min 24h poboru mocy i temperatury serwera
- zbieranie danych diagnostycznych serwera do paczki
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

Certyfikowane systemy operacyjne

- Microsoft Windows Server 2025, 2022;
- VMWare ESXi 8.0, 9.0;
- Suse Linux Enterprise Server 15;
- Red Hat Enterprise Linux 9.x, 10.x;
- Ubuntu 22.04 LTS, 24.04 LTS,
- Oracle Linux 9.x;
- Xen Server 8,8.2

Gwarancja

- 3 lata gwarancji producenta serwera w trybie on-site z czasem reakcji następnego dnia roboczego. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
- Funkcja automatycznego zgłaszania usterek i awarii sprzętowych w helpdesk/servicedesk producenta sprzętu;
- Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;

- Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera w 24h od zgłoszenia usterki (podać koszt na dzień składania oferty).

Dodatkowo, zamawiający wymaga dostarczenia licencji Serwerowego Systemu Operacyjnego (SSO), o poniższych funkcjonalnościach:

L.p.	Element, parametr lub warunek	Opis minimalnych wymagań
1.	Cechy licencji	<p>Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i 2 wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.</p> <p>Oprogramowanie musi być dostarczone w najnowszej wersji.</p>
2.	Cechy SSO	<p>Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy.</p> <ol style="list-style-type: none"> 1. Możliwość wykorzystania, do 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym. 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności do 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych z możliwością kompresji danych, bez zatrzymywania ich pracy, między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.

		9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
		a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
		b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
		c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
		d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
		10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
		11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
		12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET.
		13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
		14. Wbudowana zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
		15. Graficzny interfejs użytkownika.
		16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
		17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu.
		18. Wsparcie dla urządzeń peryferyjnych tj. drukarek, urządzeń sieciowych itp.
		19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
		20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
		21. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach.
		22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:

		a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
		b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
		i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
		ii. Ustawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
		iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza,
		iv. Ustawianie praw dostępu do określonych zasobów dla użytkowników nie dołączonych do domeny.
		c. Zdalna dystrybucja oprogramowania na stacje robocze.
		d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej.
		e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego umożliwiające:
		- Dystrybucję certyfikatów poprzez http,
		- Konsolidację CA dla wielu lasów domeny,
		- Automatyczne rejestrowanie certyfikatów pomiędzy różnymi lasami domen.
		f. Szyfrowanie plików i folderów.
		g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
		h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
		i. Serwis udostępniania stron WWW.
		j. Wsparcie dla protokołu IP w wersji 6 (IPv6).
		k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows.

		1. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:
		- Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
		- Obsługi ramek typu jumbo frames dla maszyn wirtualnych,
		- Obsługi 4-KB sektorów dysków,
		- Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,
		- Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API,
		- Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk mode).
		23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
		24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
		25. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
3	Dokumentacja, inne	26. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
		27. Sterowniki i dokumentacja od producenta sprzętu.
		28. Materiały edukacyjne w języku polskim.
		Wykonawca dostarcza oprogramowanie wraz z licencjami oraz nośnikami instalacyjnymi.

Biblioteka taśmowa wraz z kompletem taśmek:

- Obudowa przystosowana do montażu w standardowej szafie rack 19". Maksymalna wysokość oferowanego rozwiązania - 1U.
- Biblioteka taśmowa musi być wyposażona w min. 1 napęd taśmowy LTO9 z interfejsem SAS.
- Biblioteka musi być wyposażona w nie mniej niż 9 slotów na taśmy.
- Biblioteka musi być wyposażona w czytnik kodów kreskowych.
- Biblioteka musi być wyposażona w komplet magazynków na taśmy, tak by możliwa była pełna obsada biblioteki taśmami LTO.
- Możliwość zdalnego zarządzania biblioteki poprzez interfejs WWW.
- Możliwość monitorowania stanu biblioteki i napędów.
- Biblioteka musi posiadać panel sterowania oraz wyświetlacz informujący o błędach urządzenia, aktywności napędów.
- Biblioteka powinna umożliwiać partycjonowanie.
- Biblioteka musi posiadać zasilacz o mocy nie większej niż 90W.
- Razem z biblioteką należy dostarczyć min. 15 taśm LTO-9 RW oznaczonych kodami kreskowymi , 1 taśmę czyszczącą oraz przewód łączący urządzenie z serwerem backupu.
- Gwarancja minimum 36 miesięcy on-site NBD.

Do biblioteki należy dostarczyć:

- Niezbędne kable zasilające.
- Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu (najnowsza wersja firmware na dzień dostawy).
- Wszystkie oferowane urządzenia muszą być fabrycznie nowe.
- Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- Urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V \pm 10%, 50 Hz.
- Oferowane produkty (urządzenia, sprzęty) muszą spełniać wymagania norm CE, lub równoważne.

Serwer plików:

Procesor	Czterordzeniowy procesor AnnapurnaLabsAlpine AL324 64-bitowy ARM® Cortex-A57 1,7 GHz
Obudowa	Rack 1U
Pamięć RAM	16 GB UDIMM DDR4
Ilość obsługiwanych dysków	4 dyski 3,5-calowych SATA 6 Gb/s, 3 Gb/s o maksymalnej pojemności 18TB każdy

Ilość zainstalowanych dysków	4 dyski o pojemności 10TB, 7200 RPM i 256MB cache klasy Enterprise DataCenter
Interfejsy sieciowe	2 porty 2,5 Gigabit sieci Ethernet (2,5G/1G/100M) 2 porty 10GbE SFP+ <ul style="list-style-type: none"> obsługa VLAN i Jumbo Frame.
Porty	4x USB 3.2 Gen 1 1x port PCIe Gen2
Wskaźniki LED	HDD 1–4, stan, LAN, Rozszerzanie pamięci masowej
Obsługa RAID	Pojedynczy dysk, JBOD, RAID 0,1,5,5+Spare ,6 ,10,. Obsługa BITMAP w celu przyspieszenia odbudowy. Możliwość skonfigurowania Global Spare Disk.
Funkcje RAID	Możliwość zwiększania pojemności i migracja między poziomami RAID online.
Szyfrowanie	Możliwość szyfrowania całych woluminów kluczem AES 256 bitów.
Protokoły	CIFS, AFP, NFS, FTP, WebDAV, iSCSI, Telnet, SSH, SNMP
Usługi	Stacja monitoringu Windows ACL Integracja w Windows ADS Serwer WWW Serwer plików Manager plików przez WWW Funkcja Virtual Disk umożliwiająca zwiększenie pojemności serwera przy pomocy protokołu iSCSI Replikacja w czasie rzeczywistym Serwer RADIUS Klient LDAP Serwer Syslog Container Station
Zarządzanie dyskami	SMART, sprawdzanie złych sektorów,
Język GUI	Polski
Gwarancja i serwis	36 miesięcy na NAS i 60 miesięcy na dyski
System plików	Dyski wewnętrzne EXT4. Dyski zewnętrzne EXT3, EXT4, NTFS, FAT32, HFS+
iSCSI	Obsługa MPIO, MC/S i SPC-3 Persistent Reservation
Liczba kont użytkowników	4096
Liczba grup	512
Liczba udziałów	512
Max ilość połączeń (CIFS)	700

Max liczba migawek	256
Zasilanie	Redundantne o mocy max 250 W, 100–240 V
Wentylatory	2 x 40mm, 12VDC
UPS	Obsługa sieciowych awaryjnych zasilaczy UPS.

Oprogramowanie do wykonywania kopii zapasowych:

Nazwa
Wymagania minimalne
Rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych, przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
Microsoft Server z rolą Hyper-V min. w wersjach 2022, 2019, 2016, 2012R2, 2012
Vmware vSphere min. w wersjach v5.5 - v8.0U3
Nutanix AHV v6.5.4 (LTS)
Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
Microsoft 365 (Exchange online, One Drive for Business, Sharepoint, Teams)
Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
Oprogramowanie musi być niezależne sprzętowo i posiadać możliwość uruchomienia:
na serwerze Windows lub Linux
jako maszyna wirtualna VMware
jako maszyna wirtualna Amazon
na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS
Oprogramowanie nie może wymagać instalacji dedykowanego agenta wewnątrz maszyny wirtualnej w celach backupu/przywracania
Oprogramowanie nie może wymagać dodatkowej instalacji zewnętrznych aplikacji lub baz danych (jeżeli oprogramowanie wymaga bazy danych musi ona być instalowana automatycznie z paczki opracowanej przez producenta i nie wymagać dodatkowych licencji).
Licencjonowanie
Wszystkie funkcje i komponenty oprogramowania dla środowisk VMware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji. Licencjonowanie powinno być realizowane w wariantcie wieczystym, w którym licencja nie ma terminu ważności
Dopuszczalne jest dostarczenie oprogramowania w wersji umożliwiającej ograniczoną rozbudowę środowiska, wersja ta powinna jednak umożliwiać rozbudowę do nie mniej niż 6 gniazd procesorów w obrębie środowiska
W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 3 lat wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie

oferowanego oprogramowania
W ramach dostawy wymagane jest dostarczenie licencji na ochronę 4 gniazd procesorów w hostach Vmware lub Hyper-V
Licencjonowanie innych środowisk może być realizowane na zasadzie wymagającej zakupu dedykowanej licencji dla środowiska
Ochrona danych
Oprogramowanie musi posiadać funkcje backupu i replikacji:
Backup maszyn wirtualnych Vmware
Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
Backup maszyn wirtualnych Hyper-V
Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych). Replikacja nie może wymagać utworzenia backupu
Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów. Kopia tworzona jest zgodnie z określonym harmonogramem
Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
Optymalizacja wykorzystania miejsca na dane
Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
Kompresja backupu, w tym konfigurowalny stopień kompresji
Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
Spójność danych
Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:
Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji:

Microsoft Exchange 2013, 2016, 2019
Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022
Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
Przywracanie danych
Oprogramowanie musi posiadać poniższe funkcje:
Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji
Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej)
Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu):
Microsoft Exchange
MS Active Directory
MS SQL
Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
Wydajność
Oprogramowanie do backupu musi pozwalać na:
Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
Zarządzanie
Oprogramowanie musi pozwalać na następujące formy zarządzania:
Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych
Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.

Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji

Oprogramowanie musi umożliwiać integrację z Active Directory

Oprogramowanie musi wspierać tzw. tryb multitenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach

6. Segmentacja sieci i zwiększenie przepustowości – dostosowanie sieci LAN do wymagań środowiska wirtualnego, podział na strefy bezpieczeństwa, podniesienie przepustowości łącza, rewitalizacja punktów dystrybucyjnych

Zakres prac obejmuje wykonanie i realizację kompleksowego projektu sieciowego, którego celem jest podniesienie poziomu bezpieczeństwa i uporządkowanie komunikacji wewnętrznej poprzez wdrożenie segmentacji logicznej sieci, przy jednoczesnym zachowaniu ciągłości pracy infrastruktury teleinformatycznej.:

1. Wykonanie audytu obecnej infrastruktury sieciowej LAN, w tym identyfikacja wszystkich aktywnych urządzeń, punktów dystrybucyjnych, urządzeń końcowych.
2. Zebranie danych konfiguracyjnych z przełączników i urządzeń brzegowych, w tym zrzuty konfiguracji, schematy VLANów, zidentyfikowane porty trunk/uplink, adresacja IP.
3. Opracowanie mapy logiczno-fizycznej sieci LAN, uwzględniającej aktualną topologię oraz planowane zmiany w związku z wdrożeniem segmentacji.
4. Zaprojektowanie szczegółowego planu segmentacji sieci z wykorzystaniem technologii VLAN, obejmującego:
 - rozdzielenie ruchu pomiędzy różnymi strefami funkcjonalnymi
 - przypisanie VLAN ID, zakresów adresów IP, adresów bram domyślnych oraz polityk dostępowych
5. Przygotowanie Analizy Przedwdrożeniowej (AP) i Projektu Technicznego (PT) zawierającego:
 - mapę VLANów i przypisanie do urządzeń i portów,
 - strukturę routingu między VLANami,
 - listę niezbędnych zmian fizycznych i logicznych,
 - wytyczne do konfiguracji firewalli oraz przełączników
6. Przekazanie AP oraz PT do zatwierdzenia przez Zamawiającego. W przypadku konieczności Zamawiający zgłasza konieczności wyjaśnienia oraz uzupełnienia dokumentacji. Wykonawca w przeciągu trzech dni dostarczy poprawioną dokumentację bądź udzieli wyjaśnień. Warunkiem przystąpienia do dalszych prac jest akceptacja AP i PT przez Zamawiającego.
7. Rekonfiguracja przełączników warstwy 2:

- przypisanie portów do odpowiednich VLANów (access i trunk),
 - konfiguracja Spanning Tree, loop protection, SNMP, DHCP snooping,
 - wykonanie aktualizacja firmware,
 - integracja z systemem NAC w celu dynamicznej zmiany vlanów oraz utworzenie polityk ACL,
 - dokładny opis portów na przełącznikach.
8. Konfiguracja przełączników warstwy 3:
- utworzenie interfejsów vlan i nadanie adresów IP,
 - konfiguracja routingu pomiędzy podsieciami,
 - konfiguracja statycznych wpisów w tablicy routingu,
 - utworzenie polityk ACL,
 - konfiguracja IPHELPER.
9. Konfiguracja dynamicznego routingu pomiędzy przełącznikiem CORE pracującym w warstwie L3, a urządzeniem UTM.
10. Utworzenie puli dynamicznej dla każdej adresacji na serwerze DHCP.
11. Indywidualne podejście do urządzeń końcowych podczas zmian adresów IP.
12. Test komunikacji między VLANami zgodnie z założonymi regułami – zapewnienie separacji tam, gdzie wymagane, oraz dostępności usług zgodnie z wymaganiami Zamawiającego.
13. Weryfikacja polityk bezpieczeństwa na firewallu – kontrola aplikacji, inspekcja pakietów, segmentacja stref, polityki DPI/AV/IPS/Content Filter.
14. Opracowanie pełnej dokumentacji powdrożeniowej:
- aktualne konfiguracje urządzeń (firewalle i przełączniki),
 - końcowa mapa sieci VLAN,
 - zestawienie adresacji, rezerwacji DHCP i przypisań portów,
 - dokumentacja dostępów administracyjnych
15. Przeprowadzenie szkolenia technicznego (transfer wiedzy) dla administratorów Zamawiającego w zakresie:
- zarządzania VLANami na przełącznikach,
 - administracji firewallami,
 - modyfikacji reguł międzysegmentowych,

- diagnozy problemów sieciowych.
16. Całość konfiguracji i wdrożenia musi być zgodna z dobrymi praktykami producentów sprzętu, w tym szczególnie w zakresie wysokiej dostępności, separacji stref, monitorowania i audytowalności konfiguracji.
 17. Transfer wiedzy w tym szkolenia /instruktarze szkolenia dla administratorów Zamawiającego z wdrożonego rozwiązania. Szkolenia /instruktarze prowadzone będą dla 2 osób. Ilość godzinowa oraz forma szkolenia (on-line/ stacjonarnie) zostanie ustalona wspólnie przez Zamawiającego i Wykonawcę .
 18. Dokumentacja Powdrożeniowa (DP) : DP zawierać musi opis wdrożonych rozwiązań oraz instrukcje konfiguracji wdrożonych rozwiązań do wykorzystania przez administratorów Zamawiającego.
 19. Zamawiający wymaga od wykonawcy 3 letniego świadczenia usług utrzymaniowych w zakresie przeprowadzonego wdrożenia segmentacji. W ramach usług utrzymaniowych wymagane jest:
 - bieżące wsparcie w zakresie utrzymania poprawnej konfiguracji segmentacji sieci,
 - nadzór nad integralnością reguł routingu i polityk bezpieczeństwa pomiędzy segmentami sieci,
 - konsultacje techniczne i rekomendacje dotyczące optymalizacji segmentacji sieci,
 - interwencje serwisowe w przypadku błędów lub incydentów związanych z konfiguracją VLAN,
 - przygotowywanie dokumentacji powdrożeniowej i aktualizacja schematów logicznych sieci w przypadku modyfikacji
 - zapewnienie systemu zgłoszeniowego (np. w formie portalu serwisowego lub dedykowanego adresu e-mail) umożliwiającego rejestrowanie zgłoszeń serwisowych

7. Switche dostępne – rozbudowa infrastruktury LAN, zapewniająca bezpieczny dostęp do środowiska wirtualnego i usług IT dla użytkowników (10 szt.)

Wymagania podstawowe

1. Przełącznik do sieci LAN w metalowej obudowie
2. Wysokość urządzenia maksymalnie 1U - montaż w standardowej szafie 19"
3. Głębokość urządzenia nie większa niż 35 cm
4. Przełącznik musi posiadać wbudowany zasilacz AC 230V
5. Przełącznik wyposażony w min.:
 - 48 portów 10/100/1000BASE-T
 - 8 portów SFP+ 1/10G
6. Porty 10/100/1000BASE-T muszą pracować w trybie Full/Half Duplex
7. Przełącznik musi wspierać IEEE 802.3az Energy Efficient Ethernet
8. Przełącznik musi wspierać obsługę diagnostyki wkładek SFP/SFP+

9. Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów
10. Przełącznik musi posiadać możliwość łączenia do 8 przełączników w stos
11. Przepustowośćstosu min. 40 Gb/s
12. Możliwość budowy stosu za pomocą portów 10G SFP+
13. Stos musi zachowywać się jako jedno urządzenie logiczne, a w szczególności musi mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem
14. Nieblokująca architektura o wydajności przełączania min. 256 Gb/s
15. Szybkośćprzełączania: 190.5 Mp/s
16. Pamięć operacyjna: min. 1 GB pamięci DRAM
17. Pamięć flash: min. 1 GB pamięci Flash
18. Dedykowany port konsoli szeregowej RS-232 (RJ45)
19. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika
20. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
21. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
22. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash
23. Możliwośćmonitorowaniazajętości CPU
24. Możliwośćmonitorowaniazajętości pamięci
25. Zabezpieczenie przełącznikaprzedatakami DoS
 - Network Ingress Filtering RFC 2267
 - SYN Attack Protection
 - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
26. Wsparciemirroringuruchu
 - Lokalny mirroring na przełączniku
 - Zdalny mirroring
 - Zdalny mirroring do wskazanego adresu IP poprzez tunel - np. GRE
 - Możliwość mirroringu ruchu ingress wybranego za pomocą listy kontroli dostępu ACL - ingress

Funkcje L2 przełącznika

27. Tablica MAC adresów min. 32 tys.
28. Obsługa sieci wirtualnych IEEE 802.1Q - min. 4 tys.
29. Obsługa przypisywania ruchu do VLAN na podstawie typu protokołu lub rodzaju enkapsulacji
30. Obsługa sieci wirtualnych bazujących na MAC adresach
31. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieciowych
32. Obsługa Q-in-Q IEEE 802.1ad
33. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
34. Obsługa STP (Spanning Tree Protocol) IEEE 802.1D
35. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
36. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s
37. Obsługa PVST+ (Per-VLAN Spanning Tree Protocol)
38. Obsługa min. 64 instancji MSTP

39. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP
 - obsługa min. 128 grup łączy typu Link Aggregation
 - obsługa umożliwiająca grupowanie min. 8 portów
40. Obsługa MLAG (Multi Chassis Link Aggregation)
41. Przełącznik musi posiadać funkcję umożliwiającą statyczne skonfigurowanie portu głównego zapasowego. W stanie normalnym, bez awarii, jest używany port główny, port zapasowy jest nieaktywny. Gdy port wskazany jako główny ulegnie awarii, czyli wykryje brak połączenia (link down), to port zapasowy się automatycznie aktywuje
42. Obsługa protokołu EAPS - RFC 3619
43. Obsługa protokołu ERPS / G.8032
44. Obsługa Quality of Service
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
 - 8 kolejek priorytetów na każdym porcie wyjściowym
 - Obsługa kolejek Strict Priority
 - Obsługa kolejek Weighted Round Robin
 - Obsługa WRED (Weighted Random Early Detection)
45. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
46. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
47. Obsługa CDPv1 oraz CDPv2
48. Przełącznik musi posiadać obsługę AVB (Audio Video Bridging)
49. Przełącznik musi wspierać Voice VLAN
 - bazujący na LLDP
 - bazujący na adresie OUI
50. Kontrola szturmów:
 - Możliwość ograniczenia liczby pakietów Multicast na porcie
 - Możliwość ograniczenia liczby pakietów Broadcast na porcie
 - Możliwość ograniczenia liczby pakietów Unknown Unicast na porcie
51. Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP
52. Wsparcie DCB (Data Center Bridging):
 - DCBX - Data Center Bridging eXchange
 - PFC - Priority-based Flow Control

Funkcje L3 przełącznika IPv4

53. Obsługa min. 1500 interfejsów IP
54. Wsparcie dla IP multinetting - wiele adresów przypisanych do jednej sieci VLAN
55. Sprzętowa obsługa routingu IPv4
56. Pojemność sprzętowej tabeli routingu min. 12 tys. wpisów
57. Obsługa routingu statycznego IPv4
58. Obsługa routingu dynamicznego IPv4
 - RIP v1/v2
 - OSPFv2 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję
 - BGPv4 min. 2 sąsiadów
 - ISIS - możliwość rozszerzenia przez licencję

59. Obsługa redundancji routingu VRRP dla IPv4
60. Policy Based Routing dla IPv4
61. Wsparcie routingu ECMP (Equal-Cost Multi-Path)
62. Obsługa DHCP Relay
63. Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów
64. Obsługa Opcji 82 dla DHCP

Funkcje L3 przełącznika IPv6

65. Sprzętowa obsługa routingu IPv6
66. Pojemność tabeli routingu min. 6 tys. wpisów
67. Obsługa routingu statycznego IPv6
68. Obsługa routingu dynamicznego IPv6
 - RIPng
 - OSPFv3 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję
 - BGPv4 min. 2 sąsiadów
 - ISIS - możliwość rozszerzenia przez licencję
69. Obsługa redundancji routingu VRRP dla IPv6
70. Policy Based Routing dla IPv6
71. Wsparcie routingu ECMP (Equal-Cost Multi-Path)
72. Obsługa 6to4 (RFC 3056)
73. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

Obsługa ruchu rozgłoszeniowego

74. Statyczne przyłączanie portu do grupy multicast
75. Filtrowanie IGMP
76. Obsługa IGMP v1 - RFC 1112
77. Obsługa IGMP v2 - RFC 2236
78. Obsługa IGMP v3 - RFC 3376
79. Obsługa IGMP v1/v2 snooping
80. Obsługa IGMP v3 snooping
81. Obsługa PIM-SM
82. Obsługa PIM-DM - możliwość rozszerzenia przez licencję
83. Obsługa PIM-SSM - możliwość rozszerzenia przez licencję
84. Obsługa MLDv1
85. Obsługa MLDv2
86. Obsługa MLD snooping
87. Obsługa MVR (Multicast VLAN Registration)

Funkcje bezpieczeństwa

88. Obsługa logowania do sieci Network Login
 - IEEE 802.1x based Network Login
 - MAC address based Network Login
 - Web based Network Login
89. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
90. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation

91. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x
92. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication
93. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink
94. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na portach dołączonych do przełączników obsługujących IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging
95. Automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA
96. Automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA
97. Przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów
98. Obsługa Guest VLAN dla IEEE 802.1x
99. Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci
100. Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu - CoA RFC 5176
101. Obsługa wymuszania ponownego periodycznego uwierzytelnienia (Reauthentication)
102. Obsługa RADIUS Authentication (RFC 2865)
103. Obsługa RADIUS Accounting (RFC 2866)
104. Obsługa RADIUS Authentication over TLS (RadSec)
105. Obsługa RADIUS Accounting over TLS (RadSec)
106. Obsługa TACACS+ (RFC 1492)
107. Bezpieczeństwo MAC adresów
 - ograniczenie liczby MAC adresów na porcie
 - zatrzaśnięcie MAC adresów na porcie
 - możliwość wpisania statycznych MAC adresów na port/vlan
108. Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning)
109. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4
 - Adres MAC źródłowy i docelowy plus maska
 - Adres IP źródłowy i docelowy plus maska dla IPv4
 - Adres IP źródłowy i docelowy plus maska dla IPv6
 - Protokół - np.. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd..
 - Numery portów źródłowych i docelowych TCP, UDP
 - Zakresy portów źródłowych i docelowych TCP, UDP
 - Identyfikator sieci VLAN - VLAN ID
 - Quality of Service IEEE 802.1p
 - Quality of Service DiffServ/DSCP
 - Flagi TCP
 - Obsługa fragmentów

110. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika
111. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI
112. Wsparcie 8 tys. wpisów ACL na wejściu (Ingress)
113. Wsparcie 1 tys. wpisów ACL na wyjściu (Egress)
114. Obsługa IP Security
 - Trused DHCP Server
 - DHCP Snooping and Guard
 - Gratuitous ARP Protection
 - DHCP Secured ARP/ARP Validation
 - IP Source Guard
115. Ograniczenie przepustowości (ratelimiting) na portach wyjściowych
116. Ograniczenie przepustowości (ratelimiting) ruchu wybranego przez ACL
117. Obsługa wykrywania periodycznego zaniku linku (Port-Flap):
 - możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu na wskazany czas
 - możliwość raportowania zdarzenia poprzez Syslog
 - możliwość raportowania zdarzenia poprzez Trap SNMP
118. Możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-128
119. Możliwość rozbudowy przełącznika o wsparcie szyfracji MACSec IEEE 802.1AE - GCM-AES-256
120. Wydajność MACSec po rozbudowie przełącznika nie mniejsza niż: 25 Gb/s

Zarządzanie

121. Zarządzenia przez SNMP v1/v2/v3
122. Obsługa SNMP Traps
123. Obsługa synchronizacji czasu NTP
124. Obsługa synchronizacji czasu NTP
125. Obsługa DNS klienta
126. Zarządzanie przez przeglądarkę www - protokół http i https
127. Możliwość zarządzania przez protokół XML
128. Możliwość zarządzania przez protokół RESTConf
129. Obsługa serwera SSH dla IPv4
130. Obsługa serwera SSH dla IPv6
131. Obsługa klienta SSH dla IPv4
132. Obsługa klienta SSH dla IPv6
133. Obsługa serwera Telnet dla IPv4
134. Obsługa serwera Telnet dla IPv6
135. Obsługa klienta Telnet dla IPv4
136. Obsługa klienta Telnet dla IPv6
137. Obsługa transferu plików:

- TFTP
 - SFTP
 - SCP
138. Obsługa SYSLOG
 139. Obsługa Secure SYSLOG (TLS)
 140. Obsługa SYSLOG - konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń
 141. Obsługa logowania komend CLI do logu systemowego
 142. Obsługa logowania komend do serwera SYSLOG
 143. Obsługa ping dla IPv4 i IPv6
 144. Obsługa traceroute dla IPv4 i IPv6
 145. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events
 146. Obsługa RMON2
 147. Obsługa logowania ruchy typu Flow

Inne

148. Współpraca przełącznika z lokalnym (onsite) systemem zarządzającym oferowanym przez producenta przełączników
149. Współpraca przełącznika z chmurowym systemem zarządzającym oferowanym przez producenta przełączników
150. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników
151. Wbudowany DHCP Server
152. DHCP Server z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
153. Wbudowany DHCP Client - per VLAN
154. Obsługa skryptów CLI
155. Obsługa funkcji TCL/Tk w skryptach CLI
156. Obsługa skryptów Python 3.x
157. Możliwość uruchamiania skryptów:
 - ręcznie z CLI przez administratora
 - o określonym czasie lub co wskazany czas
 - na podstawie zdarzeń z logu systemowego
158. Możliwość edycji skryptów bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych
159. Wsparcie standardu IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging
160. Wsparcie VXLAN

Zgodność z normami

161. EU RoHS - 2011/65/EU
162. EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage
163. EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation
164. EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational

Gwarancja

165. Dożywotnia gwarancja na sprzęt - min. 5 lat po zakończeniu sprzedaży

166. Dożywnia aktualizacja oprogramowania na przełączniku - min. 2 lata po zakończeniu sprzedaży

Dodatkowo, zamawiający wymaga dostarczenia systemu zarządzania siecią (NMS) o poniższych funkcjonalnościach:

- Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.
 - Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare, Hyper-V, Nutanix.
 - Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
- Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
- Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami.
- Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępuów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
- Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
- Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
- Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
- Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
- Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
- Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
- Aplikacja musi zapewniać możliwość zarządzania urządzeniami poprzez SNMP MIB-I oraz SNMP MIB-II
- Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.
- Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
- Aplikacja musi posiadać wbudowany Syslog serwer.
- Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
- Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
- Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.
- Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
 - Wysłanie e-mail do wskazanej grupy adresowej
 - Wysłanie informacji SYSLOG do wskazanego serwera
 - Wysłanie TRAP SNMP do wskazanego adresu IP
 - Uruchomienie skryptu w systemie operacyjnym Linux

- Uruchomienie skryptu skonfigurowanego w systemie zarządzającym
- Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
- Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
- Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
- Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
 - połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
 - konfiguracji sieci VLAN
- Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
- Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
 - adres IP urządzenia
 - adresu MAC urządzenia
 - nazwy urządzenia
 - wersji oprogramowania
 - wersji bootrom
 - lokalizacji urządzenia
 - danych kontaktowych administratora
 - numeru seryjnego
 - numeru inwentaryzacyjnego – własna numeracja
- Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
 - możliwość automatycznej periodicznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
 - możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
 - możliwość odtworzenia wskazanej konfiguracji urządzenia
 - możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
 - możliwość obsługi backup'u urządzeń sieciowych różnych producentów
- Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
- Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
- Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
- Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
- Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
 - przyłączenia do sieci VLAN
 - przyłączenia do serwisu w ramach „Fabric” z wykorzystaniem IEEE 802.1Qcj,
 - konfiguracji Quality of Service
 - konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
 - możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest

przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.

- Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
 - szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
 - wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
 - wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
 - generowanie raportów
- Aplikacja zarządzająca musi zapewniać zarządzania siecią bezprzewodową.
 - Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
 - Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax
 - Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
 - adres IP kontrolera
 - liczba obsługiwanych klientów
 - szczytowe wartości zajmowanego pasma
 - wersja oprogramowania
 - Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
 - adres IP punktu dostępowego
 - MAC adres punktu dostępowego
 - wersja oprogramowania
 - typ punktu dostępowego
 - kanały pracy poszczególnych interfejsów radiowych
 - szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
 - Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
 - adres IP klienta
 - MAC adres klienta
 - nazwa użytkownika
 - nazwa punktu dostępowego, do którego dołączony jest użytkownik
 - BSSID, do którego dołączony jest użytkownik
 - SSID, do którego dołączony jest użytkownik
 - Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
 - zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
 - zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
 - lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych

- Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:
 - adresu MAC
 - adresu IP
 - nazwy komputera
 - typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
 - nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
 - adres IP urządzenia, do którego dołączony jest klient.
 - identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
 - typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberosnooping itp.
 - nazwa przydzielonej polityki bezpieczeństwa.
- System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
- System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
- System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:
 - Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
 - Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
 - Realizacji przyłączenia do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC
 - Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.
 - Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
- System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.
- Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.
- System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.

- System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS
- System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.
- System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.
- System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.
- System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
 - liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
 - liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
 - liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
 - liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
 - liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
- System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
- W chwili dostawy Zamawiający nie wymaga dostarczenia żadnych licencji ani subskrypcji na uruchomienie systemu zarządzania tożsamością, niemniej jednak wszystkie wymienione funkcjonalności muszą być możliwe do spełnienia w chwili kiedy Zamawiający będzie chciał wdrożyć system zarządzania tożsamością zintegrowany z systemem zarządzania siecią w późniejszym czasie.
- System zarządzania przy współpracy z dostarczonymi urządzeniami musi pozwolić na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej.
- Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.
- Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.
- System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos
- System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.
- Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.
- System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.
- System Analityki musi zapewniać możliwość tworzenia raportów.

- System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.
- System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
- System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
- System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
- System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub okresowo (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu
- System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
- System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:
 - Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall takimi jak: PaloAlto, Fortinet, Checkpoint
 - Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
 - Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM
- System zarządzania musi być objęty **minimum 3 letnim** wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.
- Zamawiający wymaga, aby wszystkie dostarczane urządzenia sieciowe pochodziły od jednego producenta, co ma na celu zapewnienie unifikacji infrastruktury teleinformatycznej, spójności zarządzania, kompatybilności funkcjonalnej oraz uproszczenie utrzymania i serwisowania systemu.

8. Switch warstwy rdzeniowej (4 szt.)

Wymagania podstawowe

1. Przełącznik do sieci LAN w metalowej obudowie
2. Wysokość urządzenia maksymalnie 1U - montaż w standardowej szafie 19"
3. Zasilacze muszą mieć możliwość wymiany w trakcie pracy przełącznika (Hot-swap), w chwili dostawy przełącznik wyposażony w 2 zasilacze
4. Redundancjawentylacji - min. N+1
5. Wentylatory wymienne w czasie pracy (Hot Swap)
6. Przełącznik wyposażony w min.:
 - 24 porty 1/10G SFP+
 - 2 porty 40G QSFP+
 - 4 porty 10/25G SFP28 z obsługą MACSec
7. Możliwość wyposażenia przełącznika w moduł rozszerzeń:
 - 4 porty 1/10 SFP+
 - 4 porty 1/10 SFP+ z obsługą MACSec oraz wkładek 10GBASE-LRM

8. Przełącznik musi wspierać obsługę diagnostyki wkładek SFP/SFP+/SFP28/QSFP/QSFP28
9. Wszystkie porty muszą być aktywne i zgodne z wymaganiami co do prędkości i liczby portów
10. Przełącznik musi posiadać możliwość łączenia do 8 przełączników w stos
11. Przepustowośćstosu min. 160 Gb/s
12. Możliwość budowy stosu za pomocą portów 10G SFP+
13. Możliwość budowy stosu za pomocą portów 40G QSFP+
14. Dedykowane 2 porty do budowy stosu przełączników
15. Stos musi zachowywać się jako jedno urządzenie logiczne, a w szczególności musi mieć możliwość bezpośredniej konfiguracji wszystkich fizycznych portów dostępnych na przełącznikach połączonych w stos, oraz posiadać jeden adres IP w celu zarządzania stosem
16. Nieblokująca architektura o wydajności przełączania min. 1080 Gb/s
17. Szybkość przełączania: 803.5 Mp/s
18. Pamięć operacyjna: min. 2 GB pamięci DRAM
19. Pamięć flash: min. 2 GB pamięci Flash
20. Dedykowany port konsoli szeregowej RS-232 (RJ45)
21. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
22. Możliwość instalacji min. dwóch wersji oprogramowania - firmware
23. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash
24. Możliwość monitorowania zajętości CPU
25. Możliwośćmonitorowaniazajętościipamięci
26. Zabezpieczenie przełącznikaprzedatakami DoS
 - Network Ingress Filtering RFC 2267
 - SYN Attack Protection
 - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
27. Wsparciemirroringuruchu
 - Lokalny mirroring na przełączniku
 - Zdalny mirroring
 - Zdalny mirroring do wskazanego adresu IP poprzez tunel - np. GRE
 - Możliwość mirroringu ruchu ingress wybranego za pomocą listy kontroli dostępu ACL - ingress

Funkcje L2 przełącznika

28. Tablica MAC adresów min. 114 tys.
29. Obsługa sieci wirtualnych IEEE 802.1Q - min. 4 tys.
30. Obsługa przypisywania ruchu do VLAN na podstawie typu protokołu lub rodzaju enkapsulacji
31. Obsługa sieci wirtualnych bazujących na MAC adresach
32. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieciowych
33. Obsługa Q-in-Q IEEE 802.1ad
34. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
35. Obsługa min. 64 instancji MSTP
36. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP
 - obsługa min. 128 grup łączy typu Link Aggregation
 - obsługaumożliwiającazgrupowanie min. 32 portów
37. Obsługa MLAG (Multi Chassis Link Aggregation)

38. Przełącznik musi posiadać funkcję umożliwiającą statyczne skonfigurowanie portu głównego zapasowego. W stanie normalnym, bez awarii, jest używany port główny, port zapasowy jest nieaktywny. Gdy port wskazany jako główny ulegnie awarii, czyli wykryje brak połączenia (link down), to port zapasowy się automatycznie aktywuje
39. Obsługa protokołu EAPS - RFC 3619
40. Obsługa protokołu ERPS / G.8032
41. Obsługa Quality of Service
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p
 - Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ
 - 8 kolejek priorytetów na każdym porcie wyjściowym
 - Obsługa kolejek Strict Priority
 - Obsługa kolejek Weighted Round Robin
 - Obsługa WRED (Weighted Random Early Detection)
42. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
43. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
44. Obsługa CDPv1 oraz CDPv2
45. Przełącznik musi posiadać obsługę AVB (Audio Video Bridging)
46. Przełącznik musi wspierać Voice VLAN
 - bazujący na LLDP
 - bazujący na adresie OUI
47. Kontrolaszturmów:
 - Możliwość ograniczenia liczby pakietów Multicast na porcie
 - Możliwość ograniczenia liczby pakietów Broadcast na porcie
 - Możliwość ograniczenia liczby pakietów UnknownUnicast na porcie
48. Przełącznik musi wspierać mechanizm zabezpieczenia przed pętlami inny niż STP
49. Wsparcie DCB (Data Center Bridging):
 - DCBX - Data Center Bridging eXchange
 - PFC - Priority-based Flow Control
 - ETS - Enhanced Transmission Selection

Funkcje L3 przełącznika IPv4

50. Obsługa min. 2048 interfejsów IP
51. Wsparcie dla IP multinetting - wiele adresów przypisanych do jednej sieci VLAN
52. Sprzętowa obsługa routingu IPv4
53. Pojemność sprzętowej tabeli routingu min. 80 tys. wpisów
54. Obsługa routingu statycznego IPv4
55. Obsługa routingu dynamicznego IPv4
 - RIP v1/v2
 - OSPFv2 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję
 - BGPv4 min. 2 sąsiadów
 - ISIS - możliwość rozszerzenia przez licencję
56. Obsługa redundancji routingu VRRP dla IPv4
57. Policy Based Routing dla IPv4
58. Wsparcie routingu ECMP (Equal-Cost Multi-Path)

- 59. Obsługa DHCP Relay
- 60. Obsługa DHCP Relay z możliwością wysłania zapytań jednocześnie do min. 4 serwerów
- 61. Obsługa Opcji 82 dla DHCP

Funkcje L3 przełącznika IPv6

- 62. Sprzętowa obsługa routingu IPv6
- 63. Pojemność tabeli routingu min. 40 tys. wpisów
- 64. Obsługa routingu statycznego IPv6
- 65. Obsługa routingu dynamicznego IPv6
 - RIPng
 - OSPFv3 min. 4 aktywne interfejsy IP - możliwość rozszerzenia do pełnej funkcjonalności przez licencję
 - BGPv4 min. 2 sąsiadów
 - ISIS - możliwość rozszerzenia przez licencję
- 66. Obsługa redundancji routingu VRRP dla IPv6
- 67. Policy Based Routing dla IPv6
- 68. Wsparcie routingu ECMP (Equal-Cost Multi-Path)
- 69. Obsługa 6to4 (RFC 3056)
- 70. Opcja IPv6 Router Advertisement dla DNS - RFC 6106

Obsługa ruchu rozgłoszeniowego

- 71. Statyczne przyłączanie portu do grupy multicast
- 72. Filtrowanie IGMP
- 73. Obsługa IGMP v1 - RFC 1112
- 74. Obsługa IGMP v2 - RFC 2236
- 75. Obsługa IGMP v3 - RFC 3376
- 76. Obsługa IGMP v1/v2 snooping
- 77. Obsługa IGMP v3 snooping
- 78. Obsługa PIM-SM
- 79. Obsługa PIM-DM - możliwość rozszerzenia przez licencję
- 80. Obsługa PIM-SSM - możliwość rozszerzenia przez licencję
- 81. Obsługa MLDv1
- 82. Obsługa MLDv2
- 83. Obsługa MLD snooping
- 84. Obsługa MVR (Multicast VLAN Registration)

Funkcje bezpieczeństwa

- 85. Obsługa logowania do sieci Network Login
 - IEEE 802.1x based Network Login
 - MAC address based Network Login
 - Web based Network Login
- 86. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants)
- 87. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation
- 88. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci IEEE 802.1x

89. Przydział sieci VLAN, ACL/QoS, dla uwierzytelnionego użytkownika lub urządzenia, podczas logowania do sieci MAC authentication
90. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na wskazanych portach uplink
91. Automatyczne wytworzenie sieci VLAN przesłanej podczas logowania IEEE 802.1x lub MAC authentication w ramach RFC 3580 wraz z automatycznym dodaniem tej sieci VLAN na portach dołączonych do przełączników obsługujących IEEE 802.1Qcj - Automatic Attachment to Provider BackboneBridging
92. Automatyczne włączenie DHCP snooping dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA
93. Automatyczne włączenie ARP Inspection dla klienta logującego się z wykorzystaniem IEEE 802.1x lub MAC authentication - poprzez RADIUS VSA
94. Przełącznik musi posiadać mechanizm pozwalający na wyłączenie uwierzytelniania na porcie, za pomocą RADIUS VSA, np. w przypadku wykrycia bezprzewodowego punktu dostępowego, który "przejmie" rolę uwierzytelniania klientów
95. Obsługa Guest VLAN dla IEEE 802.1x
96. Możliwość przekierowania klienta na Captive Portal podczas logowania do sieci
97. Obsługa wymuszenia ponownej autoryzacji w celu zmiany autoryzacji klienta (zmiana VLAN, ACL, QoS) bez konieczności wyłączenia i włączania portu - CoA RFC 5176
98. Obsługa wymuszania ponownego okresowego uwierzytelnienia (Reauthentication)
99. Obsługa RADIUS Authentication (RFC 2865)
100. Obsługa RADIUS Accounting (RFC 2866)
101. Obsługa RADIUS Authentication over TLS (RadSec)
102. Obsługa RADIUS Accounting over TLS (RadSec)
103. Obsługa TACACS+ (RFC 1492)
104. Bezpieczeństwo MAC adresów
 - ograniczenie liczby MAC adresów na porcie
 - zatrzaśnięcie MAC adresów na porcie
 - możliwość wpisania statycznych MAC adresów na port/vlan
105. Możliwość wyłączenia nauki MAC adresów na switchu (disable MAC learning)
106. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL na warstwie 2, 3 i 4
 - Adres MAC źródłowy i docelowy plus maska
 - Adres IP źródłowy i docelowy plus maska dla IPv4
 - Adres IP źródłowy i docelowy plus maska dla IPv6
 - Protokół - np.. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd..
 - Numery portów źródłowych i docelowych TCP, UDP
 - Zakresy portów źródłowych i docelowych TCP, UDP
 - Identyfikator sieci VLAN - VLAN ID
 - Quality of Service IEEE 802.1p
 - Quality of Service DiffServ/DSCP
 - Flagi TCP
 - Obsługa fragmentów
107. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika

108. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komendy CLI
109. Wsparcie 9 tys. wpisów ACL na wejściu (Ingress)
110. Wsparcie 1 tys. wpisów ACL na wyjściu (Egress)
111. Obsługa IP Security
- Trused DHCP Server
 - DHCP Snooping and Guard
 - Gratuitous ARP Protection
 - DHCP Secured ARP/ARP Validation
 - IP Source Guard
112. Ograniczenie przepustowości (ratelimiting) na portach wyjściowych
113. Ograniczenie przepustowości (ratelimiting) ruchu wybranego przez ACL
114. Obsługa wykrywania periodycznego zaniku linku (Port-Flap):
- możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu
 - możliwość automatycznej reakcji polegającej na wyłączeniu portu na wskazany czas
 - możliwość raportowania zdarzenia poprzez Syslog
 - możliwość raportowania zdarzenia poprzez Trap SNMP

Zarządzanie

115. Zarządzenia przez SNMP v1/v2/v3
116. Obsługa SNMP Traps
117. Obsługa synchronizacji czasu SNTP
118. Obsługa synchronizacji czasu NTP
119. Obsługa DNS klienta
120. Zarządzanie przez przeglądarkę www - protokół http i https
121. Możliwość zarządzania przez protokół XML
122. Możliwość zarządzania przez protokół RESTConf
123. Obsługa serwera SSH dla IPv4
124. Obsługa serwera SSH dla IPv6
125. Obsługa klienta SSH dla IPv4
126. Obsługa klienta SSH dla IPv6
127. Obsługa serwera Telnet dla IPv4
128. Obsługa serwera Telnet dla IPv6
129. Obsługa klienta Telnet dla IPv4
130. Obsługa klienta Telnet dla IPv6
131. Obsługa transferu plików:
- TFTP
 - SFTP
 - SCP
132. Obsługa SYSLOG
133. Obsługa Secure SYSLOG (TLS)
134. Obsługa SYSLOG - konfiguracja wielu serwerów SYSLOG z możliwością definicji wysyłanych zdarzeń

- 135. Obsługa logowania komend CLI do logu systemowego
- 136. Obsługa logowania komend do serwera SYSLOG
- 137. Obsługa ping dla IPv4 i IPv6
- 138. Obsługa traceroute dla IPv4 i IPv6
- 139. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events
- 140. Obsługa RMON2
- 141. Obsługa logowania ruchu typu Flow
- 142. Obsługa logowania ruchu IPFix

Inne

- 143. Współpraca przełącznika z lokalnym (onsite) systemem zarządzającym oferowanym przez producenta przełączników
- 144. Współpraca przełącznika z chmurowym systemem zarządzającym oferowanym przez producenta przełączników
- 145. Współpraca z systemem kontroli dostępu oferowanym przez producenta przełączników
- 146. Wbudowany DHCP Server
- 147. DHCP Server z możliwością definicji opcji (np. opcje 43, 60, 78 itp.)
- 148. Wbudowany DHCP Client - per VLAN
- 149. Obsługa skryptów CLI
- 150. Obsługa funkcji TCL/Tk w skryptach CLI
- 151. Obsługa skryptów Python 3.x
- 152. Możliwość uruchamiania skryptów:
 - ręcznie z CLI przez administratora
 - o określonym czasie lub co wskazany czas
 - na podstawie zdarzeń z logu systemowego
- 153. Możliwość edycji skryptów bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych
- 154. Wsparcie standardu IEEE 802.1Qcj - Automatic Attachment to Provider Backbone Bridging
- 155. Możliwość rozbudowy przełącznika o wsparcie MPLS
- 156. Wsparcie VXLAN

Zgodność z normami

- 157. EU RoHS - 2011/65/EU
- 158. EN/ETSI 300 019-2-1 v2.1.2 - Class 1.2 Storage
- 159. EN/ETSI 300 019-2-2 v2.1.2 - Class 2.3 Transportation
- 160. EN/ETSI 300 019-2-3 v2.1.2 - Class 3.1e Operational

Gwarancja

- 161. Dożywotnia gwarancja na sprzęt - min. 5 lat po zakończeniu sprzedaży
- 162. Dożywotnia aktualizacja oprogramowania na przełączniku - min. 2 lata po zakończeniu sprzedaży

Dodatkowo, zamawiający wymaga dostarczenia systemu zarządzania siecią (NMS) o poniższych funkcjonalnościach:

- Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.

- Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare, Hyper-V, Nutanix.
 - Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
- Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
- Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami.
- Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowychostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
- Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
- Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
- Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokoły SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
- Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
- Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
- Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
- Aplikacja musi zapewniać możliwość zarządzania urządzeniami poprzez SNMP MIB-I oraz SNMP MIB-II
- Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.
- Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
- Aplikacja musi posiadać wbudowany Syslog server.
- Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
- Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
- Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.
- Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
 - Wysłanie e-mail do wskazanej grupy adresowej
 - Wysłanie informacji SYSLOG do wskazanego serwera
 - Wysłanie TRAP SNMP do wskazanego adresu IP
 - Uruchomienie skryptu w systemie operacyjnym Linux
 - Uruchomienie skryptu skonfigurowanego w systemie zarządzającym
- Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
- Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
- Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
- Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem

- połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
 - konfiguracji sieci VLAN
- Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
- Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
 - adres IP urządzenia
 - adresu MAC urządzenia
 - nazwy urządzenia
 - wersji oprogramowania
 - wersji bootrom
 - lokalizacji urządzenia
 - danych kontaktowych administratora
 - numeru seryjnego
 - numeru inwentaryzacyjnego – własna numeracja
- Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
 - możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
 - możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
 - możliwość odtworzenia wskazanej konfiguracji urządzenia
 - możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
 - możliwość obsługi backup'u urządzeń sieciowych różnych producentów
- Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
- Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
- Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
- Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
- Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
 - przyłączenia do sieci VLAN
 - przyłączenia do serwisu w ramach „Fabric” z wykorzystaniem IEEE 802.1Qcj,
 - konfiguracji Quality of Service
 - konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
 - możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.
- Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
 - szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).

- wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
 - wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
 - generowanie raportów
- Aplikacja zarządzająca musi zapewniać zarządzania siecią bezprzewodową.
 - Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępnych i ich stanie (działa / nie działa).
 - Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax
 - Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
 - adres IP kontrolera
 - liczba obsługiwanych klientów
 - szczytowe wartości zajmowanego pasma
 - wersja oprogramowania
 - Musi być zapewniona widzialność parametrów wszystkich punktów dostępnych zawierających następujące informacje:
 - adres IP punktu dostępowego
 - MAC adres punktu dostępowego
 - wersja oprogramowania
 - typ punktu dostępowego
 - kanały pracy poszczególnych interfejsów radiowych
 - szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
 - Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
 - adres IP klienta
 - MAC adres klienta
 - nazwa użytkownika
 - nazwa punktu dostępowego, do którego dołączony jest użytkownik
 - BSSID, do którego dołączony jest użytkownik
 - SSID, do którego dołączony jest użytkownik
 - Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępnych. Mapy muszą zapewniać następujące funkcjonalności:
 - zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
 - zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
 - lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępnych
- Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:
 - adresu MAC
 - adresu IP
 - nazwy komputera
 - typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
 - nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.

- adres IP urządzenia, do którego dołączony jest klient.
 - identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
 - typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberosnooping itp.
 - nazwa przydzielonej polityki bezpieczeństwa.
- System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
- System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
- System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:
 - Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
 - Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
 - Realizacji przyłączenia do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC
 - Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.
 - Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
- System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.
- Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.
- System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
- System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS
- System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.
- System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.

- System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.
- System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
 - liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
 - liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
 - liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
 - liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
 - liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
- System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
- W chwili dostawy Zamawiający nie wymaga dostarczenia żadnych licencji ani subskrypcji na uruchomienie systemu zarządzania tożsamością, niemniej jednak wszystkie wymienione funkcjonalności muszą być możliwe do spełnienia w chwili kiedy Zamawiający będzie chciał wdrożyć system zarządzania tożsamością zintegrowany z systemem zarządzania siecią w późniejszym czasie.
- System zarządzania przy współpracy z dostarczonymi urządzeniami musi pozwolić na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej.
- Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.
- Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.
- System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos
- System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.
- Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.
- System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.
- System Analityki musi zapewniać możliwość tworzenia raportów.
- System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.
- System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
- System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)

- System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
- System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu
- System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
- System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:
 - Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall takimi jak: PaloAlto, Fortinet, Checkpoint
 - Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
 - Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM
- System zarządzania musi być objęty **minimum 3 letnim** wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.
- Zamawiający wymaga, aby wszystkie dostarczane urządzenia sieciowe pochodziły od jednego producenta, co ma na celu zapewnienie unifikacji infrastruktury teleinformatycznej, spójności zarządzania, kompatybilności funkcjonalnej oraz uproszczenie utrzymania i serwisowania systemu.

9. Zakup małych switchy dostępowych w celu eliminacji obecnie pracujących urządzeń bez wsparcia (mini switche) (10 szt.)

Wymagania podstawowe

1. Przełącznik posiadający 8 portów 10/100/1000BASE-T
2. Przełącznik posiadający 4 porty 1GBE SFP
3. Wysokość urządzenia 1U
4. Nieblokująca architektura o wydajności przełączania min. 36 Gb/s
5. Szybkość przełączania min. 26.5 Milionów pakietów na sekundę
6. Tablica MAC adresów min. 16k
7. Pamięć operacyjna: min. 512 MB pamięci DRAM
8. Pamięć flash: min. 128 MB pamięci Flash
9. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
10. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci
11. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
12. Obsługa Q-in-Q IEEE 802.1ad
13. Obsługa Quality of Service
 - a. IEEE 802.1p
 - b. DiffServ
 - c. 8 kolejek priorytetów na każdym porcie wyjściowym
14. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB
15. Obsługa LLDP Media Endpoint Discovery (LLDP-MED)
16. Przełącznik wyposażony w modułarny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
17. Wbudowany DHCP Serwer i klient
18. Możliwość instalacji min. dwóch wersji oprogramowania - firmware

19. Możliwość przechowywania min. kilkunastu wersji konfiguracji w plikach tekstowych w pamięci Flash
20. Możliwość monitorowania zajętości CPU
21. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring)
22. Obsługa CDPv2
23. Obsługa IPv4 unicast i multicast L2
24. Obsługa IPv6 unicast i multicast L2

Obsługa Multicastów

25. Filtrowanie IGMP
26. Obsługa Multicast VLAN Registration - MVR
27. Obsługa IGMP v1/v2/v3 snooping

Bezpieczeństwo

28. Obsługa Network Login
 - a. IEEE 802.1x - RFC 3580
 - b. Web-based Network Login
 - c. MAC based Network Login
29. Obsługa wielu klientów Network Login na jednym porcie (Multiplesuplicants)
30. Możliwość integracji funkcjonalności Network Login z Microsoft NAP
31. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
32. Obsługa Guest VLAN dla IEEE 802.1x
33. Możliwość dynamicznego przypisania VLAN, QOS, ratelimiting użytkownikowi zidentyfikowanemu poprzez 802.1x lub MAC authentication
34. Obsługa Identity Management
35. Zabezpieczenie CPU przełącznika urządzenia przed atakami DoS
36. Obsługa RADIUS Authentication (RFC 2138)
37. RADIUS and TACACS+ per-command Authentication
38. Bezpieczeństwo MAC adresów
 - a. ograniczenie liczby MAC adresów na porcie
 - b. zatrzaśnięcie MAC adresu na porcie
 - c. możliwość wpisania statycznych MAC adresów na port/vlan
39. Możliwość wyłączenia MAC learning
40. Obsługa SNMPv3
41. Klient SSH2
42. Listy kontroli dostępu ACL
 - a. Adres MAC źródłowy i docelowy plus maska
 - b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6
 - c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.
 - d. Numery portów źródłowych i docelowych TCP, UDP
 - e. Zakresy portów źródłowych i docelowych TCP, UDP
 - f. Identyfikator sieci VLAN - VLAN ID
 - g. Flagi TCP
 - h. Obsługa fragmentów
43. Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika
44. Obsługa bezpiecznego transferu plików SCP/SFTP
45. Obsługa DHCP Option 82

Bezpieczeństwo sieciowe

46. Możliwość konfiguracji portu głównego i zapasowego
47. Obsługa STP (Spanning Tree Protocol) IEEE 802.1D
48. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
49. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s

50. Obsługa PVST+
51. Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619
52. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP

Zarządzanie

53. Obsługa synchronizacji czasu SNTP (Simple Network Time Protocol)
54. Obsługa synchronizacji czasu NTP
55. Zarządzanie przez SNMP v1/v2/v3
56. Zarządzanie przez przeglądarkę WWW – protokół HTTPS/SSL
57. Możliwość zarządzania poprzez protokół XML
58. Telnet Serwer/Klient dla IPv4 / IPv6
59. SSH2 Serwer/Klient dla IPv4 / IPv6
60. Ping dla IPv4 / IPv6
61. Traceroute dla IPv4 / IPv6
62. BOOTP relay dla IPv4 / IPv6
63. Obsługa SYSLOG z możliwością definiowania wielu serwerów
64. Obsługa sFlow
65. Obsługa RMON min. 4 grupy: Status, History, Alarms, Events (RFC 1757)
66. Obsługa RMON2 (RFC 2021)

Inne

67. Zakres temperatury pracy 0-40 °C
68. Obsługa skryptów CLI
69. Obsługa funkcji TCL/Tk w skryptach CLI
70. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych)
71. Możliwość uruchamiania skryptów
 - a. Ręcznie
 - b. O określonym czasie lub co wskazany okres czasu
 - c. Na podstawie wpisów w logu systemowym

Gwarancja

72. Dożywotnia gwarancja na sprzęt - min. 5 lat po zakończeniu sprzedaży
73. Dożywotnia aktualizacja oprogramowania na przełączniku - min. 2 lata po zakończeniu sprzedaży

Dodatkowo, zamawiający wymaga dostarczenia systemu zarządzania siecią (NMS) o poniższych funkcjonalnościach:

- Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.
 - Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare, Hyper-V, Nutanix.
 - Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
- Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
- Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami.
- Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
- Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.

- Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
- Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
- Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
- Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
- Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
- Aplikacja musi zapewniać możliwość zarządzania urządzeniami poprzez SNMP MIB-I oraz SNMP MIB-II
- Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.
- Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapy SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
- Aplikacja musi posiadać wbudowany Syslog server.
- Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
- Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
- Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.
- Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
 - Wysłanie e-mail do wskazanej grupy adresowej
 - Wysłanie informacji SYSLOG do wskazanego serwera
 - Wysłanie TRAP SNMP do wskazanego adresu IP
 - Uruchomienie skryptu w systemie operacyjnym Linux
 - Uruchomienie skryptu skonfigurowanego w systemie zarządzającym
- Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
- Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
- Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
- Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
 - połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
 - konfiguracji sieci VLAN
- Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
- Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
 - adres IP urządzenia
 - adresu MAC urządzenia
 - nazwy urządzenia
 - wersji oprogramowania
 - wersji bootrom
 - lokalizacji urządzenia

- danych kontaktowych administratora
 - numeru seryjnego
 - numeru inwentaryzacyjnego – własna numeracja
- Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
 - możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
 - możliwość realizacji backup'u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
 - możliwość odtworzenia wskazanej konfiguracji urządzenia
 - możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
 - możliwość obsługi backup'u urządzeń sieciowych różnych producentów
- Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
- Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
- Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
- Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
- Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
 - przyłączenia do sieci VLAN
 - przyłączenia do serwisu w ramach „Fabric” z wykorzystaniem IEEE 802.1Qcj,
 - konfiguracji Quality of Service
 - konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
 - możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.
- Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
 - szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
 - wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
 - wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
 - generowanie raportów
- Aplikacja zarządzająca musi zapewniać zarządzania siecią bezprzewodową.
 - Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
 - Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax

- Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
 - adres IP kontrolera
 - liczba obsługiwanych klientów
 - szczytowe wartości zajmowanego pasma
 - wersja oprogramowania
- Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
 - adres IP punktu dostępowego
 - MAC adres punktu dostępowego
 - wersja oprogramowania
 - typ punktu dostępowego
 - kanały pracy poszczególnych interfejsów radiowych
 - szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
- Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
 - adres IP klienta
 - MAC adres klienta
 - nazwa użytkownika
 - nazwa punktu dostępowego, do którego dołączony jest użytkownik
 - BSSID, do którego dołączony jest użytkownik
 - SSID, do którego dołączony jest użytkownik
- Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
 - zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
 - zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
 - lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
- Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:
 - adresu MAC
 - adresu IP
 - nazwy komputera
 - typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
 - nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
 - adres IP urządzenia, do którego dołączony jest klient.
 - identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
 - typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberosnooping itp.
 - nazwa przydzielonej polityki bezpieczeństwa.
- System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.

- System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
- System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:
 - Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
 - Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
 - Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC
 - Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.
 - Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
- System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.
- Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.
- System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
- System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS
- System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.
- System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.
- System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.
- System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
 - liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
 - liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
 - liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
 - liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
 - liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.

- System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
- W chwili dostawy Zamawiający nie wymaga dostarczenia żadnych licencji ani subskrypcji na uruchomienie systemu zarządzania tożsamością, niemniej jednak wszystkie wymienione funkcjonalności muszą być możliwe do spełnienia w chwili kiedy Zamawiający będzie chciał wdrożyć system zarządzania tożsamością zintegrowany z systemem zarządzania siecią w późniejszym czasie.
- System zarządzania przy współpracy z dostarczonymi urządzeniami musi pozwolić na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej.
- Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.
- Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.
- System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos
- System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.
- Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.
- System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.
- System Analityki musi zapewniać możliwość tworzenia raportów.
- System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.
- System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
- System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
- System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
- System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub okresowo (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czasu
- System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
- System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:
 - Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall takimi jak: PaloAlto, Fortinet, Checkpoint

- Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
 - Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM
- System zarządzania musi być objęty **minimum 3 letnim** wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.
- Zamawiający wymaga, aby wszystkie dostarczane urządzenia sieciowe pochodziły od jednego producenta, co ma na celu zapewnienie unifikacji infrastruktury teleinformatycznej, spójności zarządzania, kompatybilności funkcjonalnej oraz uproszczenie utrzymania i serwisowania systemu.

10. Pakiet ochrony antywirusowej – zabezpieczenie serwerów, maszyn wirtualnych oraz urządzeń końcowych przed zagrożeniami malware, ransomware i innymi atakami

Zamawiający wymaga dostarczenia licencji dla 170 stanowisk, na okres 3 lat, o poniższych funkcjonalnościach:

Administracja zdalna

1. Konsola centralnego zarządzania musi być dostępna w wersji lokalnej (on-prem) oraz w wersji chmurowej (SaaS).
2. Rozwiązanie musi umożliwiać dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW.
3. Rozwiązanie musi być zabezpieczone za pośrednictwem protokołu szyfrowanego SSL/TLS.
4. Rozwiązanie musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
5. Rozwiązanie musi posiadać dedykowaną aplikację pochodzącą od tego samego producenta co konsola zarządzająca, umożliwiającą co najmniej:
 - 5.1. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną i serwerem centralnego zarządzania,
 - 5.2. Pośredniczenie w komunikacji pomiędzy stacją zarządzaną a serwerami aktualizacjami producenta,
 - 5.3. Buforowanie ruchu HTTPS.
6. Rozwiązanie musi posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
7. Rozwiązanie musi posiadać możliwość wymuszenia dwuskładnikowego uwierzytelnienia podczas logowania do konsoli administracyjnej.
 - 7.1. Uwierzytelnianie dwuskładnikowe musi być realizowane co najmniej przy pomocy następujących aplikacji mobilnych dla systemów iOS oraz Android:
 - 7.1.1. Google Authenticator,
 - 7.1.2. Microsoft Authenticator,
 - 7.1.3. Authy,
 - 7.1.4. Aplikacji pochodzącej od tego samego producenta konsoli centralnego zarządzania.
8. Rozwiązanie musi posiadać minimum 80 szablonów raportów, przygotowanych przez producenta.

9. Rozwiązanie musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
 - 9.1. 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:
 - 9.1.1. adresy sieciowe IP,
 - 9.1.2. aktywne zagrożenia,
 - 9.1.3. stan funkcjonowania oraz ochrony,
 - 9.1.4. wersja systemu operacyjnego,
 - 9.1.5. podzespoły komputera.
10. Rozwiązanie musi posiadać możliwość uruchomienia zadań automatycznie oraz co najmniej z wyzwalaczem:
 - 10.1. wyrażenie CRON,
 - 10.2. codziennie,
 - 10.3. cotygodniowo,
 - 10.4. co miesiąc,
 - 10.5. co rok,
 - 10.6. po wystąpieniu nowego zdarzenia,
 - 10.7. po automatycznym umieszczeniu hosta w grupie dynamicznej.
11. Konsola centralnego zarządzania musi być dostępna co najmniej w językach polskim oraz angielskim
 - 11.1. Język konsoli centralnego zarządzania musi być możliwy do zmiany bez przeinstalowania ani ponownego uruchomienia procesu systemu centralnego zarządzania
12. Rozwiązanie musi mieć możliwość tagowania obiektów.
13. Rozwiązanie musi posiadać możliwość eksportu danych do zewnętrznych systemów, w tym co najmniej Syslog.
 - 13.1. Eksport danych musi być możliwy w co najmniej następujących formatach:
 - 13.1.1. JSON,
 - 13.1.2. LEEF,
 - 13.1.3. CEF.

Ochrona stacji roboczych - Windows

1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - 3.1. wirus,
 - 3.2. trojan,
 - 3.3. robak,
 - 3.4. adware,
 - 3.5. spyware,
 - 3.6. dialer,
 - 3.7. phishing,
 - 3.8. backdoor.
4. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami aktywnymi oraz ukrywającymi się.

6. Rozwiązanie musi posiadać ochronę przed podłączeniem hosta do sieci botnet.
7. Rozwiązanie musi posiadać funkcjonalność automatycznego przywracania plików po ich zaszyfrowaniu przez oprogramowanie typu ransomware.
 - 7.1. Technologia ta musi być autorskim rozwiązaniem producenta rozwiązania ochrony stacji roboczych.
 - 7.2. Technologia umożliwiająca przywrócenie plików po ich zaszyfrowaniu nie może wykorzystywać mechanizmu VSS (Volume ShadowCopy Service).
 - 7.3. Technologia, która tworzy kopię zapasową plików musi działać w czasie rzeczywistym i zabezpieczać pliki przed modyfikacją przez podejrzane procesy.
8. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
9. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 10.1. całego dysku,
 - 10.2. wybranych katalogów,
 - 10.3. pojedynczych plików,
 - 10.4. plików spakowanych oraz skompresowanych,
 - 10.5. dysków sieciowych,
 - 10.6. dysków przenośnych.
11. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 11.1. wybranych plików,
 - 11.2. wybranych procesów,
 - 11.3. wybranych lokalizacji,
 - 11.4. wybranych rozszerzeń,
 - 11.5. nazwy wykrycia,
 - 11.6. sumy kontrolnej (SHA1).
12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
13. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - 13.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - 13.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 13.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
14. 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).
15. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów co najmniej HTTPS, POP3S, IMAPS.
16. 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 heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.

17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:

17.1. typ urządzenia:

- 17.1.1. pamięci masowe,
- 17.1.2. optyczne pamięci masowe,
- 17.1.3. pamięci masowe Firewire,
- 17.1.4. urządzenia do tworzenia obrazów,
- 17.1.5. drukarki USB,
- 17.1.6. urządzenia Bluetooth,
- 17.1.7. czytniki kart inteligentnych,
- 17.1.8. modemy,
- 17.1.9. porty LPT/COM, 17.1.10. urządzenia przenośne.

17.2. parametry urządzenia:

- 17.2.1. numer seryjny, 17.2.2. producent,
- 17.2.3. model.

17.3. typ dostępu:

- 17.3.1. brak możliwości zapisu,
- 17.3.2. pełen dostęp,
- 17.3.3. ostrzeżenie użytkownika, 17.3.4. brak dostępu.

18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

- 18.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- 18.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- 18.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- 18.4. 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,
- 18.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.

19. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.

19.1. 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.

19.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.

19.3. Raport musi posiadać co najmniej:

- 19.3.1. Listę zainstalowanych aplikacji,

- 19.3.2. Listę usług systemowych,
 - 19.3.3. Informacje o systemie operacyjnym i sprzęcie,
 - 19.3.4. Listę aktywnych procesów i połączeń sieciowych,
 - 19.3.5. Harmonogram systemu operacyjnego,
 - 19.3.6. Szczegóły pliku hosts,
 - 19.3.7. Informacje o sterownikach.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
- 20.1. antywirus,
 - 20.2. zaporą osobista
 - 20.3. sandbox,
 - 20.4. antyspyware,
 - 20.5. metody heurystyczne.
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń atakujących, jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową realizowaną przez dedykowaną wtyczkę.
- 22.1. Wtyczka ta musi być dostępna jako plugin dla klienta pocztowego Microsoft Outlook.
 - 22.2. Ochrona musi być realizowana w oparciu o co najmniej:
 - 22.1.1. globalna czarna lista RBL,
 - 22.1.2. czarna lista użytkownika,
 - 22.1.3. biała lista użytkownika, na którą automatycznie muszą zostać dodane adres email z książki adresowej klienta Microsoft Outlook.
23. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
- 23.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 23.1.1. Skanowanie portów TCP oraz UDP,
 - 23.1.2. Wykrywanie duplikacji adresu IP,
 - 23.1.3. Atak zatrutowania ARP,
 - 23.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.
 - 23.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
 - 23.2.1. RDP,
 - 23.2.2. SMB,
 - 23.2.3. My SQL,
 - 23.2.4. MS SQL.
 - 23.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
24. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
- 24.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
 - 24.2. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
 - 24.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,

- 24.2.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - 24.2.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - 24.2.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
 - 24.2.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.
25. Rozwiązanie musi posiadać moduł bezpiecznej przeglądarki, pochodzący od producenta tego samego rozwiązania antywirusowego.
- 25.1. Bezpieczna przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
 - 25.2. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
 - 25.3. W przypadku połączenia aplikacji zdalnej (w tym przynajmniej aplikacja TeamViewer) kolor ramki musi ulec zmianie oraz musi pojawić się alert informujący o zdalnym połączeniu.
26. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych pochodzący od tego samego producenta.
- 26.1. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 160 kategorii i podkategorii.
 - 26.2. Rozwiązanie musi umożliwiać stworzenie własnego komunikatu na zablokowanych stronach w oparciu o co najmniej: 26.2.1. Treść komunikatu, 26.2.2. Obraz.

Ochrona stacji roboczych – MacOS

- 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 11 (Big Sur) oraz nowszych.
- 2. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
- 3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - 3.1. wirus,
 - 3.2. trojan,
 - 3.3. robak,
 - 3.4. adware,
 - 3.5. spyware,
 - 3.6. dialer,
 - 3.7. phishing, 3.8. backdoor.
- 4. 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.
- 5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
- 6. Rozwiązanie musi chronić pliki co najmniej za pomocą:
 - 6.1. Sygnatur wirusów.
 - 6.2. Reputacji chmurowej.

7. Rozwiązanie musi umożliwiać 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).
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - 8.1. Sprawdzenie reputacji działających aplikacji i plików co najmniej z poziomu interfejsu programu.
 - 8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 9.1. całego dysku,
 - 9.2. wybranych katalogów,
 - 9.3. pojedynczych plików,
 - 9.4. plików spakowanych oraz skompresowanych,
 - 9.5. Dysków sieciowych,
 - 9.6. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 10.1. wybranych plików,
 - 10.2. wybranych procesów,
 - 10.3. wybranych lokalizacji,
 - 10.4. wybranych rozszerzeń,
 - 10.5. nazwy wykrycia,
 - 10.6. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
 - 11.1. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 30 wbudowanych reguł, stworzonych przez producenta.
 - 11.2. Zapora osobista musi posiadać co najmniej dwa tryby pracy:
 - 11.2.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 11.2.2. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,

Ochrona stacji roboczych – Linux

1. Rozwiązanie musi wspierać co najmniej następujące systemy operacyjne:
 - 1.1. Ubuntu Desktop, 1.2.Red Hat Enterprise Linux
 - 1.3.Linux Mint.
2. Rozwiązanie musi obsługiwać co najmniej następujące środowiska pulpitu:
 - 2.1. Cinnamon,
 - 2.2. GNOME,
 - 2.3. KDE,
 - 2.4. MATE,

2.5. XFCE.

3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - 3.1. wirus,
 - 3.2. trojan,
 - 3.3. robak,
 - 3.4. adware,
 - 3.5. spyware,
 - 3.6. dialer,
 - 3.7. phishing,
 - 3.8. backdoor.
4. 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.
5. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
6. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - 6.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 6.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
7. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 7.1. całego dysku,
 - 7.2. wybranych katalogów,
 - 7.3. pojedynczych plików,
 - 7.4. plików spakowanych oraz skompresowanych,
 - 7.5. dysków sieciowych,
 - 7.6. dysków przenośnych.
8. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 8.1. wybranych plików,
 - 8.2. wybranych procesów,
 - 8.3. wybranych lokalizacji,
 - 8.4. wybranych rozszerzeń,
9. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - 9.1. typ urządzenia:
 - 9.1.1. pamięci masowe,
 - 9.1.2. optyczne pamięci masowe,
 - 9.2. parametry urządzenia:
 - 9.2.1. numer seryjny, 9.2.2. producent,
 - 9.2.3. model.
 - 9.3. typ dostępu:
 - 9.3.1. brak możliwości zapisu,

9.3.2. pełen dostęp, 9.3.3. brak dostępu.

Ochrona serwera – Windows Server

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
 - 1.1. Microsoft Windows Server 2012 R2,
 - 1.2. Microsoft Windows Server 2016, 1.3. Microsoft Windows Server 2019,
 - 1.4. Microsoft Windows Server 2022, 1.5. Microsoft Windows Server 2025.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - 3.1. wirus,
 - 3.2. trojan,
 - 3.3. robak,
 - 3.4. adware,
 - 3.5. spyware,
 - 3.6. dialer,
 - 3.7. phishing,
 - 3.8. backdoor.
4. Rozwiązanie musi zapewniać możliwość skanowania dysków sieciowych typu NAS.
5. 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.
6. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
7. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
8. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:
 - 8.1. Sprawdzenie reputacji działających procesów i plików co najmniej z poziomu interfejsu programu oraz menu kontekstowego.
 - 8.2. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 8.3. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
9. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 9.1. całego dysku,
 - 9.2. wybranych katalogów,
 - 9.3. pojedynczych plików,
 - 9.4. plików spakowanych oraz skompresowanych,
 - 9.5. dysków sieciowych,
 - 9.6. dysków przenośnych.
10. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 10.1. wybranych plików,
 - 10.2. wybranych procesów,

- 10.3. wybranych lokalizacji,
 - 10.4. wybranych rozszerzeń,
 - 10.5. nazwy wykrycia,
 - 10.6. sumy kontrolnej (SHA1).
11. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
12. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- 12.1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
 - 12.2. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
 - 12.3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
 - 12.4. 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,
 - 12.5. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
13. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji.
- 13.1. 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.
 - 13.2. Musi istnieć możliwość wygenerowania raportu na temat stacji przy pomocy dedykowanej aplikacji typu standalone pochodzącej od tego samego producenta co oprogramowanie do zabezpieczenia stacji roboczej.
 - 13.3. Raport musi posiadać co najmniej:
 - 13.3.1. Listę zainstalowanych aplikacji,
 - 13.3.2. Listę usług systemowych,
 - 13.3.3. informacje o systemie operacyjnym i sprzęcie,
 - 13.3.4. Listę aktywnych procesów i połączeń sieciowych,
 - 13.3.5. harmonogram systemu operacyjnego,
 - 13.3.6. Szczegóły pliku hosts,
 - 13.3.7. Informacje o sterownikach.
14. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci operacyjnej, z którego korzystają co najmniej następujące funkcje systemu
- 14.1. antywirus,
 - 14.2. zapora osobista
 - 14.3. sandbox,
 - 14.4. antyspyware,
 - 14.5. metody heurystyczne.
15. Rozwiązanie musi skanować system wirtualny w trybie online oraz offline w środowisku Hyper-V.

16. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
17. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników oraz grup urządzeń na stacji w oparciu o co najmniej:
 - 17.1. typ urządzenia:
 - 17.1.1. pamięci masowe,
 - 17.1.2. optyczne pamięci masowe,
 - 17.1.3. pamięci masowe Firewire,
 - 17.1.4. urządzenia do tworzenia obrazów,
 - 17.1.5. drukarki USB,
 - 17.1.6. urządzenia Bluetooth,
 - 17.1.7. czytniki kart inteligentnych,
 - 17.1.8. modemy,
 - 17.1.9. porty LPT/COM, 17.1.10. urządzenia przenośne.
 - 17.2. parametry urządzenia:
 - 17.2.1. numer seryjny, 17.2.2. producent,
 - 17.2.3. model.
 - 17.3. typ dostępu:
 - 17.3.1. brak możliwości zapisu,
 - 17.3.2. pełen dostęp,
 - 17.3.3. ostrzeżenie użytkownika, 17.3.4. brak dostępu.
18. Rozwiązanie musi automatycznie wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki co najmniej dla następujących usług:
 - 18.1. MS SQL,
 - 18.2. Active Directory,
 - 18.3. IIS,
 - 18.4. Sysvol,
 - 18.5. DNS,
 - 18.6. DHCP,
 - 18.7. Hyper-V,
 - 18.8. Konsola centralnego zarządzania tego samego producenta rozwiązania antywirusowego.
19. Rozwiązanie musi posiadać wbudowany system IDS, który musi posiadać co najmniej następujące funkcjonalności:
 - 19.1. Ochrona przed anomaliami sieciowymi, w tym co najmniej:
 - 19.1.1. Skanowanie portów TCP oraz UDP,
 - 19.1.2. Wykrywanie duplikacji adresu IP,
 - 19.1.3. Atak zatrutowania ARP,
 - 19.1.4. Nieprawidłowa długość pakietu TCP oraz UDP.
 - 19.2. Ochrona przed atakami typu brute-force dla co najmniej usług oraz protokołów:
 - 19.2.1. RDP,
 - 19.2.2. SMB,
 - 19.2.3. My SQL,
 - 19.2.4. MS SQL.

- 19.3. Możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
20. Rozwiązanie musi posiadać moduł zapory osobistej, która pochodzi od tego samego producenta rozwiązania antywirusowego.
21. Zapora osobista musi działać w oparciu o reguły i musi posiadać co najmniej 60 wbudowanych reguł, stworzonych przez producenta.
- 21.1. Zapora osobista musi posiadać co najmniej cztery tryby pracy:
- 21.1.1. tryb automatyczny – rozwiązanie blokuje ruch przychodzący i zezwala tylko na połączenia wychodzące,
 - 21.1.2. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
 - 21.1.3. tryb oparty na regułach – rozwiązanie blokuje ruch przychodzący i wychodzący,
 - 21.1.4. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące.
- 21.1.4.1. Administrator musi posiadać możliwość skonfigurowania czasu działania trybu.

Ochrona serwera – Linux

1. Rozwiązanie musi wspierać systemy w tym co najmniej:
 - 1.1. RedHat Enterprise Linux (RHEL),
 - 1.2. Rocky Linux,
 - 1.3. Ubuntu,
 - 1.4. Debian,
 - 1.5. SUSE Linux Enterprise Server (SLES),
 - 1.6. Oracle Linux,
 - 1.7. Amazon Linux.
2. Rozwiązanie musi zapewniać wykrywanie i usuwanie zagrożeń co najmniej typu:
 - 2.1. wirus,
 - 2.2. trojan,
 - 2.3. robak,
 - 2.4. adware,
 - 2.5. spyware,
 - 2.6. dialer,
 - 2.7. phishing,
 - 2.8. backdoor.
3. Rozwiązanie musi zapewniać możliwość zdalnego skanowania przy pomocy protokołu ICAP oraz ICAPS.
4. 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.
5. Rozwiązanie musi wspierać automatyczną, inkrementacyjną aktualizację silnika detekcji.
6. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
7. Rozwiązanie musi posiadać system wczesnego ostrzegania oparty na chmurze pochodzący od tego samego producenta oprogramowania antywirusowego, który umożliwia co najmniej:

- 7.1. Konfigurację wysyłania wszystkich plików do analizy oprócz dokumentów użytkowników.
 - 7.2. Konfigurację dodatkowych wykluczeń rozszerzeń plików, które nie mają być wysyłane do analizy.
8. Rozwiązanie musi zapewniać skanowanie na żądanie, z menu kontekstowego oraz zgodnie z harmonogramem co najmniej:
 - 8.1. całego dysku,
 - 8.2. wybranych katalogów,
 - 8.3. pojedynczych plików,
 - 8.4. plików spakowanych oraz skompresowanych,
 - 8.5. dysków sieciowych,
 - 8.6. dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania co najmniej:
 - 9.1. wybranych plików,
 - 9.2. wybranych procesów,
 - 9.3. wybranych lokalizacji,
 - 9.4. wybranych rozszerzeń,
10. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
 - 10.1. Lokalna konsola administracyjna nie może wymagać do swojej pracy uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
11. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
12. 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.
13. Rozwiązanie musi wykrywać oraz podejrzane działania w kontenerach i blokować je. Ochrona musi skanować kontener co najmniej w następujących fazach:
 - 13.1. proces budowania obrazu kontenera,
 - 13.2. wdrażanie obrazu kontenera.

Mobile Device Management

1. Konsola centralnego zarządzania dostępna w wersji chmurowej musi posiadać możliwość zarządzania urządzeniami mobilnymi – MDM.
2. MDM musi pochodzić od tego samego producenta konsoli centralnego zarządzania.
 - 2.1. MDM musi umożliwiać zarządzanie urządzeniami mobilnymi z systemami:
 - 2.1.1. Android,
 - 2.1.2. iOS,
 - 2.1.3. iPadOS.
 - 2.2. MDM musi posiadać możliwość integracji co najmniej z następującymi rozwiązaniami:
 - 2.2.1. Microsoft Entra ID (co najmniej w zakresie synchronizacji użytkowników),

- 2.2.2. Microsoft Intune (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - 2.2.3. VMware Workspace One (co najmniej w zakresie automatycznej rejestracji urządzenia mobilnego z systemem Android w konsoli zdalnego zarządzania),
 - 2.2.4. Apple Business Manager (ABM),
 - 2.2.5. Android Enterprise (co najmniej w zakresie Device Owner).
- 3. MDM musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
 - 3.1. usunięcie zawartości urządzenia,
 - 3.2. przywrócenie urządzenia do ustawień fabrycznych,
 - 3.3. zablokowanie urządzenia,
 - 3.4. uruchomienie sygnału dźwiękowego,
 - 3.5. lokalizację GPS,
 - 3.6. Resetowanie hasła blokady ekranu.
- 4. MDM musi zapewniać administratorowi podejrzanie listy zainstalowanych aplikacji.
- 5. MDM musi umożliwiać co najmniej:
 - 5.1. Dla systemów iOS oraz iPadOS
 - 5.1.1. konfigurację kont e-mail,
 - 5.1.2. konfigurację połączeń VPN,
 - 5.1.3. Konfigurację połączeń Wi-Fi,
 - 5.1.4. Konfigurację listy certyfikatów,
 - 5.1.5. możliwość uruchomienia trybu jednej aplikacji.
 - 5.2. Dla systemu Android:
 - 5.2.1. blokadę wykonywania połączeń,
 - 5.2.2. blokadę konfiguracji sieci Wi-Fi,
 - 5.2.3. blokadę konfiguracji tuneli VPN,
 - 5.2.4. zarządzanie aktualizacjami systemu operacyjnego, 5.2.5. blokadę zmiany tapety urządzenia.

Mobile Threat Defense (MTD) dla systemu Android

- 1. Rozwiązanie musi posiadać pełne wsparcie dla systemów Android 9 (Pie) oraz nowszych.
- 2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania:
 - 2.1. Inteligentne – tylko skanowanie aplikacji w pamięci wewnętrznej i na karcie SD.
 - 2.2. Dokładne - skanowanie wszystkich typów plików w pamięci wewnętrznej i na karcie SD.
- 3. Rozwiązanie musi zapewniać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).
- 4. Rozwiązanie musi posiadać możliwość zdefiniowania poziomu zabezpieczeń urządzenia w tym przynajmniej:
 - 4.1. Złożoność kodu blokady ekranu:
 - 4.1.1. Wzór,
 - 4.1.2. PIN,
 - 4.1.3. Hasło,
 - 4.2. Przywrócenie urządzenia do ustawień fabrycznych w przypadku przekroczenia dopuszczalnej liczby prób odblokowania ekranu,

- 4.3. Zdefiniowanie czasu obowiązywania (ważności) kodu blokady ekranu.
5. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
- 5.1. nazwę aplikacji,
 - 5.2. nazwę pakietu,
 - 5.3. kategorię sklepu Google Play,
 - 5.4. uprawnienia aplikacji,
 - 5.5. pochodzenie aplikacji z nieznanego źródła.
6. Rozwiązanie musi posiada ochronę przed zagrożeniami typu phishing.

Sandbox w chmurze

1. Rozwiązanie musi być integralną częścią oprogramowania antywirusowego, bez potrzeby instalacji dodatkowych rozszerzeń.
2. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi wspierać systemy w tym co najmniej:
 - 3.1. Microsoft Windows 10 oraz 11,
 - 3.2. Microsoft Windows Server,
 - 3.3. macOS 11 (Big Sur) oraz nowszych
 - 3.4. RedHat Enterprise Linux (RHEL),
 - 3.5. Rocky Linux,
 - 3.6. Ubuntu,
 - 3.7. Debian,
 - 3.8. SUSE Linux Enterprise Server (SLES),
 - 3.9. Oracle Linux,
 - 3.10. Amazon Linux.
4. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
5. Rozwiązanie musi wykorzystywać do działania chmurę producenta tego samego rozwiązania antywirusowego.
6. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym co najmniej:
 - 6.1. archiwa,
 - 6.2. skrypty,
 - 6.3. pliki wykonywalne,
 - 6.4. pliki rejestru systemowego (.reg),
 - 6.5. możliwy spam,
 - 6.6. dokumenty.
7. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta w tym co najmniej:
 - 7.1. natychmiast po ich przeanalizowaniu,
 - 7.2. po upływie 30 dni,
 - 7.3. nigdy.
8. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
9. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
10. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy z poziomu konsoli centralnego zarządzenia.
11. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizację stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.

12. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika, za pomocą wspieranego produktu.
 - 12.1. Administrator musi mieć dostęp do informacji jakie pliki zostały wysłane oraz przez kogo zostały wysłane.
13. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku musi zakończyć się jednym z poniższych wyników:
 - 13.1. czysty,
 - 13.2. podejrzany,
 - 13.3. bardzo podejrzany,
 - 13.4. szkodliwy.
14. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość co najmniej:
 - 14.1. wstrzymania uruchamiania pobieranych plików z następujących źródeł:
 - 14.1.1. przeglądarki internetowe,
 - 14.1.2. programy poczty e-mail,
 - 14.1.3. nośniki wymienne,
 - 14.1.4. pliki wyodrębnione z archiwum.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić pliki poddane kwarantannie oraz utworzyć dla nich wyłączenia z poziomu konsoli centralnego zarządzania oraz z poziomu klienta antywirusowego.

Szyfrowanie

1. Rozwiązanie musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Rozwiązanie nie może bazować na rozwiązaniu Microsoft Bitlocker.
3. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
4. Rozwiązanie musi umożliwiać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault) poprzez dedykowanego klienta pochodzącego od tego samego producenta rozwiązania antywirusowego.
5. Rozwiązanie musi posiadać autentykację typu pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
 - 5.1. Rozwiązanie musi umożliwiać całkowite oraz czasowe wyłączenia tego uwierzytelnienia.
 - 5.2. Uwierzytelnienie użytkownika musi odbywać się poprzez hasło, którego złożoność może ustalić administrator konsoli centralnego zarządzania.
6. W przypadku gdy użytkownik zapomni hasła, administrator musi mieć możliwość wygenerowania hasła odzyskiwania z poziomu konsoli centralnego zarządzania.
 - 6.1. Hasło odzyskiwania po użyciu musi zostać zmodyfikowane.
 - 6.2. Hasło odzyskiwania nie może być krótsze niż 8 znaków.
 - 6.3. Hasło odzyskiwania nie może być dłuższe niż 20 znaków.
7. Rozwiązanie musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. Rozwiązanie musi umożliwiać zalogowanie się do systemu przy pomocy metody jednokrotnego logowania (SSO) przy wykorzystaniu poświadczeń użytkownika Active Directory.
9. Rozwiązanie musi umożliwiać wykorzystanie modułu TPM w wersji co najmniej 2.0.
10. Rozwiązanie musi wspierać dyski wykorzystujące funkcji OPAL w wersji co najmniej 2.0.
11. W przypadku awarii urządzenia, administrator musi mieć możliwość wygenerowania pliku odzyskiwania który umożliwia odszyfrowanie dysku.

Endpoint Detection and Response / eXtended Detection and Response

1. Moduł EDR / XDR musi pochodzić od tego samego producenta rozwiązania antywirusowego.
2. Ochrona EDR /XDR musi być realizowana przy pomocy dedykowanego konektora, który musi pochodzić od tego samego producenta rozwiązania antywirusowego.
3. Rozwiązanie musi zbierać co najmniej następujące informacje z systemu operacyjnego:
 - 3.1. tworzenie procesów,
 - 3.2. uruchamianie, zatrzymanie i modyfikacja usług,
 - 3.3. utworzenie, uruchomienie, modyfikacja oraz usunięcie zadań w harmonogramie systemowym,
 - 3.4. usuwanie oraz zmiana nazw plików,
 - 3.5. tworzenie i usuwanie kluczy rejestru systemowego,
 - 3.6. ładowanie bibliotek DLL,
 - 3.7. zalogowanie użytkowników,
 - 3.8. elementy sieciowe, w tym co najmniej
 - 3.8.1. pobranie plików wykonywalnych,
 - 3.8.2. zestawienie połączeń TCP/IP, 3.8.3. zapytania HTTP, 3.8.4. zapytania DNS.
4. Rozwiązanie musi posiadać ponad 1500 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa.
 - 4.1. Administrator powinien mieć możliwość edytowania akcji przypisanych do reguł utworzonych zarówno przez producenta, jak i przez siebie, a także możliwość wdrażania automatyzacji tych reguł, opartych co najmniej na następujących akcjach:
 - 4.1.1. blokowanie pliku wykonywalnego,
 - 4.1.2. blokowanie pliku wykonywalnego i poddanie go kwarantannie,
 - 4.1.3. blokowanie podejrzanej biblioteki DLL,
 - 4.1.4. zakończenie procesu,
 - 4.1.5. skanowanie komputera w poszukiwaniu zagrożeń,
 - 4.1.6. wyłączenie komputera,
 - 4.1.7. izolacja sieciowa hosta,
 - 4.1.8. wylogowanie użytkownika.
 - 4.2. Administrator musi posiadać możliwość utworzenia własnych reguł w oparciu o język XML.
5. Rozwiązanie musi posiadać możliwość tworzenia wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
 - 5.1. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy historyczne, które pasują do utworzonego wykluczenia.
 - 5.2. Podstawowe wykluczenia muszą być konfigurowane w oparciu o przynajmniej:
 - 5.2.1. proces,
 - 5.2.2. proces nadrzędny (proces rodzica),
 - 5.2.3. nazwę procesu,
 - 5.2.4. ścieżkę procesu,

- 5.2.5. wiersz polecenia,
 - 5.2.6. wydawcę,
 - 5.2.7. typ podpisu,
 - 5.2.8. SHA-1,
 - 5.2.9. SHA-2,
 - 5.2.10. użytkownika.
- 5.3. Administrator musi mieć możliwość utworzenia wykluczeń zaawansowanych w oparciu o język XML.
- 6. Rozwiązanie musi mieć możliwość blokowania plików po sumach kontrolnych.
 - 6.1. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji usuwania blokowanego pliku.
 - 6.2. Blokowanie pliku musi być możliwe na podstawie co najmniej następujących funkcji skrótu (funkcje hashujące):
 - 6.2.1. SHA-1,
 - 6.2.2. SHA-256.
- 7. Rozwiązanie musi dawać możliwość weryfikacji plików wykonywalnych w środowisku z możliwością podglądu szczegółów wybranego pliku w tym przynajmniej:
 - 7.1. hash pliku SHA-1,
 - 7.2. hash pliku SHA-256,
 - 7.3. hash pliku MD5,
 - 7.4. typ sygnatury podpisu cyfrowego,
 - 7.5. wydawcę certyfikatu,
 - 7.6. wersję pliku,
 - 7.7. oryginalną nazwę pliku,
 - 7.8. rozmiar pliku,
 - 7.9. reputację i popularność pliku w oparciu o system reputacji producenta tego samego rozwiązania antywirusowego,
 - 7.10. pierwsze uruchomienie pliku w środowisku,
 - 7.11. ostatnie uruchomienie pliku w środowisku,
- 8. Rozwiązanie musi dawać możliwość wykonywania następujących czynności dla plików wykonywalnych oraz plików DLL:
 - 8.1. oznaczania ich jako bezpieczne lub niebezpieczne,
 - 8.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - 8.3. zablokowania wykonywania i wykorzystania pliku,
 - 8.4. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
- 9. Rozwiązanie musi dawać możliwość weryfikacji uruchomionych skryptów w środowisku wraz z informacją dotyczącą parametrów uruchomienia (wiersz poleceń).
 - 9.1. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
 - 9.2. pobierania ich do dalszej analizy, a pobierany plik musi być zabezpieczony hasłem,
 - 9.3. wysyłania do sandbox tego samego producenta rozwiązania antywirusowego.
 - 9.4. administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
- 10. Rozwiązanie musi umożliwiać zestawienie sesji terminalowej powershell do stacji końcowej oraz serwera.

- 10.1. Moduł połączenia terminalowego musi być dostępny jedynie dla użytkowników konsoli posiadających skonfigurowane dwuskładnikowe uwierzytelnienia do konsoli.
11. Rozwiązanie musi posiadać mechanizm sztucznej inteligencji, który będzie wspomagał administratora w tworzeniu wykluczeń dla pojawiających się w środowisku alertów.
12. Rozwiązanie musi wspierać integrację z zewnętrznymi silnikami do przeprowadzenia głębszej analizy plików, w tym co najmniej VirusTotal.

11. System zarządzania urządzeniami końcowymi – centralna kontrola nad infrastrukturą IT, monitoring stacji roboczych i serwerów, wsparcie dla bezpieczeństwa środowiska IT

1.	Typ:	Oprogramowanie do zarządzania środowiskiem IT i bezpieczeństwem.
2.	Opis ogólny:	<p>Budowa modułowa: serwera zarządzającego, zdalne konsole oraz agenty. Komunikacja pomiędzy Serwerem a Agentami i Konsolami nawiązywana przy użyciu szyfrowanego protokołu TLS 1.2. Moduły umożliwiają kompleksowy monitoring sieci, monitoring sprzętu komputerowego na stanowiskach użytkowników pod kątem zmian sprzętowych i programowych oraz pomocy w formie interaktywnego połączenia sieciowego z obsługiwany użytkownikiem.</p> <p>Program wykorzystuje darmowy silnik bazy danych z kodem źródłowym dostępnym na licencji open-source (np. PostgreSQL) dzięki czemu nie jest objęty limitem danych.</p> <p>Instalacja Serwera oraz konsol zarządzających dla 64-bitowego systemu operacyjnego Windows.</p> <p>Dane, które dotyczą działań pracownika na komputerze: historia aktywności, polityka korzystania z Internetu oraz aplikacji, dostęp do zewnętrznych nośników danych itp., odseparowane od danych technicznych tj. informacji o stacji roboczej. Grupowane w osobnym, dedykowanym oknie. Zgodnie z RODO, usuwanie danych wybranego użytkownika bez konieczności usunięcia informacji o stacji roboczej.</p> <p>Dostęp do danych osobowych oraz danych z monitoringu, zgodnie z RODO, objęte jest kontrolą na poziomie wybranych Administratorów – możliwość nadawania kontom administracyjnym różnych poziomów dostępu oraz uprawnień zarówno do funkcji Programu, grup urządzeń, jak i użytkowników.</p> <p>Główny Administrator ma możliwość zarządzania uprawnieniami konfiguracyjnymi programu dla innych kont z rolą administracyjną np. może wyłączyć możliwość zdalnej deinstalacji Agenta, ograniczyć dostęp do opcji programu oraz logów działań innych administratorów. Działania administratorów są logowane oznacza to, że program posiada dziennik z listą czynności wykonanych przez administratorów, które zmodyfikowały obiekty znajdujące się w systemie w tym m.in. logowanie dostępu do Opcji programu, logowanie dostępu do informacji o aktywności użytkownika, logowanie poleceń deinstalacji Agenta. Działania administratorów mogą być automatycznie eksportowane do zewnętrznego kolektora Syslog. Lista kont użytkowników, w tym</p>

		<p>administratorów, może być synchronizowana z Active Directory wraz z awatarami, również przez szyfrowane połączenie LDAPS. Program umożliwia również tworzenie lokalnych kont użytkowników wraz z awatarami w środowiskach bez Active Directory. Liczba kont użytkowników w konsoli nie jest objęta limitem i nie podlega licencjonowaniu.</p> <p>Program umożliwia konfigurację polityki haseł do lokalnych kont użytkowników konsoli. Polityk pozwala na określenie: minimalnej długości hasła, liter, cyfr, znaków specjalnych oraz automatycznie wymusza dostosowanie bieżących haseł do obowiązujących zasad.</p>
3.	Licencjonowanie:	Licencja wieczysta na 170 stacji roboczych, możliwość zwiększenia liczby zarządzanych stacji roboczych w ramach jednej licencji w dowolnym czasie. Nielimitowana liczba monitorowanych urządzeń sieciowych.
4.	Konsola administracyjna:	Możliwość instalacji wielu zdalnych konsoli administracyjnych.
5.	Umowa serwisowa:	36 miesięcy, aktualizacje, pomoc techniczna,
7.	Monitorowanie infrastruktury (bezagentowo):	<p>Obejmuje serwery Windows, Linux, Unix, Mac; routery, przełączniki, urządzenia VoIP i firewalle w zakresie:</p> <ul style="list-style-type: none"> <input type="checkbox"/> wykrywania urządzeń w sieci poprzez skanowanie ping oraz arp-ping <input type="checkbox"/> wykrywania urządzeń na podstawie informacji odczytanych z Active Directory (wraz z informacją o OU) <input type="checkbox"/> wizualizacji stanu urządzeń w postaci ikon urządzeń na graficznych mapach sieci <input type="checkbox"/> wizualizacji urządzeń na mapach z funkcją siatki umożliwiającą korygowanie pozycji ikon na mapie do najbliższej linii siatki <input type="checkbox"/> wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z dowolnym kolorem tła. <input type="checkbox"/> wizualizacji map urządzeń poprzez tworzenie spersonalizowanych map z wykorzystaniem jako tła zaimportowanych obrazków np. schematu rozmieszczenia pomieszczeń w budynku <input type="checkbox"/> wizualizacji map urządzeń poprzez grupowanie urządzeń na narysowanych czworokątach o dowolnym rozmiarze i kolorze <input type="checkbox"/> wizualizacji map urządzeń poprzez wstawianie dowolnego tekstu na mapie <input type="checkbox"/> wizualizacji połączeń pomiędzy urządzeniami a przełącznikami za pomocą linii i informacji, do którego portu przełącznika podłączone jest dane urządzenie w sposób manualny oraz automatyczny <input type="checkbox"/> zablokowania mapy urządzeń przed przypadkową edycją <input type="checkbox"/> serwisów TCP/IP, HTTP, POP3, SMTP, FTP i innych wraz z możliwością definiowania własnych serwisów. Program monitoruje czas ich odpowiedzi i procent utraconych pakietów <input type="checkbox"/> serwerów pocztowych: <ul style="list-style-type: none"> - program monitoruje czas logowania do serwisu odbierającego oraz czas wysyłania poczty - program ma możliwość monitorowania stanu systemów i wysyłania powiadomienia (e-mail, SMS i inne), w razie gdyby przestały one odpowiadać lub funkcjonowały wadliwie (np. gdy ważne parametry znajdą się poza

	<p>zakresem)</p> <ul style="list-style-type: none"> - program ma możliwość wykonywania operacji testowych - program ma możliwość wysłania powiadomienia jeśli serwer pocztowy nie działa <input type="checkbox"/> monitorowania serwerów WWW i adresów URL <input type="checkbox"/> cyklicznego monitorowania czasu ładowania strony internetowej, zmiany treści na stronie internetowej i statusu protokołu HTTPS <input type="checkbox"/> obsługi szyfrowania SSL/TLS w powiadomieniach e-mail <input type="checkbox"/> obsługi urządzeń SNMP wspierających SNMP v1/2/3 z szyfrowaniem oraz autoryzacją, (np. przełączniki, routery, drukarki sieciowe, urządzenia VoIP itp.) – monitorowanie wartości za pomocą nazw zmiennych oraz OID <input type="checkbox"/> obsługi komunikatów syslog i pułapek SNMP i ewidencjonowanie odebranych z nich danych <input type="checkbox"/> monitoringu routerów i przełączników wg: <ul style="list-style-type: none"> - zmian stanu interfejsów sieciowych - ruchu sieciowego - podłączonych stacji roboczych – graficzna prezentacja panelu switcha - ruchu generowanego przez podłączone do portów stacje robocze <input type="checkbox"/> serwisów Windows: monitor serwisów Windows alarmuje gdy serwis przestanie działać oraz pozwala na jego uruchomienie/zatrzymanie/zrestartowanie <input type="checkbox"/> wyświetlania statystyk przy każdym urządzeniu na mapie takich jak: czas odpowiedzi urządzenia, czas od ostatniej poprawnej odpowiedzi, nazwa DNS, adres IP, status zarządzalności SNMP, ostrzeżenie o zdarzeniu na urządzeniu <input type="checkbox"/> monitorowania stanu maszyn wirtualnych Vmware: działa, nie działa, wstrzymano <input type="checkbox"/> zarządzania stanem maszyn wirtualnych Vmware: wysyłanie poleceń włączenia, wstrzymania i wyłączenia zasilania do każdej maszyny <input type="checkbox"/> wydajności systemów Windows: <ul style="list-style-type: none"> - obciążenie CPU, pamięci, zajętość dysków, transfer sieciowy <p>Program posiada Inteligentne Mapy i Oddziały, które służą do lepszego zarządzania logiczną strukturą urządzeń w przedsiębiorstwie (Oddziały) oraz tworzą dynamiczne mapy wg własnych filtrów (Mapy Inteligentne). Kryteria automatycznego filtrowania dotyczyć mogą m.in. statusu Agenta, wygenerowanych alarmów, zainstalowanych aplikacji, przynależności do oddziału, serwisów sieciowych, danych z SNMP, danych z inwentaryzacji urządzenia itp. Program posiada również funkcję kompilatora plików MIB, który umożliwia dodawanie definicji dla modułów SNMP.</p> <p>Program umożliwia również nakładanie na urządzenia liczników wydajności WMI oraz SNMP wg szablonów definiowanie alarmów z wykorzystaniem akcji związanych ze zdarzeniami w systemie, m.in.: wysłanie komunikatu pulpitu, wysłanie wiadomości e-mail, wysłanie SMS, wysłanie wiadomości SMS poprzez integrację z serwisem smsapi.pl, wysłanie wiadomości przez Microsoft Teams oraz Slack, uruchomienie programu, wysłanie pułapki SNMP, wysłanie pakietu Wake-On-LAN, zatrzymanie/restart usługi Windows, wyłączenie/restart komputera. Alarmy budowane są przez administratora z wykorzystaniem ciągu przyczynowo skutkowego – oznacza to, że administrator</p>
--	--

		<p>samodzielnie może wskazać dowolne zdarzenie z listy, którego wykrycie wzbudzi alarm oraz dowolną liczbę akcji wybranych z listy, które zostaną wykonane jako reakcja na wykryte zdarzenie. Wykonywanie akcji alarmów można skonfigurować automatycznie po wykryciu zdarzenia, z opóźnieniem, na końcu zdarzenia oraz cyklicznie np. co 5 minut. Dla akcji można nałożyć ograniczenie czasowe np. nie wykonuj między 8:00-16:00. Alarmy pozwalają na priorytetyzację urządzeń, grupowanie wg. ważności i typu urządzenia. Oprogramowanie umożliwia wykorzystanie w alarmowaniu skrzynek e-mail z wykorzystaniem autoryzacji OAuth 2.0</p> <p>Program ma możliwość integracji ze sprzętową bramką GSM HW-SMS-GW 3 w celu wysyłania powiadomień SMS z wykorzystaniem protokołu netGSM (SOAP) oraz poprzez integrację z bramkami SMSEagle.</p>
8.	Inwentaryzacja:	<p>Program automatycznie gromadzi informacje o sprzęcie i oprogramowaniu na stacjach roboczych oraz:</p> <ol style="list-style-type: none"> 1. Prezentuje szczegóły dotyczące sprzętu: modelu, procesora, pamięci, płyty głównej, napędów, kart itp. 2. Umożliwia odczyt parametrów S.M.A.R.T. dysków twardych, dysków SSD, w tym NVMe. 3. Obejmuje m.in.: zestawienie posiadanych konfiguracji sprzętowych, wolne miejsce na dyskach, średnie wykorzystanie pamięci, informacje pozwalające na wytypowanie systemów, dla których konieczny jest upgrade. 4. Informuje o zainstalowanych aplikacjach oraz aktualizacjach Windows co bezpośrednio umożliwia audytowanie i weryfikację użytkowania licencji w organizacji. 5. Zbiera informacje w zakresie wszystkich zmian przeprowadzonych na wybranej stacji roboczej: instalacji/deinstalacji aplikacji, zmian adresu IP itd. 6. Posiada możliwość wysyłania powiadomienia np. e-mailem w przypadku zainstalowania programu lub jakiegokolwiek zmiany konfiguracji sprzętowej komputera. 7. Umożliwia odczytanie numeru seryjnego (klucze licencyjne). 8. Umożliwia automatyczne zarządzanie instalacjami i deinstalacjami oprogramowania poprzez określenie paczek aplikacji wymaganych oraz nieautoryzowanych. 9. Umożliwia przegląd informacji o konfiguracji systemu, np. komend startowych, zmiennych środowiskowych, kontach lokalnych użytkowników, harmonogramie zadań itp. 10. Umożliwia utworzenie listy plików użytkowników z określonym rozszerzeniem (np. filmy .AVI) znalezionych na stacjach roboczych oraz ich zdalne usuwanie wraz z wykrywaniem metadanych plików użytkownika: obrazów (wymiary obrazka), video (długość filmu), audio (długość nagrania), archiwów (liczba plików w środku, rozmiar po wypakowaniu). 11. Umożliwia wymianę plików do i ze stacją roboczą poprzez funkcję Menedżera plików. Działania administratorów wykonywane w tej funkcji są logowane. <p>Moduł inwentaryzacji zasobów umożliwia prowadzenie bazy ewidencji majątku IT w zakresie sprzętu i programowania:</p> <ul style="list-style-type: none"> <input type="checkbox"/> przechowywania wszystkich informacji dotyczących infrastruktury IT w jednym miejscu oraz automatycznego aktualizowania zgromadzonych informacji, <input type="checkbox"/> przydzielania dostępu administratorów do zasobów na podstawie praw do oddziałów, <input type="checkbox"/> tworzenia powiązań między zasobami a urządzeniami, <input type="checkbox"/> tworzenia powiązań między zasobami a kontami użytkowników (zarówno

	<p>lokalnymi, jak i zsynchronizowanymi z Active Directory), wskazywanie osób odpowiedzialnych,</p> <ul style="list-style-type: none"> <input type="checkbox"/> tworzenia relacji pomiędzy zasobami, <input type="checkbox"/> wskazania osób uprawnionych do użycia zasobów poprzez rozbudowane mechanizmy, <input type="checkbox"/> definiowania własnych typów zasobów (elementów wyposażenia), ich atrybutów oraz wartości - dla danego urządzenia lub oprogramowania istnieje możliwość dodawania dodatkowych informacji, np. numer inwentarzowy, osoba odpowiedzialna, numer dokumentu zakupu, wartość sprzętu lub oprogramowania, nazwa sprzedawcy, termin upływu gwarancji, termin kolejnego przeglądu (można podać datę, po której administrator otrzyma powiadomienie e-mail o zbliżającym się terminie przeglądu lub upływie gwarancji), nazwa firmy serwisującej, lub własny komentarz, <input type="checkbox"/> określenia atrybutów wymaganych, które są obowiązkowe dla wszystkich zasobów, <input type="checkbox"/> określenia atrybutów dodatkowych tylko dla wybranych typów zasobów, <input type="checkbox"/> masową edycję atrybutów zasobów, <input type="checkbox"/> definiowanie własnych list jednokrotnego wyboru jako dodatkowe informacje o zasobie, <input type="checkbox"/> importu danych z zewnętrznego źródła (.CSV), <input type="checkbox"/> przechowywania dowolnych dokumentów (np. pliki .DOCX, .XLSX, .PDF), np.: skan faktury zakupu, gwarancji, dowolnego dokumentu itp., <input type="checkbox"/> tworzenia powiązań między zasobami a dokumentami w relacji 1:N, <input type="checkbox"/> oznaczania statusów zasobów, np. w użyciu, w naprawie, zutylizowany itp., <input type="checkbox"/> ewidencji czynności wykonywanych na zasobach, np.: aktualizacja, naprawa w serwisie, konserwacja itp. wraz z możliwością określenia kosztu oraz czasu przeznaczonego na wykonanie czynności, <input type="checkbox"/> generowania zestawienia wszystkich zasobów, w tym urządzeń i zainstalowanego na nich oprogramowania, <input type="checkbox"/> przygotowanie wielu szablonów generowanych dokumentów i protokołów przekazania zasobów wraz z konfigurowalną sekcją zawierającą dane i logo organizacji, <input type="checkbox"/> konfiguracji stylu automatycznego numerowania dodawanych zasobów wg zdefiniowanego wzorca, <input type="checkbox"/> konfiguracji stylu automatycznego numerowania dodawanych dokumentów i protokołów wg zdefiniowanego wzorca, <input type="checkbox"/> archiwizacji i porównywania audytów zasobów, <input type="checkbox"/> tworzenia kodów kreskowych dla zasobów, <input type="checkbox"/> drukowania kodów kreskowych oraz dwuwymiarowych kodów alfanumerycznych (QR Code) dla zasobów, które posiadają numer inwentarzowy, <input type="checkbox"/> inwentaryzacji zasobów posiadających kody kreskowe za pomocą aplikacji mobilnej dla systemu Android poprzez wyszukiwanie zasobów, skanowanie etykiet, dodawanie i edycję zasobów, dodawanie czynności serwisowych, drukowanie etykiet, <input type="checkbox"/> możliwość zmiany portu komunikacyjnego wykorzystywanego przez aplikację mobilną dla systemu Android, <input type="checkbox"/> inwentaryzacji stacji roboczych niepodłączonych do sieci (bez instalacji Agenta poprzez manualne wykonanie skanów inwentaryzacji offline), <input type="checkbox"/> definiowania alarmów z powiadomieniami e-mail dla dowolnych pól czasowych typu „data” z atrybutów zasobów lub licencji (np. „za 2 tygodnie wygaśnięcie licencji/gwarancja”). <p>Inwentaryzacja oprogramowania zapewnia funkcjonalność w zakresie pozyskiwania informacji o oprogramowaniu i audycie licencji poprzez:</p>
--	---

		<ol style="list-style-type: none"> 1. Skanowanie plików wykonywalnych i multimedialnych na stacjach roboczych, skanowanie archiwów ZIP. 2. Informacje o aplikacjach używanych w organizacji. 3. Tworzenie własnych wzorców aplikacji. 4. Tworzenie dowolnych kategorii aplikacji, np. nowe, zabronione, projektowe itp. 5. Informacje o komputerach, na których aplikacja została wykryta. 6. Zarządzanie posiadanymi licencjami. 7. Wskazywanie osób odpowiedzialnych za licencję. 8. Wskazanie użytkowników licencji. 9. Tworzenia powiązań między licencjami a dokumentami w relacji 1:N. 10. Rozbudowane i konfigurowalne scenariusze zarządzania licencjami poprzez: przypisywanie do użytkownika, przypisywanie do wielu komputerów tego samego użytkownika, przypisywanie wg numerów seryjnych, przypisywanie wg różnych wersji aplikacji na jednym urządzeniu. 11. Łatwy audyt legalności oprogramowania oraz powiadamianie tylko w razie przekroczenia liczby posiadanych licencji - w każdej chwili istnieje możliwość wykonania aktualnych raportów audytowych. 12. Zarządzanie posiadanymi licencjami: raport zgodności licencji. 13. Możliwość przypisania do programów numerów seryjnych, wartości itp. <p>Okna audytowe posiadają możliwość filtrowania elementów per oddział.</p>
9.	Obsługa użytkowników:	<p>Program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez monitorowanie:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), <input type="checkbox"/> Procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika) wraz informacją o uruchomieniu na podwyższonych uprawnieniach, <input type="checkbox"/> Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona) wraz z informacją, na którym komputerze wykonano daną aktywność, <input type="checkbox"/> Informacji o edytowanych przez użytkownika dokumentach, <input type="checkbox"/> Historii pracy (cykliczne zrzuty ekranowe), <input type="checkbox"/> Listy odwiedzanych stron WWW (tytuły, adresy, liczba i czas wizyt), <input type="checkbox"/> Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), <input type="checkbox"/> Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania" drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków, <input type="checkbox"/> Nagłówków przesyłanej w aplikacjach klienckich poczty e-mail. <p>Program ponadto posiada możliwość:</p> <ul style="list-style-type: none"> <input type="checkbox"/> wykrywania podejrzanej aktywności przez popularne „jigglerzy”, mającej na celu symulowanie faktycznej pracy. <input type="checkbox"/> zdefiniowania czasu (min. 15 minut) gdy wykrywana będzie symulowana aktywność wyłącznie przez ruch myszą bez kliknięcia lub wprowadzanie tego samego znaku z klawiatury. <input type="checkbox"/> wyszczególnienia podejrzanej aktywności w raportach. <input type="checkbox"/> wygenerowania alarmu i wykonania akcji po wykryciu podejrzanej aktywności.

		<ul style="list-style-type: none"> <input type="checkbox"/> automatycznego włączenia zapisywania zrzutów ekranowych po wykryciu podejrzanej aktywności. <input type="checkbox"/> blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla stacji roboczej, na której zalogowany jest użytkownik, z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.domena.pl). Reguły w postaci listy domen tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane lub współdzielone pomiędzy grupami lub kontami. <input type="checkbox"/> integracji list stron w formie plików .TXT z dowolnego adresu zewnętrznego np. CERT. <input type="checkbox"/> skorzystania z wbudowanej listy stron sklasyfikowanych jako zagrożenia. <input type="checkbox"/> automatycznego odświeżania list stron zintegrowanych z adresów zewnętrznych. <input type="checkbox"/> blokowania ruchu na wskazanych portach TCP/IP, <input type="checkbox"/> blokowania pobierania poprzez przeglądarki internetowe plików z określonym rozszerzeniem, <input type="checkbox"/> prowadzenia rejestru naruszeń blokad, <input type="checkbox"/> wysyłania powiadomień gdy użytkownik: odwiedzi stronę z określonej grupy domen; pobierze lub wyśle określoną ilość danych w ciągu dnia w sieci lokalnej lub Internet; wydrukuje określoną ilość stron w ciągu dnia, naruszy skonfigurowane blokady, <input type="checkbox"/> przygotowania zestawienia (metryki) ustawień monitorowania użytkownika w postaci raportu (który można dołączyć np. do akt pracownika), <input type="checkbox"/> definiowania godzin lub dni tygodnia, w których monitorowanie użytkowników jest wyłączone. <p>Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. Mechanizm blokowania uruchamiania aplikacji wg maski nazwy oraz lokalizacji pliku. Reguły w postaci listy blokowanych plików lub lokalizacji tworzone są dla użytkownika lub grupy użytkowników i mogą być kopiowane pomiędzy grupami lub kontami.</p> <p>Program posiada Grupy użytkowników oraz Grupy Inteligentne, które służą do lepszego zarządzania użytkownikami, polityką monitorowania oraz blokowania aplikacji i stron internetowych.</p>
10.	Zdalna pomoc:	<p>W ramach kontroli stacji użytkownika dostępny jest podgląd pulpitu użytkownika i możliwość przejęcia nad nim kontroli wraz z możliwością zdefiniowania czy użytkownik powinien zostać zapytany o zgodę na połączenie i opcją odrzucenia takiego połączenia przez użytkownika (np. w przypadku pracowników wysokiego szczebla). Podczas dostępu zdalnego, zarówno użytkownik jak i administrator widzą ten sam ekran. Administrator w trakcie zdalnego dostępu ma możliwość wyboru dowolnego ekranu (monitora) oraz zablokowania działania myszy oraz klawiatury dla użytkownika. Funkcja zdalnego dostępu umożliwia równoczesne podłączenie do tego samego komputera kilku administratorom.</p> <p>W niniejszym module znajduje się baza zgłoszeń umożliwiająca użytkownikom zgłaszanie problemów technicznych poprzez dedykowany portal oraz przetwarzanie wiadomości e-mail, które są przetwarzane i przyporządkowywane odpowiednim administratorom, otrzymującym automatycznie powiadomienie o przypisanym im problemie. Oprogramowanie pozwala na integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0. Moduł umożliwia również przetwarzanie zgłoszeń w trybie anonimowym (wsparcie w realizacji wymogów „Dyrektywy o sygnalistach”) oraz zawiera dokumenty prawne dot. ochrony sygnalistów w tym</p>

	<p>szablon regulaminu zgłoszeń wewnętrznych wymagany przez Dyrektywę. Kolejną ważną funkcjonalnością jest umożliwienie użytkownikom monitorowania procesu rozwiązywania zgłoszonych przez nich problemów i ich aktualnych statusów, jak również możliwość wymiany informacji z administratorem poprzez komentarze, które są wpisywane i widoczne dla obu stron. System umożliwia użycie pośredniego statusu „zgłoszenie rozwiązane” przed ostatecznym zamknięciem zgłoszenia.</p> <p>Moduł ten zawiera również komunikator (czat), który umożliwia prowadzenie rozmów w czasie rzeczywistym oraz archiwizację historii wiadomości pomiędzy zalogowanymi użytkownikami, pracownikami pomocy technicznej i administratorami (wraz z wyszukiwarką rozmów i wiadomości wg słów kluczowych oraz automatycznym oczyszczaniem historii rozmów). Ponadto czat pozwala na:</p> <ul style="list-style-type: none"> <input type="checkbox"/> zarządzanie dostępem do czatu w 3 poziomach uprawnień: pełny dostęp, brak dostępu lub dostęp ograniczony wyłącznie do pomocy technicznej <input type="checkbox"/> rozmowy również między „zwykłymi” użytkownikami <input type="checkbox"/> osadzanie załączników w treści wiadomości, <input type="checkbox"/> osadzanie obrazków w treści wiadomości, <input type="checkbox"/> formatowanie tekstu, <input type="checkbox"/> tworzenie pokoi tematycznych, rozmów grupowych <input type="checkbox"/> oznaczanie kontaktów jako „ulubionych” na liście kontaktów <input type="checkbox"/> uruchomienie z poziomu ikony dostępowej Agenta oraz bezpośrednio w interfejsie WWW heldpesku <input type="checkbox"/> może być wyświetlany w trybie jasnym lub ciemnym <p>W module zawarta jest również baza wiedzy pomagająca użytkownikom samodzielnie rozwiązywać najprostsze, powtarzające się problemy wraz z możliwością nadawania artykułom 1 z 3 statusów (opublikowany, wewnętrzny, szkic). Program umożliwia informowanie pracowników o zdarzeniach, np. planowanych przestojach w dostępie do usług, przez komunikaty z graficznym formatowaniem treści oraz łączami do artykułów w bazie wiedzy. Użytkownik ma możliwość przeglądnięcia historii odczytanych komunikatów bezpośrednio z poziomu ikony Agenta. Administrator ma możliwość tworzenia szkiców i archiwizowania komunikatów.</p> <p>Dostęp do systemu zgłoszeń oraz bazy wiedzy realizowany jest przez dedykowany portal dostępny przez przeglądarkę internetową, który może być wyświetlany w trybie jasnym lub ciemnym. Funkcjonalność modułu umożliwia również uzyskanie dostępu z prywatnego komputera tylko do swojego komputera firmowego, który pozostał w organizacji, za pomocą funkcji zdalnego dostępu przez każdego pracownika.</p> <p>Moduł pomocy zdalnej umożliwia również:</p> <ul style="list-style-type: none"> <input type="checkbox"/> pobieranie listy użytkowników z Active Directory wraz z awatarami, <input type="checkbox"/> wyświetlanie w systemie zgłoszeń wizytówki użytkownika wraz z jego numerem telefonu, adresem e-mail oraz informacją o przełożonym, <input type="checkbox"/> zarządzanie lokalnymi kontami Windows w zakresie: tworzenia, usuwania, aktywacji, edycji uprawnień, resetu hasła, edycji kont, <input type="checkbox"/> zarządzanie dostępem pracowników HelpDesku do zgłoszeń poprzez rozbudowany system zarządzania regułami widoczności zgłoszeń, <input type="checkbox"/> zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii zgłoszeń, <input type="checkbox"/> zarządzanie dostępem zwykłych użytkowników końcowych do wybranych kategorii artykułów bazy wiedzy, <input type="checkbox"/> tworzenie własnego drzewa kategorii zgłoszeń wraz z możliwością grupowania kategorii w folderach (do 4 poziomów kategorii), opisami kategorii oraz klauzulą RODO,
--	---

		<input type="checkbox"/> automatyczne przypisywanie konkretnych pracowników helpdesk do zgłoszeń w określonych kategoriach lub pochodzących od określonych grup użytkowników, <input type="checkbox"/> definiowanie ścieżek akceptacji zgłoszeń – procesu, w którym użytkownik uzyskuje akceptację na realizację zgłoszenia od wyznaczonych osób w organizacji, <input type="checkbox"/> przypisywanie ścieżek akceptacji zgłoszeń do określonych kategorii, <input type="checkbox"/> procesowanie zgłoszeń użytkowników z wiadomości e-mail, <input type="checkbox"/> dostęp do plików źródłowych wiadomości e-mail przetworzonych na zgłoszenia, <input type="checkbox"/> obsługę wielu adresów e-mail jednego użytkownika w celu przetwarzania jako zgłoszeń pochodzących od tej samej osoby, <input type="checkbox"/> eksportowania listy zgłoszeń do plików CSV i XLSX, <input type="checkbox"/> integrację ze wieloma skrzynkami e-mail w celu obsługi różnych kanałów zgłoszeń wraz z automatyzacjami, <input type="checkbox"/> integrację ze skrzynkami e-mail w oparciu o klasyczną autoryzację login/hasło oraz mechanizm OAuth 2.0, <input type="checkbox"/> tworzenie formularzy z niestandardowymi polami opisowymi, dedykowanymi do wybranych kategorii zgłoszeń, <input type="checkbox"/> wykonywanie operacji na wielu zgłoszeniach równocześnie, <input type="checkbox"/> dołączanie załączników do zgłoszeń, <input type="checkbox"/> usuwanie zamkniętych zgłoszeń, <input type="checkbox"/> rozbudowane wyszukiwanie zgłoszeń i artykułów w bazie wiedzy, <input type="checkbox"/> szybki dostęp do ostatnich zgłoszeń, artykułów bazy wiedzy i załączników, <input type="checkbox"/> wprowadzenie komentarza oraz informacji o czasie poświęconym na rozwiązanie w kreatorze wyświetlanym przy zamykaniu zgłoszenia, <input type="checkbox"/> zrzuty ekranowe (podgląd pulpitu), <input type="checkbox"/> zdalną modyfikację rejestrów, <input type="checkbox"/> dystrybucję oprogramowania przez Agenty, <input type="checkbox"/> definiowanie aplikacji dozwolonych do samodzielnej instalacji przez użytkowników z pakietów MSI w postaci Kiosku z Aplikacjami, <input type="checkbox"/> przypisywanie dostępnych w Kiosku instalatorów do grup użytkowników, <input type="checkbox"/> dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), <input type="checkbox"/> zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecenia operacji następuje kolejkowanie zadania dystrybucji pliku, <input type="checkbox"/> możliwość skonfigurowania automatyzacji procesowania zgłoszeń wraz z powiadomieniami e-mail wysyłanymi do określonych aktorów w zgłoszeniu, <input type="checkbox"/> możliwość skonfigurowania automatyzacji dodających komentarze publiczne wraz z załącznikami i odnośnikami do artykułów w Bazie Wiedzy, <input type="checkbox"/> planowanie nieobecności pracowników helpdesk, <input type="checkbox"/> obsługę umów o gwarantowanym poziomie świadczenia usług (SLA) wraz z raportami np. przekroczeń SLA wraz z podsumowaniem, <input type="checkbox"/> generowanie raportów obsługi helpdesk, <input type="checkbox"/> zdalne wykonywanie poleceń poprzez Agenty (np. utworzenie / edycja konta lokalnego użytkownika systemu), <input type="checkbox"/> zarządzania procesami systemu Windows (w zakresie: zakończ proces, zakończ drzewo procesu, uruchom nowy proces w sesji użytkownika wraz z parametrami), <input type="checkbox"/> wymiany plików do i ze stacji roboczej poprzez funkcję Menedżera plików bez blokowania interfejsu programu podczas przesyłania plików.
11.	Ochrona danych przed wyciekiem:	1. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może

		<p>skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny.</p> <p>2. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek.</p> <p>3. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA.</p> <p>4. Blokowanie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane.</p> <p>5. Alarmowanie o zdarzeniach podłączenia/odłączenia urządzeń zewnętrznych wraz z możliwością ograniczenia alarmów tylko do nośników niezauważalnych.</p> <p>6. Funkcje wspierające bezpieczeństwo systemu: integracja i zarządzanie ustawieniami Windows Defender.</p> <p>7. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu szyfrowania dysków BitLocker.</p> <p>8. Funkcje wspierające bezpieczeństwo systemu: zdalne szyfrowanie dysków za pomocą BitLocker.</p> <p>9. Funkcje wspierające bezpieczeństwo systemu: zapisywanie klucza odzyskiwania do pliku oraz jako zasób w bazie danych programu.</p> <p>10. Funkcje wspierające bezpieczeństwo systemu: integracja z Windows Defender w zakresie odczytu stanu ochrony, włączenia i wyłączenia ochrony, tworzenia reguł ruchu.</p> <p>11. Funkcje wspierające bezpieczeństwo systemu: odczytanie informacji o aktywnym oprogramowaniu antywirusowym firm trzecich, innym niż Windows Defender.</p> <p>12. Funkcje wspierające bezpieczeństwo systemu: monitorowanie stanu modułu TPM.</p> <p>Zarządzanie prawami dostępu do urządzeń:</p> <p>1. Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików.</p> <p>2. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane.</p> <p>3. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników.</p> <p>4. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci.</p> <p>5. Możliwość usuwania z listy znanych urządzeń tych nośników, które np. zostały zutylizowane.</p> <p>Audyt operacji na plikach na urządzeniach przenośnych:</p> <p>1. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych.</p> <p>2. Podłączenie/odłączenie urządzenia przenośnego.</p> <p>Monitorowanie operacji na plikach w lokalnych folderach komputera użytkownika.</p> <p>Definiowanie reguł monitorowanych folderów w postaci list.</p> <p>Monitorowanie operacji na plikach na udostępnionych zasobach sieciowych (udziałach) na urządzeniach nieobsługiwanych przez Agent (np. macierze, NAS itp.)</p> <p>Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. Przydzielanie uprawnień również do kont użytkowników lokalnych.</p> <p>Program umożliwia prowadzenie rejestru naruszeń blokad podłączanych nośników.</p>
12.	Zarządzanie czasem, aktywność użytkowników:	<p>Program WSPIERA ZARZĄDZANIE CZASEM I ANALIZOWANIE AKTYWNOŚCI UŻYTKOWNIKÓW poprzez dostarczenie informacji o czasie poświęconym na pracę w poszczególnych aplikacjach i na stronach WWW z dowolnie wybranego okresu. Każdy pracownik organizacji może oznaczyć sesję</p>

		<p>aktywności jako czas prywatny gdy wykonuje czynności prywatne na sprzęcie firmowym. Może również uzyskać dostęp do własnych wskaźników aktywności w czasie pracy. Menedżerowie oraz przełożeni mogą uzyskać automatyczny dostęp do aktywności podwładnych w zespołach i indywidualnie oraz mogą przeanalizować aktywności w danym okresie i zyskać pełny obraz obszarów wymagających największego zaangażowania. Pracownik może przeglądać swoje historyczne dane, wybierając okres aktywności, który go interesuje. Zastosowane reguły pozwalają zidentyfikować różnego rodzaju rozpraszacze i nieefektywne działania. Dostęp realizowany jest przez przeglądarkę internetową a strona może być wyświetlana w trybie jasnym lub ciemnym.</p> <ol style="list-style-type: none"> 1. Statystyki czasu pracy i osobistej aktywności w wybranym przedziale czasu. 2. Statystyki aktywności grupy i jej członków widoczne dla menedżera grupy. 3. Statystyki aktywności podwładnych widoczne dla przełożonego. 4. Lista odwiedzanych stron internetowych i aplikacji wraz ze spędzonym na nich czasem. 5. Podgląd listy użytkowników korzystających z wybranej aplikacji we wskazanym zakresie czasu. 6. Statystyki popularności stron i aplikacji w organizacji, grupie i u poszczególnych użytkowników. 7. Ocena produktywności użytkownika na podstawie czasu spędzonego w aplikacjach i na stronach internetowych. 8. Grupowanie stron internetowych i aplikacji z podziałem na: produktywne, neutralne i nieproduktywne. 9. Możliwość przypisywania wyjątków produktywności dla określonych grup użytkowników w przypadku aplikacji globalnie sklasyfikowanych jako nieproduktywne co pozwala na sklasyfikowanie aktywności użytkowników będących członkami takiej grupy jako produktywnej przy ocenie ich pracy. 10. Jednoczesna edycja klasyfikacji aplikacji pod kątem oceny produktywności oraz przeznaczenia (kategoryzowanie). 11. Wskaźnik czasu poświęconego na aktywność produktywną. 12. Definiowanie wymaganego progu produktywności i limitu nieproduktywności, możliwość włączenia dla nich alarmów e-mail. 13. Przypisywanie kategorii aplikacjom i stronom internetowym, np. Biuro, Produkcja, Rozrywka - predefiniowana lista kategorii z możliwością edycji. 14. Lista kontaktów w organizacji z wbudowaną wyszukiwarką dostępna dla każdego pracownika w organizacji z możliwością ukrycia wybranych kontaktów.
13.	Portal informacyjny:	<p>Oprogramowanie posiada również obszar funkcjonalny w formie platformy WWW, który pozwala na tworzenie wielu interaktywnych paneli informacyjnych (dashboardów) z responsywnymi widgetami, których nazwy można zmieniać wg potrzeb. Na każdym z dashboardów widgety są rozłożone na siatce o rozmiarze ustalonym przez administratora. Zawartość każdego z paneli informacyjnych jest automatycznie odświeżana oraz może być:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Udostępniana w trybie „tylko do odczytu” z zabezpieczeniem tokenem. <input type="checkbox"/> Wyświetlana w trybie jasnym lub ciemnym (nocnym). <p>Oprogramowanie umożliwia zarządzanie uprawnieniami administratorów do funkcjonalności portalu informacyjnego.</p> <p>Widgety prezentują dane ze wszystkich modułów funkcjonalnych oprogramowania:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Mapa sieci, <input type="checkbox"/> Liczniki wydajności, Alarmy (wraz z filtrowaniem) oraz odpowiedzi serwisów TCP/IP, Ostatnie urządzenia w sieci, <input type="checkbox"/> Zmiany w konfiguracji sprzętowej urządzeń z Agentami, Zmiany w konfiguracji aplikacyjnej urządzeń z Agentami, Alarmy dla Zasobów, <input type="checkbox"/> Statystyki z obszaru wydruków, Statystyki użycia aplikacji, Użycie łącza,

		Aktywność WWW, naruszenia reguł blokad, <input type="checkbox"/> Statystyki z obsługi zgłoszeń, Lista najnowszych nierozwiązanych zgłoszeń, Lista najstarszych nierozwiązanych zgłoszeń, Zgłoszenia z naruszonym SLA, Zgłoszenia, których SLA wkrótce wygaśnie, <input type="checkbox"/> Ostatnio podłączone nośniki zewnętrzne, Ostatnie operacje na plikach (wraz z filtrowaniem), informacje o stanie Bitlocker, Windows Defender, Windows Firewall, naruszenia reguł dostępu do nośników danych, <input type="checkbox"/> Produktywność dla grupy, Statystyki czasu nieproduktywnego.
14.	Ochrona przed usunięciem:	Program zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora stacji roboczej, na której pracuje.
15.	Funkcjonalność Agent:	Możliwość automatycznego wyszukiwania serwera przez oprogramowanie monitorujące stacje robocze.
16.	Interfejs:	Program dostępny z interfejsem w języku polskim lub angielskim.

12. System NAC (kontrola dostępu do sieci) – zapewnienie bezpieczeństwa sieci poprzez segmentację, autoryzację urządzeń i użytkowników, ochrona przed nieautoryzowanym dostępem

Zamawiający wymaga dostarczenia licencji nieograniczonej czasowo (bezterminowej), z minimalnym czasem wsparcia na okres 3 lat.

Wymagania minimalne:

1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multivendor)
3. System musi być w pełni zarządzany z poziomu interfejsu graficznego dostępnego przez przeglądarkę internetową z jednej konsoli, interfejs WEB w wersji HTML5 niewymagających obsługi dodatkowych wtyczek.
4. System musi wspierać funkcjonalność instalacji rozproszonej na wielu maszynach (serwerach) fizycznych lub wirtualnych w ramach jednej licencji
5. System musi wspierać mechanizm DISASTER RECOVERY – tworzenia kopii lustrzanej całego systemu w celu zachowania ciągłości działania w ramach jednej licencji.
6. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych stacji końcowych.
7. System musi umożliwiać obsługę co najmniej 250 jednoczesnych unikatowych autoryzacji do sieci w ciągu dnia (w tym gości) oraz zapewniać skalowalność do przynajmniej 1 000 jednoczesnych unikatowych autoryzacji do sieci poprzez rozbudowę oferowanego rozwiązania.
8. Licencja ma być zwalniana po rozłączeniu urządzenia końcowego.
9. System musi umożliwiać obsługę jednocześnie podłączonych agentów oraz BYOD (BringYourOwn Device) co najmniej tyle samo co licencja na jednoczesne unikatowe autoryzacje do sieci w ciągu dnia.
10. System musi umożliwiać instalację na maszynie wirtualnej (VM), PaaS lub maszynie fizycznej, w tym:
 - VM – min. VMWare ESXi co najmniej w wersji 5.x, Hyper-V w wersji min 2012, Proxmox w wersji min 5.x, KVM w wersji min 7.x, CitrixXenServer w wersji min 4.x
 - Maszyny fizyczne - serwery wspierane przez producenta.

11. System musi posiadać funkcjonalność serwerów:
 - serwera RADIUS dla infrastruktury sieciowej,
 - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
 - serwera SYSLOG,
 - serwera TACACS+,
 - serwera Monitoringu,
 - serwera DHCP,
 - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
 - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostęp do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
15. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznymi systemami (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC), CheckPoint, Service Now.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługi wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.

26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP, Tacacs+.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.

50. Captive Portal powinien umożliwiać konfigurację maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu urządzenia, systemu operacyjnego, przez co najmniej DHCP Fingerprinting, DHCP SPAN, SNMP, Vendor OUI, TCP, Active Directory, CDP/LLDP, HTTP/S, DNS, Radius, WMI, MDM, WinRM, ONVIF.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minimum na systemach: FortiGate, PulseSecure, OpenVPN, PaloAlto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
 - Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
 - Czy włączony jest firewall
 - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
 - Czy jest włączone szyfrowanie dysku systemowego
 - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
 - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
 - Czy w systemie są uruchomione procesy wskazane przez administratora
 - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
 - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
 - Wartości klucza rejestru
 - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratorzy sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działu IT dla systemów co najmniej:
 - Microsoft Windows
 - Mac OS
 - iOS

- Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfigurator sieci).
 64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
 - MAC,
 - PAP/ASCII,
 - CHAP,
 - SNMP,
 - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
 - Tożsamość/Urządzenie końcowe,
 - Grupa tożsamości/urządzeń końcowych,
 - Parametry urządzeń końcowych, min: system operacyjny, wersja,
 - Atrybuty Active Directory,
 - Jednostka organizacyjna tożsamości/urządzeń końcowych,
 - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
 - Grupy urządzeń sieciowych,
 - Porty urządzeń sieciowych,
 - Grupy portów urządzeń sieciowych,
 - Jednostka organizacyjna portów,
 - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
 - Data, czas ważności polityki,
 - Wewnętrzny Captive Portal,
 - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MikroTik, Ubiquiti Networks.
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.
19. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
20. System musi umożliwiać przysyłanie zwrotnych parametrów do systemów zewnętrznych i/lub urządzeń sieciowych za pomocą protokołu min. HTTP zawierających min. informacje o identyfikatorze tożsamości, adresie MAC oraz IP.

Obsługa serwerów certyfikatów CA

1. System musi posiadać funkcjonalność zintegrowanego serwera certyfikacji CA (Certificate Authority) oraz zapewniać współpracę z zewnętrznymi serwerami CA.
2. Funkcja CA zintegrowana oraz zewnętrzna musi zapewniać przynajmniej następujące funkcjonalności:
 - możliwość generowania i podpisywania certyfikatów dla tożsamości i urządzeń końcowych.
 - możliwość bezpiecznego przechowywania certyfikatów tożsamości i urządzeń końcowych.
 - Możliwość generowanie certyfikatów za pomocą protokołu SCEP (Simple Certificate Enrollment Protocol).
 - usługę OCSP (Online Certificate Status Protocol).

Obsługa serwerów DHCP

1. System musi posiadać funkcję zintegrowanego serwera DHCP.
2. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu urządzenia końcowego, adresu MAC podczas pracy serwera DHCP.
3. System musi zapewniać przynajmniej następujące funkcjonalności serwera DHCP:
 - Uruchamianie usługi dla wybranych podsieci,
 - Przypisanie ustalonego adresu IP dla adresu MAC.

- Przypisanie różnych adresów IP dla konkretnego adresu MAC z różnych podsieci,
- Możliwość zwracania adresów IP wyłącznie dla wybranej i wcześniej zdefiniowanej grupy adresów MAC,
- Możliwość określania braku dostępu dla wybranych adresów MAC,
- Monitoring obciążenia puli dynamicznych, poziomu decline, braku konfiguracji, ograniczenia dla zdefiniowanej grupy adresów MAC,
- Możliwość ustawienia dodatkowych parametrów zwrotnych przesyłanych przez serwer DHCP,
- Możliwość podglądu aktualnego obciążenia podsieci w widoku graficznym adresacji IP dla przydziału statycznego i dynamicznego,
- Możliwość zmiany przydziału dynamicznego na statyczny bez restartu usługi,
- Dokonywanie zmian bez konieczności wyłączania usług.

Obsługa serwerów TACACS+

System musi umożliwiać tworzenie grup uprawnień do kontroli dostępu urządzeń sieciowych:

1. System musi umożliwiać grupowanie urządzeń końcowych oraz administratorów.
2. System musi umożliwiać tworzenia haseł administratorom.
3. System musi umożliwiać tworzenie listy komend uprawnień dla administratorów
4. System musi raportować o wszystkich wydanych komendach na kontrolowanych urządzeniach sieciowych.
5. System musi umożliwiać zmianę hasła administratora z poziomu urządzenia sieciowego wg ustalonego czasu.
6. System musi umożliwiać logowanie za pomocą poświadczeń Microsoft Active Directory.
7. System musi wspierać logowanie administratorów za pomocą tokenów OTP.
8. System musi umożliwiać przypisywanie atrybutów zwrotnych VSA podczas etapu autoryzacji.

Raportowanie i monitoring

System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

1. Monitoring autoryzacji.
2. Monitoring dla zdarzeń systemowych.
3. Monitoring dla zdarzeń DHCP.
4. Monitoring dla tożsamości.
5. Monitoring dla urządzeń końcowych.
6. Monitoring dla urządzeń sieciowych.
7. Raport stanu systemu (min. szczegółowy dane z nodów systemu, wykorzystanie polityk dostępu, ostatnie krytyczne błędy, niski status komponentów drukarek, ostanie aktywności serwerów autoryzacji, DHCP, urządzeń sieciowych uwzględniający ostatnią aktywność autoryzacji, obciążenie procesora, pamięci, zmiany konfiguracji, obciążenie serwera DHCP, autoryzacji, obciążenia portów – przepustowość, liczby autoryzacji) dostępny min. z poziomu konsoli CLI, interfejsu WWW oraz raportu email.
8. Raport ze zdarzeń logowania z informacją o nadanym adresie IP.
9. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.
10. Raport z logów DHCP z informacją o polityce dostępu logowania do sieci.

11. System musi posiadać mechanizm graficznego podglądu stanu przełącznika i portów w czasie rzeczywistym.
12. System musi wspierać mechanizm graficznego podglądu urządzeń sieciowych działających w stosie.
13. System musi wspierać mechanizm graficznego podglądu wykrytych niezgodności vlanów w urządzeniach sieciowych działających w środowisku.
14. System musi wspierać funkcjonalność graficznego monitoringu zasobów zarządzanych drukarek sieciowych.
15. System musi posiadać mechanizm graficznego podglądu stanu tożsamości oraz urządzeń końcowych w tym podstawowe dane, ostatnia autoryzacja do sieci, wykorzystanie urządzeń końcowych wg tożsamości na dzień, parametry urządzeń końcowych, min: system operacyjny, wersja.
16. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.
17. Raport z logów OTP z informacją o poprawnej i błędnej autoryzacji, wysłanego tokenu przez bramkę SMS.
18. Raport zdarzeń Microsoft Active Directory, minimum:
 - Logowania, wylogowania z system w tym błędne logowania
 - Logowania do sieci 802.1X

Alarmy

1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:
 - wiadomości e-mail,
 - Syslog,
 - notyfikacji systemowych.
2. Alarmy mogą być generowane w sytuacjach, min:
 - Ilości obsługiwanych transakcji RADIUS,
 - Opóźnienie obsługi transakcji RADIUS,
 - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
 - badanie łączności IP za pomocą ping, traceroute,
 - tcpdump protokołów RADIUS, TACACS+,
 - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
 - nazwy użytkownika,
 - adresu MAC,
 - statusu uwierzytelnienia (udana lub nieudana),
 - powodu, jeżeli uwierzytelnienie nieudane,
 - zakresu czasowego, co do dnia, godziny i minuty,
 - wykonanie zdalnego polecenia na urządzeniu sieciowym.

13. Oprogramowanie do monitoringu infrastruktury

Zamawiający wymaga dostarczenia i wdrożenia centralnego systemu monitoringu infrastruktury IT, umożliwiającego bieżący nadzór nad dostępnością oraz podstawowymi parametrami pracy zasobów informatycznych. System monitoringu musi zostać dostarczony wraz z licencją umożliwiającą

monitorowanie do 3000 usług (serwisów) w rozumieniu elementów monitorowanych przez system (np. usługi, zasoby, parametry).

Wymagane funkcjonalności:

1. Monitoring dostępności urządzeń

- Serwerów
- Urządzeń sieciowych
- Innych wskazanych zasobów IT

2. Monitoring podstawowych parametrów pracy

- obciążenia procesora
- wykorzystania pamięci operacyjnej
- dostępnej przestrzeni dyskowej

3. Zbieranie danych monitorujących

- z wykorzystaniem agenta instalowanego na monitorowanych systemach
- poprzez standardowe protokoły monitoringu sieciowego

4. Centralny interfejs zarządzania

- dostęp do systemu poprzez przeglądarkę internetową
- prezentacja aktualnego stanu monitorowanych zasobów

5. Powiadomienia o zdarzeniach

- sygnalizowanie przekroczenia zdefiniowanych progów lub braku dostępności
- możliwość wysyłania powiadomień co najmniej za pomocą poczty elektronicznej

6. Historia Zdarzeń

- rejestrowanie zmian stanu monitorowanych zasobów
- możliwość przeglądu zdarzeń historycznych

7. Wymagania ogólne

- System powinien pracować w trybie ciągłym (24/7)
- Rozwiązanie powinno umożliwiać rozbudowę o kolejne monitorowane zasoby
- Wykonawca zapewni podstawową konfigurację systemu oraz uruchomienie monitoringu wskazanych elementów infrastruktury

8. Licencja

- System monitoringu musi zostać dostarczony wraz z licencją umożliwiającą monitorowanie do 3000 usług (serwisów) w rozumieniu elementów monitorowanych przez system.
- Licencja systemu monitoringu musi obowiązywać przez okres 36 miesięcy od dnia uruchomienia systemu.

14. Oprogramowanie do przechowywania logów z urządzeń sieciowo/serwerowych

1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:
 - a. System operacyjny powinien być na licencji Open Source.
 - b. Platformą sprzętową dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego fizyczny serwer będący na wyposażeniu Zamawiającego
 - c. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source
 - d. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 2TB.

- e. Tworzenie użytkowników w systemie centralnego składowania logów może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
 - f. 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.
 - g. 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.
 - h. System centralnego składowania dzienników zdarzeń powinien udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.
 - i. 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.
 - j. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
2. W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:
- a. Instalacja systemu operacyjnego na wybranym przez Zamawiającego serwerze fizycznym.
 - b. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca proponuje rozwiązanie pozwalające na uspoźnienie zegarów czasów sieci Zamawiającego.
 - c. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
 - d. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktywnych prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
 - e. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu.
 - f. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
 - g. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
 - h. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.
 - i. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.

- j. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
 - k. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.
3. Gwarancja i asysta techniczne:
- a. Zamawiający wymaga aby Wykonawca w czasie do 24 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
 - b. Zamawiający wymaga aby Wykonawca w okresie do 24 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
 - c. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
 - d. 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.

15. Komputery dla administracji i obsługi środowiska wirtualnego – stacje robocze dla personelu odpowiedzialnego za zarządzanie i utrzymanie infrastruktury IT szpitala, UPS do komputera (20szt.)

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiającą jednoznaczną identyfikację oferowanej konfiguracji.
2.	Obudowa	Typu Small Form Factor, umożliwiającą montaż minimum dwóch dysków SSD oraz jednego dysku HDD 3,5". Obudowa trwale oznaczona nazwą producenta i modelem komputera.
3.	Chipset	Dostosowany do zaoferowanego procesora
4.	Płyta główna	Zaprojektowana i wyprodukowana przez producenta komputera, trwale oznaczona nazwą producenta komputera (na etapie produkcji). Płyta główna wyposażona w: <ul style="list-style-type: none"> - 3 sloty M.2 - 4 sloty DIMM na pamięć RAM - 1 slot PCIe min. 4.0 x16 o niskim profilu - 1 slot PCIe min. 3.0 x1 o niskim profilu - 2 sloty SATA

5.	Procesor	Procesor klasy x86, zaprojektowany do pracy w komputerach stacjonarnych o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core Ultra 5 225 na podstawie PerformanceTest w teście CPU Mark według wyników Average CPU Mark opublikowanych na stronie http://www.cpubenchmark.net . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
6.	Pamięć operacyjna	Fabrycznie zainstalowane min. 32GB DDR5 5600MHz w trybie dual channel Możliwość rozbudowy pamięci do min. 128 GB. Min. 2 sloty wolne.
7.	Dysk twardy	Min. 512GB SSD PCIeNVMe Opal, zawierający partycję RECOVERY umożliwiającą odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość rozbudowy jednostki komputerowej o 2 dodatkowe dyski twarde.
8.	Karta graficzna	Zintegrowana z procesorem
9.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowany głośnik multimedialny o mocy 1W.
10.	Sieć	Karta sieciowa LAN obsługująca prędkości 10/100/1000 i WoL Karta sieciowa WLAN w standardzie BE oraz Bluetooth min. 5.4
11.	Porty/złącza	<p>Z przodu obudowy:</p> <ul style="list-style-type: none"> - 1x USB 3.2 typu C z możliwością ładowania podłączonych urządzeń - 4x USB 3.2 typu A - złącze audio combo <p>Z tyłu obudowy:</p> <ul style="list-style-type: none"> - 4x USB 3.2 typu A - 1x HDMI 2.1 - 2x DisplayPort 1.4a - 1x RJ-45 - 1x line-out <p>Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów nie może być osiągnięta w wyniku stosowania konwerterów i przejściówek.</p>
12.	Klawiatura/mysz	Przewodowe USB: klawiatura w układzie US + mysz z rolką

13.	Zasilacz	Energooszczędny zasilacz o mocy max. 200W oraz sprawności na poziomie min. 90%.
14.	System operacyjny	<p>System operacyjny klasy PC musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:</p> <ol style="list-style-type: none"> Dostępne dwa rodzaje graficznego interfejsu użytkownika: <ol style="list-style-type: none"> Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, Dotykowy umożliwiający sterowanie dotykkiem na urządzeniach typu tablet lub monitorach dotykowych Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modulem „uczenia się” pisma użytkownika – obsługa języka polskiego Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim Możliwość tworzenia pulpitu wirtualnych, przenoszenia aplikacji pomiędzy pulpitem i przełączanie się pomiędzy pulpitem za pomocą skrótów klawiaturowych lub GUI. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim Wbudowany system pomocy w języku polskim. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont

		<p>użytkowników.</p> <p>15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze.</p> <p>16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk".</p> <p>17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy.</p> <p>18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązywania problemu z komputerem.</p> <p>19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.</p> <p>20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.</p> <p>21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci.</p> <p>22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika.</p> <p>23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)."</p> <p>24. Wbudowany mechanizm wirtualizacji typu hypervisor."</p> <p>25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego.</p> <p>26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego.</p> <p>27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.</p> <p>28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).</p> <p>29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokiowanie</p>
--	--	--

		<p>bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niez zarządzanymi.</p> <p>30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne.</p> <p>31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami.</p> <p>32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM</p> <p>33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych.</p> <p>34. Możliwość tworzenia wirtualnych kart inteligentnych.</p> <p>35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (SecureBoot)</p> <p>36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.</p> <p>37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.</p> <p>38. Mechanizmy logowania w oparciu o:</p> <ul style="list-style-type: none"> a. Login i hasło, b. Karty inteligentne i certyfikaty (smartcard), c. Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d. Certyfikat/Klucz i PIN e. Certyfikat/Klucz i uwierzytelnienie biometryczne <p>39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5</p> <p>40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej.</p> <p>41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach</p> <p>42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń</p> <p>43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń</p>
15.	BIOS	<p>BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego</p>

		<p>oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:</p> <ul style="list-style-type: none"> - modelu komputera, - numerze seryjnym, - wersji BIOS, - zainstalowanym procesorze wraz z taktowaniem, - zainstalowanej pamięci RAM wraz z taktowaniem, - adresie MAC karty sieciowej. <p>Administrator z poziomu BIOS musi mieć możliwość:</p> <ul style="list-style-type: none"> - wyłączenia portów USB - wyłączenia karty sieciowej - wyłączenia karty audio - wyłączenia funkcji Wake on LAN - wyłączenia wirtualizacji - ustawienia hasła: administratora, Power-On, dysku twardego - zdefiniowania sekwencji bootowania - załadowania optymalnych ustawień BIOS <p>bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych</p>
16.	System Diagnostyczny	<p>Zaimplementowany w UEFI BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednocześnie przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System obsługiwany za pomocą myszy lub klawiatury, umożliwiający wykonanie minimum następujących czynności diagnostycznych:</p> <p>1. Wykonanie testu komponentów w zakresie przyspieszonym lub rozszerzonym z możliwością wyboru algorytmów testowania oraz liczby cykli testowych do przeprowadzenia. System diagnostyczny powinien umożliwiać wykonanie testu następujących komponentów:</p>

		<ul style="list-style-type: none"> - pamięci ram, - procesora, - pamięci masowej, - płyty głównej <p>2. Identyfikację jednostki i jej komponentów w następującym zakresie:</p> <ul style="list-style-type: none"> - urządzenie (producent, model, numer seryjny), - bios (wersja oraz data wydania), - procesor (nazwa, taktowanie, ilości pamięci L1, L2, L3, liczba rdzeni), - pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny), - dysk twardy (producent, model, numer seryjny, pojemność), - płyta główna (liczba złączy USB, liczba złączy PCI)
17.	Bezpieczeństwo	<ul style="list-style-type: none"> - Złącze typu Kensington Lock - Oczko na kłódkę, zabezpieczającą urządzenie przed nieautoryzowanym otwarciem - Sprzętowy moduł TPM 2.0 (dTPM 2.0) z certyfikacją TCG - Czujnik otwarcia obudowy
18.	Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów, pamięci i urządzeń I/O realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
19.	Oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikację i instalację sterowników oraz oprogramowania użytkowego producenta, w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralną bazą sterowników i oprogramowania użytkowego producenta, sprawdzać dostępne aktualizacje i zapewniać ich zbiorczą instalację.
20.	Gwarancja i wsparcie techniczne producenta	<p>Min. 36 miesięcy świadczona w miejscu użytkowania sprzętu (on-site). W razie awarii dysku twardego pozostaje on własnością Zamawiającego. Firma serwisująca posiadająca certyfikat ISO 9001:2000 na świadczenie usług serwisowych. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.</p> <p>Dedykowany portal techniczny producenta komputera, wyposażony w funkcję automatycznej identyfikacji urządzenia, umożliwiający Zamawiającemu uzyskanie informacji w zakresie co najmniej:</p>

		- fabrycznej konfiguracji urządzenia, - rodzaju gwarancji, - dacie wygaśnięcia gwarancji, - aktualizacjach. Zaawansowana diagnostyka urządzenia i oprogramowania dostępna na stronie producenta komputera.
--	--	--

Monitor komputerowy

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne monitorów
1.	Monitor	Monitor będzie wykorzystywany dla potrzeb aplikacji biurowych, obróbki zdjęć lub wideo. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację monitora
2.	Wielkość ekranu	Przekątna ekranu min. 23,8"
3.	Matryca	Powłoka matrycy o wykończeniu matowym typu IPS
4.	Nominalna rozdzielczość	Rozdzielczość nie mniejsza niż: FHD (1920x1080)
5.	Kąty widzenia	Kąty widzenia min. 178 stopni w pionie i w poziomie
6.	Plamka	Wielkość plamki (pojedynczego piksela) nie większa niż 0.275mm
7.	Częstotliwość odświeżania	Nie mniejsza niż 100Hz
8.	Jasność	Nie mniejsza niż 250 nitów
9.	Czas reakcji matrycy	Nie większy niż 6ms
10.	Zakres kolorów	Nie mniejszy niż 99% sRGB Obsługa min. 16,7 miliona kolorów
11.	Kontrast statyczny	Nie mniejszy niż: 1300:1
12.	Porty/złącza	– 1x HDMI – 1x DisplayPort – 1x VGA

13.	Waga	Nieprzekraczająca 5 kg z podstawą według karty katalogowej producenta
14.	Ergonomia	Możliwość regulacji ustawienia monitora w zakresie: <ul style="list-style-type: none"> – Przód / tył w zakresie min. -5 do 21 stopni – Lewo / prawo w zakresie 360 stopni – Pivot w zakresie min. -90 do 90 stopni – Wysokość do min. 150mm
15.	Obudowa	<ul style="list-style-type: none"> – Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej – Możliwość zainstalowania monitora na ścianie przy wykorzystaniu ściennego systemu montażowego VESA (100x100) – Wbudowane głośniki min. 2x 2W
16.	Bezpieczeństwo	Złącze typu Kensington Lock
17.	Ukompletowanie	Kabel HDMI o długości min. 1,8m Kabel zasilający o długości min. 1,8m
18.	Gwarancja i wsparcie	Minimum 36 miesięcy

UPS do komputera

Parametr	Wymagania minimalne
Moc pozorna	minimum 2000VA
Moc rzeczywista	minimum 1200W
Technologia	minimum line-interactive
Typ obudowy	tower
Wejście	
Napięcie wejściowe	minimum 220/230/240 VAC
Zakres napięcia wejściowego	minimum 140-300 VAC
Częstotliwość	minimum 50/60 Hz (auto wykrywanie)
Wyjście	
Regulacja napięcia	minimum +/- 10 %
Kształt napięcia wyjściowego	minimum symulowana sinusoida
Typowy czas przełączania	2-6 ms
Baterie	
Baterie wewnętrzne w UPS	minimum 2x 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania (dla 50% Pmax)	minimum 5 minut
Pozostałe	
Wejście zasilania	kabel zamontowany na stałe w obudowie UPS zakończony wtykiem PL/FR
Ilość i typ gniazd wyjściowych	minimum 4 gniazda Schuko (z podtrzymaniem)

Stabilizacja napięcia AVR Boost & Buck	wymagana
Filtr RJ45	wymagany
Ładowanie w trybie wyłączenia	wymagane
Funkcja autorestartu po powrocie zasilania	wymagana
Funkcja zimnego startu	wymagana
Sygnalizacja	Dźwiękowa, Wyświetlacz LCD
Alarmy dźwiękowe	minimum Tryb baterijny, Rozładowana bateria, Przeciążenie, Awaria
Informacje wyświetlane na panelu LCD	minimum napięcie wejściowe i wyjściowe, poziom obciążenia, poziom naładowania baterii, praca z sieci/baterii, przeciążenie, niski poziom baterii
Alarmy dźwiękowe	minimum Tryb baterijny, Rozładowana bateria, Przeciążenie, Awaria
Interfejs komunikacyjny	USB
Zabezpieczenia	Minimum ochrona przed zwarcie, przeciążeniem, rozładowaniem
Gwarancja	minimum 24 miesiące na elektronikę i 12 miesięcy na akumulatory;
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.
	naprawa w maksymalnie 14 dni roboczych
	serwis realizowany w systemie door to door
Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS
	wsparcie dla systemów: Windows, Linux
	wymagane wsparcie producenta w języku polskim (telefoniczne oraz mailowe)

16. Szkolenia w zakresie dostarczonego sprzętu oraz technologii

Zamawiający wymaga przeprowadzenia szeregu specjalistycznych szkoleń z zakresu bezpieczeństwa sieciowego, dedykowanych dla personelu IT odpowiedzialnego za administrowanie infrastrukturą sieciową i systemami ochrony zasobów informatycznych. Forma szkolenia : on-line bądź stacjonarnie. Wszystkie szkolenia powinny uwzględniać kadrę 4 informatyków:

1. Szkolenia specjalistyczne z zakresu zarządzania urządzeniami klasy UTM (Unified Threat Management) oraz zabezpieczeń sieciowych z dostarczonego rozwiązania:

Zakres tematyczny szkolenia:

- Konfigurowanie i zarządzanie urządzeniami bezpieczeństwa sieciowego klasy UTM
- Ustawienia i struktura sieci – konfiguracja interfejsów, trasowania i stref bezpieczeństwa
- Tworzenie i zarządzanie politykami dostępu oraz kontami użytkowników
- Konfiguracja zapór ogniowych i mechanizmów inspekcji ruchu sieciowego
- Wdrażanie i zarządzanie wirtualnymi sieciami prywatnymi (VPN)
- Zastosowanie mechanizmów głębokiej inspekcji pakietów szyfrowanych (SSL/TLS)
- Filtrowanie treści i kontrola aplikacji w sieci
- Konfiguracja rozwiązań zwiększających niezawodność sieci

- Monitorowanie zdarzeń bezpieczeństwa oraz analiza logów
- Narzędzia diagnostyczne i metody rozwiązywania problemów w środowisku zabezpieczeń sieciowych
- Część praktyczna powinna być realizowana w środowisku testowym/laboratoryjnym symulującym rzeczywiste przypadki wdrożeniowe
- Uczestnik szkolenia powinien otrzymać imienny certyfikat potwierdzający udział i zakres zrealizowanych zagadnień

2. Szkolenie specjalistyczne z zakresu zarządzania dostarczonym systemem kontroli dostępu do sieci (NAC)

- Instalacja i podstawowa konfiguracja systemu kontroli dostępu do sieci (NAC)
- Integracja z infrastrukturą sieciową – przełączniki, punkty dostępowe, serwery autoryzacji
- Zarządzanie politykami dostępu, profilowaniem urządzeń i tożsamościami użytkowników
- Obsługa mechanizmów dynamicznego przypisywania uprawnień i ról w sieci
- Zaawansowana konfiguracja polityk, reguł dostępu, segmentacji i automatyzacji reakcji
- Analiza zdarzeń bezpieczeństwa, logów i informacji diagnostycznych
- Integracja z systemami zewnętrznymi (np. AD, DHCP, RADIUS, syslog, API)
- Rozwiązywanie problemów i analiza przypadków błędnego działania systemu kontroli dostępu
- Najlepsze praktyki w zakresie zarządzania, skalowania i utrzymania systemu NAC
- Przegląd przypadków użycia i scenariuszy wdrożeniowych w środowisku produkcyjnym
- Część praktyczna powinna być realizowana w środowisku testowym/laboratoryjnym symulującym rzeczywiste przypadki wdrożeniowe
- Uczestnik szkolenia powinien otrzymać imienny certyfikat potwierdzający udział i zakres zrealizowanych zagadnień
- Szkolenie musi być przeprowadzone przez producenta systemu posiadającego uprawnienia do prowadzenia szkoleń z danego systemu oraz wydawania oficjalnych certyfikatów potwierdzających ukończenie kursu

3. Szkolenie specjalistyczne z zakresu instalacji, konfiguracji oraz zarządzania dostarczonym systemem monitorowania i zarządzania infrastrukturą sieciową:

- Instalacja oraz podstawowa konfiguracja systemu do monitorowania i zarządzania infrastrukturą sieciową
- Integracja z urządzeniami sieciowymi (przełączniki, punkty dostępowe, routery, firewalle)
- Konfiguracja źródeł danych i mechanizmów zbierania informacji o stanie sieci
- Tworzenie i zarządzanie topologią sieci oraz widokami logicznymi i fizycznymi
- Tworzenie harmonogramów zadań zarządczych oraz polityk konfiguracji
- Obsługa systemu zarządzania konfiguracją urządzeń (archiwizacja, porównywanie, przywracanie)
- Obsługa systemu alarmów i powiadomień – definicje, poziomy, automatyzacja reakcji
- Zarządzanie cyklem życia urządzeń w sieci – wykrywanie, rejestrowanie, usuwanie
- Konfigurowanie dostępu użytkowników i ról administracyjnych w systemie
- Praca z raportami, eksportami danych i integracjami z systemami zewnętrznymi
- Część praktyczna powinna być realizowana w środowisku testowym/laboratoryjnym symulującym rzeczywiste przypadki wdrożeniowe

- Uczestnik szkolenia powinien otrzymać imienny certyfikat potwierdzający udział i zakres zrealizowanych zagadnień
- Szkolenie musi być przeprowadzone przez autoryzowany ośrodek szkoleniowy posiadający uprawnienia do prowadzenia szkoleń z danego systemu oraz wydawania oficjalnych certyfikatów potwierdzających ukończenie kursu

4. Szkolenie dla informatyków z zakresu instalacji i konfiguracji dostarczonych urządzeń sieciowych:

- Wykonawca zapewni warsztaty dotyczące instalacji, konfiguracji i zarządzania infrastrukturą sieciową w środowiskach opartych na dostarczonych przełącznikach sieciowych.
- Warsztaty obejmą zagadnienia takie jak:
 - Podstawy funkcjonowania sieci i mechanizmy warstwy 2 i 3
 - Konfiguracja VLAN, agregacji łączy i mechanizmów redundancji
 - Implementacja routingu statycznego oraz dynamicznego
 - Podstawy obsługi protokołów multicast i IPv6.
- Wykonawca dostarczy każdemu uczestnikowi materiały szkoleniowe w formie elektronicznej
- Po zakończeniu warsztatów uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo oraz nabycie umiejętności w zakresie instalacji i konfiguracji przełączników sieciowych
- Forma warsztatów - zdalna

17. Wdrożenie infrastruktury IT -instalacja i konfiguracja klastra wirtualnego, usług katalogowych (AD), backupu, systemów bezpieczeństwa i segmentacji siec

Serwery z macierzą

Wymagania wdrożeniowe

1. Przygotowanie planu wdrożenia i migracji
Plan wdrożenia powinien obejmować pełny harmonogram prac, opis działań instalacyjnych i konfiguracyjnych, zakres zadań migracyjnych, plan testów powdrożeniowych oraz sposób odtworzenia środowiska w przypadku awarii.
Dokument powinien uwzględniać strukturę połączeń sieciowych, zasady pracy klastra wysokiej dostępności oraz integrację z istniejącą infrastrukturą Zamawiającego.
2. Instalacja dostarczonego sprzętu
Serwery oraz macierz dyskowa powinny zostać zainstalowane w szafie rack w siedzibie Zamawiającego.
Proces instalacji obejmuje montaż fizyczny, podłączenie zasilania, sieci komunikacyjnych i zarządzających oraz wstępną weryfikację poprawności działania komponentów.
3. Aktualizacja i konfiguracja systemowa
W ramach przygotowania środowiska serwerowego należy przeprowadzić:
 - aktualizację oprogramowania sprzętowego (firmware) oraz BIOS,

- konfigurację parametrów zarządzania i monitorowania urządzeń,
- przygotowanie konfiguracji sprzętowej zgodnej z wytycznymi projektu wdrożenia,
- zapewnienie dostępu do paneli konfiguracyjnych i konsol zarządzania przez wydzieloną sieć administracyjną.

4. Integracja z infrastrukturą Zamawiającego

Serwery oraz macierz dyskowa muszą zostać podłączone do istniejącej infrastruktury teleinformatycznej, z zachowaniem redundancji połączeń fizycznych w sieciach LAN i SAN. Podłączenia powinny obejmować ścieżki komunikacji danych użytkowników oraz kanały zarządzania.

Zastosowane rozwiązanie musi umożliwiać elastyczne rozszerzanie topologii o kolejne węzły i zasoby.

5. Konfiguracja środowiska serwerowego i macierzowego

Konfiguracja ma obejmować przygotowanie serwerów, macierzy dyskowej oraz oprogramowania systemowego w celu uruchomienia komunikacji w oparciu o protokół iSCSI. Wymagane jest zapewnienie wielościeżkowości komunikacji (multipathing) pomiędzy serwerami a macierzą w celu podniesienia poziomu dostępności.

Środowisko powinno zostać skonfigurowane tak, aby działało w klastrze wysokiej dostępności (HA) z pełną redundancją dostępu do danych.

Konfiguracja obejmuje:

- pełne przygotowanie i konfigurację hypervisora oraz zainstalowanych systemów operacyjnych,
- środowisko oparte na dwóch serwerach fizycznych i współdzielonym zasobie macierzowym,
- utworzenie klastra HA dla maszyn wirtualnych uruchamianych równolegle na obu serwerach,
- automatyczne przenoszenie i wznowianie pracy maszyn wirtualnych w przypadku awarii jednego z serwerów,
- konfigurację wirtualnych przełączników (virtualswitches) z obsługą mechanizmów Dynamic VMMQ oraz RDMA, zapewniających optymalną wydajność sieciową.

6. Migracja środowiska wirtualnego

Wirtualne serwery funkcjonujące dotychczas w infrastrukturze Zamawiającego powinny zostać przeniesione do nowo wdrożonego środowiska serwerowego.

Migracja musi obejmować zachowanie konfiguracji maszyn wirtualnych, ich parametrów sieciowych, przestrzeni dyskowych oraz powiązań aplikacyjnych.

Po zakończeniu migracji należy przeprowadzić testy poprawności pracy środowiska wirtualnego, z uwzględnieniem wydajności oraz komunikacji między komponentami.

7. Migracja baz danych i aplikacji

Migracja powinna obejmować przeniesienie baz danych oraz najważniejszych aplikacji wykorzystywanych przez Zamawiającego na nowy system operacyjny.

Proces obejmuje przeniesienie silnika bazy danych, konfiguracji, wszystkich baz użytkowników

oraz aplikacji współpracujących z systemami zewnętrznymi.

Po migracji należy zweryfikować:

- poprawność działania aplikacji i baz danych,
 - możliwość realizacji połączeń z zasobami sieciowymi,
 - logowanie i autoryzację użytkowników,
 - dostęp do sieci Internet,
 - zgodność zasad bezpieczeństwa i uprawnień.
8. Testy powdrożeniowe i walidacja środowiska
- Po zakończeniu procesu migracji należy przeprowadzić szczegółowe testy funkcjonalne obejmujące:
- uruchomienie i pracę serwerów wirtualnych w nowym środowisku,
 - weryfikację poprawności połączeń z zasobami sieciowymi,
 - testy logowania, autoryzacji i polityk użytkowników,
 - potwierdzenie pełnej dostępności aplikacji i baz danych.

Niezależny system backupu

Wymagania wdrożeniowe

1. Instalacja sprzętu w szafie serwerowej
Urządzenia: serwer backupowy, biblioteka taśmowa oraz jednostka pamięci masowej typu NAS powinny zostać zainstalowane w szafie rack, zlokalizowanej w siedzibie Zamawiającego.
Instalacja obejmuje montaż mechaniczny, podłączenie zasilania, zapewnienie odpowiedniej wentylacji oraz wykonanie niezbędnych połączeń sieciowych i komunikacyjnych pomiędzy komponentami systemu.
2. Integracja z infrastrukturą teleinformatyczną Zamawiającego
Środowisko backupowe powinno zostać podłączone do istniejącej infrastruktury serwerowej i sieciowej z zachowaniem pełnej separacji logicznej od środowiska produkcyjnego.
Połączenia sieciowe powinny być zestawione w architekturze redundantnej, tak aby awaria pojedynczej ścieżki nie wpływała na dostępność systemu backupu.
Dostęp do interfejsów administracyjnych i monitorujących urządzenia musi być realizowany przez wydzieloną sieć zarządzającą, zapewniającą kontrolowany i bezpieczny dostęp do konfiguracji.
3. Konfiguracja systemu backupowego
Konfiguracja środowiska powinna obejmować pełne połączenie i integrację wszystkich komponentów systemu, w tym:
 - instalację i konfigurację serwera backupowego wraz z systemem operacyjnym i oprogramowaniem do wykonywania kopii zapasowych danych,
 - konfigurację urządzenia typu NAS jako repozytorium danych backupowych dla codziennych i przyrostowych kopii,

- konfigurację biblioteki taśmowej jako urządzenia archiwizacyjnego do przechowywania długoterminowych kopii danych,
 - integrację oprogramowania backupowego z biblioteką taśmową i pamięcią NAS,
 - przygotowanie harmonogramu zadań backupowych oraz konfigurację polityk retencji danych,
 - wdrożenie polityk bezpieczeństwa dostępu do środowiska backupowego, w tym mechanizmów rozdzielania ról administracyjnych i kontroli autoryzacji,
 - konfigurację alertów, raportów i powiadomień systemowych o przebiegu procesów backupu.
4. Polityka tworzenia i zarządzania kopiami zapasowymi
- Polityka backupowa powinna określać:
- częstotliwość i rodzaje wykonywanych kopii (pełne, przyrostowe, różnicowe),
 - sposób przechowywania i rotacji danych,
 - podział danych według poziomu krytyczności,
 - zasady przechowywania kopii w lokalizacji alternatywnej (odmiejscowienie danych).
5. Objęcie systemem backupu kluczowych systemów Zamawiającego
- Środowisko backupowe powinno obejmować wszystkie istotne komponenty infrastruktury Zamawiającego, w tym:
- serwery baz danych i aplikacji,
 - serwery plików i usług katalogowych,
 - maszyny wirtualne oraz ich migawki systemowe (VM snapshots),
6. Wdrożenie systemu odmiejscowienia kopii zapasowych
- W ramach wdrożenia należy przygotować i uruchomić proces tworzenia kopii zapasowych z ich przenoszeniem do lokalizacji zapasowej, poza głównym ośrodkiem przetwarzania danych. Wdrożenie obejmuje:
- konfigurację mechanizmu automatycznego eksportu kopii zapasowych na nośniki taśmowe przechowywane w innej lokalizacji,
 - przygotowanie alternatywnej lokalizacji (np. oddział, magazyn, sejf danych, serwer NAS w innej serwerowni),
 - zaplanowanie i wdrożenie harmonogramu przenoszenia kopii,
7. Testy odtworzeniowe i walidacja działania systemu
- Wdrożenie powinno zakończyć się przeprowadzeniem testów odtworzeniowych, potwierdzających możliwość przywrócenia danych z kopii zapasowych w pełnym zakresie, w tym:
- odtworzenie pojedynczych plików, kompletnej maszyny wirtualnej,
 - weryfikację poprawności integralności kopii,
 - testowanie procedur automatycznego przywracania danych w scenariuszu awaryjnym.
8. Instruktaż administratorów
- Po zakończeniu wdrożenia należy przeprowadzić instruktaż administratorów środowiska IT, obejmujący:
- zasady wykonywania i monitorowania zadań backupowych,
 - procedury odtwarzania danych i weryfikacji kopii,
 - zarządzanie użytkownikami i uprawnieniami w systemie backupowym,

- o harmonogramy archiwizacji oraz polityki retencji danych.

Konfiguracja usługi katalogowej:

Wymagania wdrożeniowe

1. Przygotowanie planu wdrożenia usług domenowych
Plan wdrożenia powinien zawierać analizę istniejącej infrastruktury, model logicznej i fizycznej struktury domeny, zasady rozmieszczenia kontrolerów domeny oraz projekt polityk bezpieczeństwa.
Projekt musi określać:
 - o strukturę jednostek organizacyjnych (OU),
 - o sposób integracji z usługami katalogowymi,
 - o plan implementacji zabezpieczeń i polityk grupowych.
2. Instalacja i konfiguracja systemu operacyjnego serwera
Na dedykowanym serwerze należy zainstalować i skonfigurować system operacyjny klasy serwer z uwzględnieniem wymagań wydajnościowych i bezpieczeństwa.
Konfiguracja powinna obejmować ustawienie parametrów sieciowych, synchronizacji czasu, regionalizacji oraz przygotowanie systemu do instalacji roli kontrolera domeny.
3. Wdrożenie usług katalogowych (Active Directory Domain Services)
Środowisko domenowe powinno zostać wdrożone z uwzględnieniem wysokiej dostępności i replikacji danych.
Zakres wdrożenia obejmuje:
 - o instalację i uruchomienie roli usług katalogowych (AD DS),
 - o konfigurację stref DNS z redundancją i replikacją,
 - o wdrożenie usługi DHCP z mechanizmem failover,
 - o konfigurację replikacji między kontrolerami domeny,
 - o utworzenie i konfigurację trust relationships pomiędzy domenami,
 - o implementację dynamicznych aktualizacji DNS (Dynamic DNS Updates),
 - o konfigurację Global Catalog oraz operacji FSMO (Flexible Single Master Operations).
4. Planowanie i implementacja struktury organizacyjnej (OU)
Należy zaprojektować i wdrożyć logiczną strukturę jednostek organizacyjnych (OU) zgodną ze schematem organizacyjnym Zamawiającego.
Struktura powinna odzwierciedlać podział organizacyjno-funkcyjny oraz umożliwiać przypisywanie odpowiednich polityk i uprawnień użytkownikom oraz stacjom roboczym.
5. Konfiguracja polityk grupowych (GPO)
W ramach wdrożenia należy zaimplementować polityki grupowe (Group Policy Objects) z elementami „baseline” bezpieczeństwa oraz najlepszymi praktykami zgodnymi z wytycznymi producenta systemu.
Zakres obejmuje:
 - o wdrożenie polityk bezpieczeństwa haseł i kont użytkowników,
 - o konfigurację zasad blokady kont po nieudanych logowaniach,
 - o ustawienia zapory systemowej, aktualizacji i uwierzytelniania,
 - o implementację polityk konfiguracyjnych dla stacji roboczych i serwerów,
 - o wdrożenie zasad audytu i raportowania zdarzeń.
6. Konfiguracja replikacji i mechanizmów wysokiej dostępności
Wdrażana infrastruktura powinna zapewniać pełną replikację danych katalogowych między kontrolerami oraz automatyczną synchronizację parametrów konfiguracji.
Replikacja ma być przeprowadzona w trybie zabezpieczonym z użyciem szyfrowania i uwierzytelnienia, minimalizując opóźnienia transmisji danych między serwerami.

7. Wdrożenie mechanizmów bezpieczeństwa i audytu

Zakres obejmuje:

- o implementację uwierzytelnienia szyfrowanego (LDAPS, Kerberos),
- o wdrożenie audytów zaawansowanych

8. Wdrożenie usług certyfikatów (ADCS)

W ramach wdrożenia należy przygotować projekt usługi certyfikatów z implementacją serwera głównego (Offline Root) oraz konfiguracją do 3 szablonów certyfikatów.

Należy przeprowadzić pełną konfigurację ról i certyfikatów pośrednich (Subordinate), obejmującą m.in.:

- o konfigurację serwera pełniącego rolę jednostki certyfikującej,
- o przygotowanie środowiska do generowania i dystrybucji certyfikatów,
- o wsparcie w procesie generowania certyfikatu głównego (ROOT).

9. Konfiguracja usług plików (File Server)

Na serwerze plików należy przeprowadzić:

- o konfigurację uprawnień NTFS i zasad dostępu do udziałów sieciowych,
- o wdrożenie polityk kwot (Quota Management) dla kontroli wykorzystania przestrzeni dyskowej,
- o konfigurację polityk dostępu i audytów plików,
- o integrację z usługą Active Directory w zakresie nadawania i modyfikacji uprawnień.

10. Wdrożenie najlepszych praktyk bezpieczeństwa dla GPO

Wszystkie wdrożone polityki grupowe muszą być oparte na uznanych standardach bezpieczeństwa i zgodne z rekomendacjami branżowymi (bestpractices).

11. Migracja użytkowników i urządzeń do domeny

W ramach wdrożenia należy przeprowadzić migrację stacji roboczych i serwerów z grupy roboczej do nowo utworzonej domeny.

Zakres obejmuje:

- o podłączenie do 30 stacji roboczych do domeny, z zachowaniem istniejących profili użytkowników i danych,
- o migrację do 5 serwerów do domeny, z utrzymaniem ciągłości usług i procesów,
- o weryfikację komunikacji z kontrolerami domeny oraz poprawności przypisania polityk i uprawnień,
- o testy poprawności logowania, autoryzacji i dostępu do zasobów po migracji.

12. Testy funkcjonalne i bezpieczeństwa

Po zakończeniu wszystkich etapów wdrożenia należy przeprowadzić testy funkcjonalne i bezpieczeństwa obejmujące:

- o sprawdzenie poprawności działania AD DS, DNS, DHCP, GPO, ADCS i replikacji,
- o testy procedur logowania, nadawania uprawnień i obsługi certyfikatów,
- o weryfikację redundancji i odtwarzalności konfiguracji,

System do zarządzania urządzeniami końcowymi

Wymagania wdrożeniowe

1. Analiza środowiska informatycznego i wymagań organizacji

Przed rozpoczęciem prac wdrożeniowych powinna zostać przeprowadzona pełna analiza środowiska informatycznego, obejmująca inwentaryzację urządzeń sieciowych, serwerów, stacji roboczych, systemów operacyjnych, aplikacji i kont użytkowników.

Analiza musi obejmować również aktualne procedury bezpieczeństwa, polityki dostępu, strukturę sieci, usługi katalogowe oraz istniejące systemy wspierające zarządzanie IT.

2. Instalacja oprogramowania serwerowego i agentów klienckich

W ramach wdrożenia należy przeprowadzić instalację oraz konfigurację komponentów serwerowych systemu, w tym:

- modułów zarządzania, monitoringu, raportowania i analiz,
- środowiska bazodanowego,
- usług komunikacyjnych i zabezpieczeń.

Równocześnie należy zainstalować i skonfigurować oprogramowanie klienckie (agentów systemowych) odpowiedzialnych za gromadzenie i przesyłanie danych dotyczących stanu urządzeń, aktywności użytkowników, wykorzystania zasobów oraz pracy aplikacji.

Konfiguracja powinna obejmować również ustawienie certyfikatów bezpieczeństwa, parametrów sieciowych oraz integrację z systemami autoryzacji użytkowników i usługami katalogowymi.

3. Konfiguracja funkcji monitorowania, raportowania i zarządzania

Wdrożenie powinno obejmować pełne uruchomienie i konfigurację funkcjonalności systemu w zakresie:

- monitorowania dostępności i wydajności urządzeń sieciowych, serwerów, stacji roboczych oraz aplikacji,
- pomiaru wykorzystania zasobów (procesor, pamięć, dysk, interfejsy sieciowe),
- definiowania progów ostrzeżeń i alarmów oraz wysyłania powiadomień o awariach lub anomaliach,
- rejestrowania aktywności użytkowników, uruchamianych procesów, aplikacji i transferów danych,
- zarządzania oprogramowaniem – ewidencjonowania licencji, instalacji i dezinstalacji aplikacji, audytu i kontroli wersji,
- zdalnego zarządzania stacjami roboczymi i serwerami (zdalny pulpit, terminal, zdalne polecenia administracyjne, dystrybucje aktualizacji),
- graficznej wizualizacji topologii sieci wraz z automatycznym wykrywaniem urządzeń i prezentacją aktywnych połączeń,
- monitorowania usług sieciowych, portów, protokołów i adresów IP,
- generowania raportów z wykorzystania zasobów, poziomu dostępności, czasu reakcji i incydentów bezpieczeństwa.

4. Konfiguracja mechanizmów bezpieczeństwa

W ramach wdrożenia należy dostosować ustawienia systemu monitorowania do polityk bezpieczeństwa organizacji, obejmujących:

- kontrolę dostępu użytkowników i nadawanie uprawnień,
- szyfrowanie transmisji danych pomiędzy serwerem a agentami,
- archiwizację logów i zdarzeń bezpieczeństwa,
- segmentację stref komunikacyjnych w oparciu o sieci logiczne VLAN.

5. Przeprowadzenie testów akceptacyjnych

Po zakończeniu konfiguracji należy przeprowadzić testy funkcjonalne, wydajnościowe i bezpieczeństwa systemu, mające na celu potwierdzenie poprawnego działania wszystkich kluczowych funkcji, w tym:

- monitoringu i raportowania,
- generowania alertów i powiadomień,
- zdalnego zarządzania stanowiskami pracy,
- integracji z systemami zewnętrznymi i bazami danych..

6. Przygotowanie dokumentacji powdrożeniowej

Dokumentacja powdrożeniowa powinna zawierać:

- pełny opis konfiguracji środowiska, w tym serwera, agentów i integracji,
- instrukcje administracyjne dla użytkowników systemu,
- procedury eksploatacji, aktualizacji i utrzymania,
- opis struktury bazy danych oraz sposobu synchronizacji z systemami zewnętrznymi,
- zalecenia w zakresie bezpieczeństwa, tworzenia kopii zapasowych i optymalizacji wydajności.

7. Szkolenie administratorów i wyznaczonych użytkowników

Po zakończeniu wdrożenia należy przeprowadzić szkolenie dla administratorów oraz wskazanych użytkowników systemu.

Zakres szkolenia powinien obejmować:

- obsługę narzędzi administracyjnych i konsoli systemu,
- konfigurację alertów, raportów i progów alarmowych,
- analizę danych monitorujących i interpretację wskaźników wydajności,
- praktyczne ćwiczenia z wykorzystania systemu w środowisku testowym.

Przełączniki sieciowe dostępne

Wymagania wdrożeniowe

1. Instalacja sprzętu w szafie serwerowej

Przełączniki dostępne należy zainstalować w szafach rack znajdujących się w siedzibie Zamawiającego.

Instalacja obejmuje montaż mechaniczny urządzeń, podłączenie do zasilania oraz do sieci komunikacyjnej zgodnie z obowiązującą topologią.

Po zakończeniu montażu należy zweryfikować poprawność połączeń oraz status działania wszystkich interfejsów.

2. Przygotowanie i konfiguracja podstawowa urządzeń

W ramach wdrożenia należy przeprowadzić podstawową konfigurację każdego przełącznika, obejmującą:

- nadanie unikalnego adresu IP w obrębie sieci zarządzającej,
- włączenie i konfigurację dostępu administracyjnego SSH,
- zmianę domyślnych haseł na zgodne z polityką bezpieczeństwa organizacji,
- przypisanie odpowiednich nazw w celu jednoznacznej identyfikacji urządzeń w systemach zarządzania.

3. Konfiguracja stosów przełączników (stacking)

Urządzenia przeznaczone do pracy w konfiguracji stosu należy połączyć logicznie zgodnie z przyjętym projektem i zaleceniami działu IT Zamawiającego.

Należy utworzyć hierarchię przełączników, określając jednostkę nadrzędną (master) i zapasową (backup), a następnie zweryfikować poprawność komunikacji między nimi.

Konfiguracja powinna uwzględniać automatyczne odtwarzanie funkcji w przypadku awarii jednego z urządzeń stosu.

4. Aktualizacja oprogramowania układowego (firmware)

Wszystkie przełączniki należy zaktualizować do najnowszej wersji oprogramowania dostępnej dla danego modelu, zapewniającej stabilność, kompatybilność i bezpieczeństwo.

Proces aktualizacji powinien zostać przeprowadzony zgodnie z wytycznymi producenta oraz polityką utrzymania infrastruktury Zamawiającego.

5. Konfiguracja mechanizmów zabezpieczających i redundancji

W ramach wdrożenia należy włączyć i skonfigurować mechanizmy zapewniające redundancję oraz ochronę przed pętlami w sieci:

- o uruchomienie i konfigurację protokołu MSTP lub równoważnego,
- o konfigurację mechanizmu detekcji i zapobiegania pętlom sieciowym (ELRP lub rozwiązanie równoważne),
- o wdrożenie protokołu STP (SpanningTreeProtocol) z odpowiednimi priorytetami dla urządzeń nadrzędnych,
- o test weryfikujący poprawność przełączania ścieżek sieciowych w sytuacjach awaryjnych.

6. Konfiguracja usług sieciowych i bezpieczeństwa warstwy drugiej (L2)

W celu zapewnienia stabilnej i bezpiecznej pracy sieci dostępnej należy skonfigurować następujące elementy:

- o włączenie i konfigurację protokołu DHCP Snooping lub równoważnego w celu zapobiegania nieautoryzowanym serwerom DHCP,
- o konfigurację Access Control List (ACL) zgodnie z wymaganiami bezpieczeństwa Zamawiającego,
- o utworzenie i przypisanie VLAN-ów zgodnie z obowiązującym projektem sieci logicznej,
- o przyporządkowanie portów do odpowiednich VLAN-ów,
- o zastosowanie port-security z limitami adresów MAC, jeśli wynika to z polityki bezpieczeństwa.

7. Konfiguracja centralnego logowania i monitoringu

Przełączniki należy skonfigurować do wysyłania logów systemowych do centralnego serwera logów.

Wdrożenie obejmuje:

- o określenie adresu serwera syslog,
- o poziomy logowania (informacje, błędy, alerty),
- o weryfikację przesyłania zapisów i ich archiwizacji.

8. Wdrożenie dobrych praktyk (bestpractices)

W ramach wdrożenia przełączników należy zastosować uznane zasady projektowania i konfiguracji infrastruktury sieciowej, w tym:

- o stosowanie VLAN-ów administracyjnych odseparowanych od ruchu użytkowego,
- o wyłączenie nieużywanych portów oraz przypisanie ich do dedykowanego VLAN-u z ograniczonym dostępem,
- o wdrożenie funkcji automatycznego blokowania portów w przypadku wykrycia anomalii,
- o stosowanie szyfrowanych kanałów komunikacji administracyjnej (SSH, HTTPS lub równoważnych),
- o egzekwowanie zasad „leastprivilegeaccess” dla kont zarządzających,
- o tworzenie kopii zapasowych konfiguracji po pełnym wdrożeniu,
- o wdrożenie dokumentacji etykietowania i oznaczeń portów fizycznych,
- o utrzymywanie jednolitego schematu nazewnictwa urządzeń i interfejsów,

9. Testy działania i odbiór wdrożenia

Po zakończeniu konfiguracji należy przeprowadzić testy funkcjonalne w zakresie:

- o poprawnego działania komunikacji w obrębie wszystkich VLAN-ów,
- o redundancji połączeń i braku pętli sieciowych,
- o poprawnej pracy protokołów routingu i przełączania,
- o dostępności połączeń SSH oraz prawidłowości reguł ACL.

10. Przygotowanie dokumentacji powdrożeniowej

Dokumentacja powinna zawierać:

- o opis konfiguracji każdego przełącznika,
- o wykaz VLAN-ów, ACL i protokołów routingu,
- o schemat połączeń logicznych i fizycznych,
- o listę urządzeń uwzględnionych w konfiguracji,
- o procedury administracyjne i utrzymaniowe.

11. Instruktaż administratorów sieci

Po zakończeniu prac wdrożeniowych należy przeprowadzić szkolenie dla administratorów sieci.

Zakres szkolenia obejmuje:

- o omówienie wprowadzonych ustawień,
- o zasady bezpieczeństwa i administracji przełącznikami,
- o procedury monitorowania i reagowania na awarie,
- o zasady aktualizacji oprogramowania i archiwizacji konfiguracji.

Przełączniki sieciowe CORE

Wymagania wdrożeniowe

1. Architektura logiczna i fizyczna

- Cztery przełączniki tworzą dwa niezależne klastry wysokiej dostępności pracujące w trybie active-active.
- Klaster A zlokalizowany jest w serwerowni A i pełni funkcję przełączników warstwy rdzeniowej/Top-of-Rack (CORE/TOR) dla:
 - o agregacji punktów dystrybucyjnych,
 - o redundantnego podłączenia środowiska serwerowego.
- Klaster B zlokalizowany jest w serwerowni B i zapewnia:
 - o obsługę połączeń z punktami dystrybucyjnymi,
 - o połączenia z lokalnym środowiskiem serwerowym w serwerowni B.

Połączenia między serwerowniami powinny zapewniać przepustowość co najmniej 50Gb/s, z możliwością rozbudowy przepustowości zgodnie z dostępnością łączy światłowodowych (np. poprzez dodawanie kolejnych łączy i grupowanie ich w port-channel/LAG lub równoważny).

2. Instalacja i rozmieszczenie przełączników

- Przełączniki klastra A należy zainstalować w szafach rack w serwerowni A, zgodnie z projektem rozmieszczenia urządzeń rdzeniowych/TOR.
- Przełączniki klastra B należy zainstalować w szafach rack w serwerowni B, jako centralne elementy agregujące połączenia dystrybucyjne i serwerowe.
- Instalacja obejmuje montaż mechaniczny, podłączenie redundantnego zasilania oraz wykonanie połączeń światłowodowych między serwerowniami.

3. Konfiguracja klastrów wysokiej dostępności (active-active)

- Każda para przełączników (klaster A i klaster B) powinna zostać skonfigurowana jako klaster wysokiej dostępności w trybie active-active z pełną synchronizacją konfiguracji.

- W ramach wdrożenia należy:
 - skonfigurować mechanizmy łączenia przełączników w klastery (stacking, MLAG, port-channel lub równoważne),
 - zapewnić równoległe wykorzystanie ścieżek transmisyjnych oraz automatyczne przełączanie w przypadku awarii jednego z przełączników,
 - zweryfikować działanie klastrów poprzez testy failover oraz równoważnego rozkładu ruchu (load-balancing).

4. Połączenia między serwerowniami i wielościeżkowość

- Pomiędzy serwerownią A a serwerownią B należy zestawić redundantne połączenia światłowodowe o sumarycznej przepustowości co najmniej 50Gb/s.
- Połączenia między klastrem A a klastrem B powinny być realizowane w topologii pełnej siatki (full-mesh) lub równoważnej, umożliwiającej pełną wielościeżkowość. W przypadku kiedy będzie dostępna odpowiednia ilość światłowodów.
- Należy skonfigurować:
 - grupy portów (LAG/port-channel lub równoważne) w celu agregacji przepustowości,
 - nadmiarowe ścieżki logiczne dla ruchu serwerowego i dystrybucyjnego.

5. Integracja z środowiskiem serwerowym i urządzeniami UTM

- W serwerowni A klastery przełączników muszą zostać podłączone do środowiska serwerowego w sposób redundantny:
 - serwery powinny posiadać minimum dwie niezależne ścieżki do klastra A (LACP/MLAG lub równoważny),
 - konfiguracja powinna zapewniać działanie w trybie active-active z równomiernym podziałem obciążenia.
- Klastery A muszą zostać podłączone do klastra urządzeń UTM z zastosowaniem wielościeżkowości i pełnej redundancji połączeń.
- Połączenia z urządzeniami UTM mają być realizowane w architekturze full-mesh lub równoważnej,

6. Integracja klastra B z punktami dystrybucyjnymi i środowiskiem serwerowym

- Klastery B w serwerowni B powinny zostać podłączone do punktów dystrybucyjnych z zachowaniem:
 - redundancji łączy uplinkowych,
 - rozdzielenia ścieżek między przełącznikami klastra.
- Środowisko serwerowe w serwerowni B należy podłączyć do klastra B z wykorzystaniem wielościeżkowości, podobnie jak w serwerowni A (port-channel/MLAG lub równoważny).
- Konfiguracja powinna zapewniać spójne zarządzanie VLAN-ami, routingiem oraz politykami bezpieczeństwa między klastrem A i B.

7. Konfiguracja warstwy L2/L3 i segmentacji

- Należy skonfigurować:
 - VLAN-y dla warstwy serwerowej, dystrybucyjnej oraz zarządzającej,
 - interfejsy warstwy trzeciej (SVI) dla obsługi ruchu międzysegmentowego,
 - protokoły routingu dynamicznego (np. OSPF, BGP lub równoważny) bądź trasy statyczne, zgodnie z projektem sieci Zamawiającego.
- Konfiguracja powinna zapewniać:
 - spójną segmentację sieci między serwerowniami,
 - optymalne trasy pomiędzy środowiskiem serwerowym a punktami dystrybucyjnymi,
 - odporność na awarie pojedynczych łączy lub przełączników.

8. Mechanizmy bezpieczeństwa i zarządzania

- Należy zastosować:
 - szyfrowane protokoły zarządzania (SSH, HTTPS lub równoważne),
 - listy kontroli dostępu (ACL) filtrujące ruch administracyjny i międzysegmentowy,
 - mechanizmy ochrony warstwy drugiej (DHCP Snooping, Dynamic ARP Inspection, port-security lub równoważne),
 - integrację z centralnym systemem logowania i monitoringu (syslog/SNMPv3 lub równoważny).

Testy, dokumentacja i szkolenie

9. Testy funkcjonalne i wysokiej dostępności

- Po zakończeniu konfiguracji należy przeprowadzić testy obejmujące:
 - przełączanie ruchu między ścieżkami w ramach klastrów active-active,
 - zachowanie ciągłości ruchu przy awarii pojedynczego przełącznika lub łącza między serwerowniami,
 - weryfikację przepustowości połączeń między serwerowniami przy obciążeniu zbliżonym do produkcyjnego,
 - poprawność działania wielościeżkowości (ECMP/LAG lub równoważny).

10. Dokumentacja powdrożeniowa

- Dokumentacja powinna zawierać:
 - schemat logiczny i fizyczny połączeń przełączników w obu serwerowniach,
 - opis konfiguracji klastrów A i B, w tym mechanizmów HA i multipath,
 - listę VLAN-ów, interfejsów, tras oraz połączeń do środowiska serwerowego i urządzeń UTM,
 - procedury awaryjne i odtworzeniowe (np. wymiana przełącznika w klastrze, odtworzenie konfiguracji).

11. Instruktaż administratorów

- Po zakończeniu wdrożenia powinien zostać przeprowadzony instruktaż dla administratorów sieci, obejmujący:
 - omówienie architektury klastrów i połączeń między serwerowniami,
 - zasady zarządzania konfiguracją i wprowadzania zmian,
 - procedury reagowania na awarie klastrów i łączy,

Urządzenia UTM

Wymagania wdrożeniowe

1. Analiza środowiska
Analiza środowiska sieciowego powinna zostać przeprowadzona w zakresie obejmującym topologię sieci, przepustowość łączy, obowiązujące polityki bezpieczeństwa oraz istniejącą segmentację.
Wyniki analizy stanowią podstawę do opracowania projektu architektury rozwiązania, uwzględniającego lokalizację urządzeń, strukturę połączeń, strefy bezpieczeństwa oraz integrację z infrastrukturą Zamawiającego.
2. Montaż urządzeń w szafie rack
3. Nadanie adresu IP
4. Konfiguracja dostępu SSH
5. Zmiana haseł dostępu
6. Aktualizacja oprogramowania do najnowszej możliwej wersji
7. Konfiguracja klastra wysokiej dostępności (HA)
Konfiguracja klastra powinna obejmować zestawienie dwóch urządzeń w trybie aktywny-

pasywny, zapewniające synchronizację konfiguracji, sesji użytkowników.

Mechanizm przełączania awaryjnego (failover) musi funkcjonować bez przerw w transmisji i bez utraty sesji użytkowników.

Działanie klastra podlega testom potwierdzającym poprawność konfiguracji.

8. Polityka bezpieczeństwa i reguły ruchu sieciowego

W ramach wdrożenia przewiduje się utworzenie i konfigurację do 500 reguł bezpieczeństwa dotyczących filtrowania protokołów, adresów, portów oraz ruchu przychodzącego i wychodzącego.

Polityka bezpieczeństwa obejmuje:

- segmentację sieci na strefy bezpieczeństwa (wewnętrzna, DMZ, zewnętrzna),
- translację adresów (NAT), przekierowania portów, kontrolę dostępu,
- mechanizmy logowania i raportowania,
- reguły oparte na tożsamości użytkownika lub grupy.

Konfiguracja powinna umożliwiać wersjonowanie i audyt zmian w regułach bezpieczeństwa.

9. Konfiguracja elementów bezpieczeństwa (security services)

Wdrożenie musi obejmować konfigurację następujących funkcji bezpieczeństwa:

- System zapobiegania włamaniom (IPS) z aktualizowanymi sygnaturami zagrożeń.
- Filtrowanie treści internetowych z możliwością definiowania wyjątków.
- Kontrola aplikacji (Application Control) z identyfikacją i blokowaniem niepożądanych aplikacji.
- System ochrony przed złośliwym oprogramowaniem.
- Ochrona przed atakami DDoS i zaawansowana detekcja anomalii.
- Filtrowanie ruchu DNS oraz blokowanie domen i adresów o złej reputacji.

Funkcje bezpieczeństwa muszą korzystać z aktualnych baz zagrożeń dostępnych online.

10. Inspekcja i deszyfracja ruchu SSL/TLS (SSL Inspection)

Konfiguracja systemu powinna obejmować wdrożenie inspekcji ruchu szyfrowanego SSL/TLS, w tym generowanie i dystrybucję certyfikatów inspekcyjnych.

Analiza powinna dotyczyć protokołów HTTPS,

System musi umożliwiać tworzenie list wyjątków (whitelist) dla usług i domen wyłączonych z inspekcji.

Proces deszyfrowania i ponownego szyfrowania ruchu powinien odbywać się bez wpływu na wydajność działania rozwiązania.

11. Połączenia VPN i zdalny dostęp

Wdrożenie powinno obejmować konfigurację połączeń VPN w standardach IPSec, SSL VPN oraz site-to-site VPN.

Konfiguracja musi zawierać polityki szyfrowania, algorytmy uwierzytelniania, listy kontroli dostępu oraz integrację z usługami katalogowymi.

Uwzględnione musi być uwierzytelnianie wieloskładnikowe (MFA) oraz portal użytkownika dla zestawiania połączeń zdalnych.

12. Integracja z systemami uwierzytelniania i monitorowania

Urządzenia powinny zostać zintegrowane z usługami.

13. Testy funkcjonalne i akceptacyjne

Po zakończeniu wdrożenia należy przeprowadzić testy potwierdzające poprawność konfiguracji klastra HA, inspekcji SSL, reguł bezpieczeństwa oraz połączeń VPN.

14. Dokumentacja powdrożeniowa

Dokumentacja powdrożeniowa powinna obejmować pełny opis konfiguracji urządzeń, reguł bezpieczeństwa, tuneli VPN, inspekcji SSL, topologii klastra i zasad utrzymania systemu.

15. Szkolenie administratorów

Szkolenie powinno obejmować obsługę, administrację systemem, zarządzanie politykami bezpieczeństwa, konfigurację VPN i inspekcji SSL oraz analizę zdarzeń bezpieczeństwa.

System NAC

Wymagania wdrożeniowe

1. Analiza środowiska i projekt architektury NAC

- Analiza istniejącej infrastruktury sieciowej, obejmująca przełączniki, punkty dostępowe oraz kontrolery, a także wykorzystywane usługi katalogowe i systemy uwierzytelniania.
- Identyfikacja kategorii użytkowników i urządzeń (stacje robocze, laptopy, urządzenia mobilne, urządzenia IoT, serwery administracyjne), które mają zostać objęte kontrolą NAC.
- Określenie polityk dostępu, w tym: kto i jakie urządzenia mogą mieć dostęp do określonych zasobów, przy jakich warunkach (lokalizacja, typ urządzenia, stan zabezpieczeń, czas).
- Opracowanie architektury systemu NAC z uwzględnieniem mechanizmów wysokiej dostępności (HA) oraz redundancji połączeń i komponentów.

2. Przygotowanie listy kontrolnej i segmentacji

- Przygotowanie listy urządzeń i segmentów sieci, które będą monitorowane i zarządzane przez system NAC (sieć przewodowa, sieć bezprzewodowa, sieć gościnna, sieci serwerowe, sieci użytkowników).
- Klasyfikacja urządzeń końcowych według typu oraz roli biznesowej, w celu przypisania właściwych polityk dostępowych i poziomów zaufania.
- Zaprojektowanie segmentacji logicznej (VLAN, ACL, polityki na przełącznikach i punktach dostępowych) powiązanej z decyzjami systemu NAC.

3. Architektura wysokiej dostępności NAC

- Zaplanowanie rozmieszczenia komponentów systemu NAC (węzły główne, zapasowe, serwery pomocnicze) w celu zapewnienia wysokiej dostępności.
- Przygotowanie konfiguracji redundancji, w tym:
 - nadmiarowych instancji systemu NAC,
 - redundantnych połączeń sieciowych do kluczowych urządzeń infrastruktury,
 - mechanizmów przełączania awaryjnego (failover) oraz równoważenia obciążenia.
- Przeprowadzenie testów odporności architektury na awarie wybranych elementów.

4. Instalacja i podstawowa konfiguracja systemu NAC

- Instalacja oprogramowania systemu NAC na wskazanych serwerach fizycznych lub wirtualnych, zgodnie z wymaganiami wydajnościowymi i bezpieczeństwa.
- Podstawowa konfiguracja systemu NAC, obejmująca:
 - integrację z domeną usług katalogowych,
 - uruchomienie mechanizmów wysokiej dostępności (HA),
 - konfigurację interfejsów sieciowych, stref czasowych, mechanizmów synchronizacji czasu oraz certyfikatów bezpieczeństwa,
 - utworzenie kont administracyjnych oraz ról uprawnień.

5. Integracja z infrastrukturą sieciową i systemami bezpieczeństwa

- Integracja systemu NAC z urządzeniami sieciowymi Zamawiającego (przełącznikami, , punktami dostępowymi Wi-Fi) w ramach funkcjonalności dostępnych na tych urządzeniach.
- Konfiguracja komunikacji z wykorzystaniem protokołów 802.1X, RADIUS, SNMP, identyfikacji po adresach MAC lub rozwiązań równoważnych, zgodnie z możliwościami środowiska.

- Konfiguracja posiadanego przez Zamawiającego urządzenia typu zaporę sieciową, w szczególności:
 - utworzenie i konfigurację VLAN-u gościnnego,
 - ustawienie odpowiednich polityk bezpieczeństwa, reguł dostępu i trasowania dla ruchu użytkowników objętych NAC.
- Integracja systemu NAC z usługą katalogową, serwerami RADIUS

6. Definiowanie i wdrożenie polityk NAC

- Zdefiniowanie polityk dostępu dla użytkowników i urządzeń, w tym:
 - warunków przyznania pełnego dostępu, dostępu ograniczonego lub kwarantanny,
 - przypisywania do odpowiednich VLAN-ów lub sieci gościnnej,
- Konfiguracja polityk dla sieci gościnnej (guest), w tym rozdziału tej sieci od zasobów wewnętrznych oraz możliwość krótkotrwałego, kontrolowanego dostępu.
- Utworzenie scenariuszy obsługi urządzeń niespełniających wymogów bezpieczeństwa (kwarantanna, ograniczony dostęp, blokada).

7. Import tożsamości i urządzeń końcowych

- Import tożsamości użytkowników z usług katalogowych oraz list dostarczonych przez Zamawiającego, w celu powiązania użytkowników z politykami NAC.
- Import listy urządzeń końcowych (adresy MAC, identyfikatory urządzeń) przekazanych przez Zamawiającego, z przypisaniem ich do odpowiednich kategorii oraz polityk dostępu.

8. Integracja urządzeń sieciowych z systemem NAC

- Konfiguracja urządzeń sieciowych Zamawiającego do współpracy z systemem NAC, z wykorzystaniem dostępnych funkcjonalności (np. tryby uwierzytelniania portów, dynamiczne przypisywanie VLAN-ów, ACL sterowane przez RADIUS).
- Wdrożenie konfiguracji na wybranych przełącznikach i punktach dostępowych w sposób kontrolowany, z wcześniejszym przetestowaniem ustawień na wydzielonym fragmencie sieci.

9. Uruchomienie mechanizmów uwierzytelniania i testy

- Uruchomienie uwierzytelniania w oparciu o 802.1X na 10 wybranych urządzeniach końcowych, wraz z przeprowadzeniem testów poprawności działania, logowania użytkowników i przypisywania polityk.
- Uruchomienie uwierzytelniania w oparciu o adres MAC na 10 urządzeniach końcowych, wraz z testami poprawności rozpoznawania urządzeń, przypisania VLAN-ów i egzekwowania polityk.
- Weryfikacja działania systemu w scenariuszach: urządzenie zgodne z polityką, urządzenie nieznane, urządzenie niespełniające wymagań bezpieczeństwa.

10. Testy funkcjonalne i bezpieczeństwa systemu NAC

- Przeprowadzenie kompleksowych testów obejmujących:
 - proces uwierzytelniania i autoryzacji użytkowników w sieci przewodowej i bezprzewodowej,
 - poprawność przypisania urządzeń do segmentów sieci zgodnie z politykami,
 - działanie mechanizmów wysokiej dostępności oraz zachowanie ciągłości usług przy awarii wybranych komponentów.

11. Dokumentacja powdrożeniowa

- Przygotowanie dokumentacji powykonawczej opisującej:
 - architekturę wdrożonego systemu NAC,
 - konfigurację serwerów NAC, integracji z domeną, RADIUS, zaporą sieciową i urządzeniami sieciowymi,
 - zastosowane polityki dostępu oraz scenariusze obsługi urządzeń,

- o sposób konfiguracji poszczególnych urządzeń sieciowych i systemów współpracujących,
- o procedury administracyjne, operacyjne i awaryjne.

12. Instruktaż administratorów

- Przeprowadzenie instruktażu dla administratorów sieci i bezpieczeństwa, obejmującego:
 - o obsługę konsoli zarządzającej systemu NAC,
 - o tworzenie i modyfikację polityk dostępowych,
 - o zarządzanie integracjami z urządzeniami sieciowymi i usługami katalogowymi,
 - o analizę logów i raportów oraz reagowanie na incydenty.

System kopii zapasowej

Wymagania wdrożeniowe

1. Analiza środowiska i przygotowanie architektury

- Analiza środowiska serwerowego i wirtualnego, obejmująca: platformy wirtualizacyjne, serwery fizyczne, macierze, urządzenia NAS oraz wymagania dotyczące ochrony danych (RPO/RTO, wolumen danych, okna backupowe).
- Określenie źródeł danych do ochrony (maszyny wirtualne, serwery fizyczne, udziału plikowe, zasoby w chmurze) oraz lokalizacji repozytoriów kopii zapasowych (lokalne, NAS, lokalizacja zdalna, chmura).
- Zaprojektowanie architektury systemu z uwzględnieniem komponentów zarządzających, transportujących dane i repozytoriów kopii.

2. Instalacja i konfiguracja komponentów systemu kopii zapasowych

- Instalacja centralnego komponentu zarządzającego na wybranym serwerze fizycznym, wirtualnym lub urządzeniu NAS, zgodnie z wymaganiami wydajnościowymi.
- Instalacja komponentów odpowiedzialnych za transfer danych (tzw. transporterów lub równoważnych) w lokalizacjach źródłowych i docelowych, zapewniających przetwarzanie danych backupowych, kompresję, szyfrowanie i optymalizację transmisji.
- Utworzenie i konfiguracja repozytoriów kopii zapasowych (lokalne, na urządzeniach NAS, w lokalizacji zdalnej lub w chmurze), z uwzględnieniem deduplikacji, kompresji oraz – tam gdzie możliwe – niezmienności (immutability) kopii.

3. Konfiguracja zadań backupowych i polityk retencji

- Utworzenie zadań kopii zapasowych dla:
 - o środowisk wirtualnych (obrazowe kopie maszyn wirtualnych z wykorzystaniem mechanizmów śledzenia zmian bloków lub równoważnych),
 - o serwerów fizycznych (backup na poziomie systemu/obrazu lub wybranych wolumenów),
 - o udziałów plikowych i zasobów NAS,
 - o wybranych usług chmurowych i usług SaaS, jeśli przewidziano w zakresie.
- Konfiguracja typów kopii zapasowych: pełnych, przyrostowych oraz syntetycznych pełnych lub równoważnych, w zależności od przyjętej strategii.
- Zdefiniowanie polityk retencji (okresy przechowywania, liczba punktów przywracania, reguły rotacji) dla poszczególnych klas danych, zgodnie z wymaganiami Zamawiającego i zasadą 3-2-1 lub równoważną.

4. Konfiguracja zabezpieczeń i odporności na incydenty

- Włączenie szyfrowania danych w transzycie oraz – tam gdzie dostępne – w spoczynku, dla repozytoriów lokalnych i zdalnych.

- Wdrożenie mechanizmów niezmienności kopii zapasowych (immutable backups) w wybranych repozytoriach, w celu ochrony przed szyfrowaniem lub usuwaniem przez złośliwe oprogramowanie.

5. Odmieszczenie kopii zapasowych i replikacja

- Przygotowanie i uruchomienie mechanizmów kopiowania danych backupowych do lokalizacji zewnętrznej (off-site), np. do drugiej serwerowni, zdalnego urządzenia NAS lub repozytorium w chmurze.
- Konfiguracja zadań kopiowania backupów lub replikacji, w tym harmonogramów, okien czasowych oraz limitów przepustowości, ze szczególnym uwzględnieniem łączności o niższej przepustowości (WAN/slow LAN).
- Weryfikacja poprawności przenoszenia kopii off-site oraz integralności danych po stronie lokalizacji zapasowej.

6. Testy odtwarzania i weryfikacji kopii

- Konfiguracja automatycznej weryfikacji poprawności tworzonych kopii, np. poprzez testowe uruchamianie maszyn wirtualnych lub równoważne mechanizmy weryfikacji.
- Przeprowadzenie testów odtworzeniowych obejmujących:
 - odtworzenie całej maszyny wirtualnej,
 - odtworzenie wybranych plików i obiektów aplikacyjnych (np. elementy systemów pocztowych, katalogowych, bazodanowych),
 - scenariusz awaryjnego odtworzenia usług w alternatywnej lokalizacji.

7. Dokumentacja powdrożeniowa

- Opracowanie dokumentacji obejmującej:
 - architekturę wdrożonego systemu (komponenty zarządzające, transportowe, repozytoria),
 - konfigurację zadań backupowych i polityk retencji,
 - opis procesów odmięscowienia kopii i replikacji,
 - procedury wykonywania kopii ręcznych oraz odtwarzania danych,
 - zalecenia dotyczące monitorowania, aktualizacji i rozbudowy systemu.

8. Instruktaż administratorów

- Przeprowadzenie instruktażu dla administratorów środowiska IT, w zakresie:
 - obsługi konsoli zarządzającej systemem kopii zapasowych,
 - konfiguracji i modyfikacji zadań backupowych oraz polityk retencji,
 - uruchamiania procedur odtwarzania (pełnego i granularnego),
 - monitorowania stanu zadań i interpretacji raportów oraz logów.

Segmentacja sieci podział na VLAN-y

Wymagania wdrożeniowe

1. Audyt i analiza istniejącej infrastruktury

- Przeprowadzenie audytu obecnej infrastruktury sieciowej LAN, obejmującego identyfikację wszystkich aktywnych urządzeń sieciowych, punktów dystrybucyjnych oraz urządzeń końcowych.
- Zebranie danych konfiguracyjnych z przełączników i urządzeń brzegowych, w tym zrzutów konfiguracji, aktualnych schematów VLAN, zidentyfikowanych portów typu trunk/uplink oraz obowiązującej adresacji IP.
- Opracowanie mapy logiczno-fizycznej sieci LAN uwzględniającej aktualną topologię oraz planowane zmiany wynikające z wdrożenia segmentacji i zwiększenia przepustowości szkieletu.

2. Projekt segmentacji sieci i szkieletu 10 Gb/s

- Zaprojektowanie szczegółowego planu segmentacji sieci z wykorzystaniem technologii VLAN, obejmującego:
 - rozdzielenie ruchu pomiędzy różnymi strefami funkcjonalnymi i bezpieczeństwa (np. środowisko wirtualne, serwery, użytkownicy biurowi, systemy krytyczne, strefa gościnna),
 - przypisanie identyfikatorów VLAN (VLAN ID), zakresów adresów IP, adresów bram domyślnych oraz wstępnych polityk dostępowych.
- Zaprojektowanie szkieletu sieci umożliwiającego komunikację pomiędzy punktami dystrybucyjnymi z docelową przepustowością 10 Gb/s, z wykorzystaniem posiadanych przez Zamawiającego łączy światłowodowych, o ile parametry techniczne istniejącej infrastruktury na to pozwalają, oraz z przygotowaniem konfiguracji uplinków/przełączników umożliwiającą osiągnięcie tej przepustowości w przypadku późniejszej rozbudowy lub modernizacji okablowania.
- Przygotowanie projektu przedwdrożeniowego zawierającego:
 - mapę VLAN i przypisania do urządzeń oraz portów,
 - strukturę routingu między VLAN,
 - wytyczne do konfiguracji urządzeń zabezpieczających oraz przełączników.
- Przekazanie projektu do zatwierdzenia przez Zamawiającego wraz z możliwością wniesienia uwag oraz ich uwzględnieniem przed realizacją prac konfiguracyjnych.

3. Rekonfiguracja przełączników warstwy 2

- Przypisanie portów przełączników warstwy 2 do odpowiednich VLAN (porty typu access i trunk) zgodnie z zatwierdzonym projektem segmentacji.
- Konfiguracja i uruchomienie uplinków 10 Gb/s pomiędzy przełącznikami rdzeniowymi a punktami dystrybucyjnymi, z wykorzystaniem światłowodów posiadanych przez Zamawiającego i odpowiednich modułów transmisyjnych.
- Konfiguracja mechanizmów bezpieczeństwa i stabilności, w tym:
 - SpanningTree (np. RSTP/MSTP lub rozwiązanie równoważne),
 - ochrony przed pętlami (loopprotection),
 - SNMP do monitorowania,
 - DHCP Snooping lub równoważnego w celu ochrony przed nieautoryzowanymi serwerami DHCP.
- Wykonanie aktualizacji oprogramowania urządzeń do rekomendowanych wersji zapewniających stabilność i bezpieczeństwo.
- Integracja z systemem kontroli dostępu do sieci (NAC), w tym konfiguracja dynamicznej zmiany VLAN oraz utworzenie polityk ACL powiązanych z decyzjami systemu NAC.
- Wprowadzenie czytelnego opisu portów na przełącznikach (opis lokalizacji, przeznaczenia i obsługiwanego VLAN oraz prędkości uplinku).

5. Konfiguracja usług adresacji i obsługi urządzeń końcowych

- Utworzenie puli adresacji dynamicznej na serwerze DHCP dla każdej nowo wydzielonej podsieci, wraz z ewentualnymi rezerwacjami adresów dla kluczowych urządzeń.
- Indywidualne podejście do urządzeń końcowych podczas zmian adresów IP, obejmujące:
 - przygotowanie planu migracji adresacji,
 - rekonfigurację urządzeń o adresach statycznych,
 - minimalizację przestojów i zapewnienie ciągłości pracy użytkowników oraz usług.

6. Testy segmentacji, szkieletu 10 Gb/s i polityk bezpieczeństwa

- Test komunikacji między VLAN zgodnie z założonymi regułami – zapewnienie pełnej separacji ruchu pomiędzy wydzielonymi strefami tam, gdzie jest to wymagane, oraz dostępności usług tam, gdzie przewidziano komunikację.
- Testy przepustowości i stabilności połączeń szkieletowych 10 Gb/s pomiędzy punktami dystrybucyjnymi, z wykorzystaniem istniejących łączy światłowodowych Zamawiającego.
- Weryfikacja poprawności działania routingu oraz serwisu adresacji (DHCP) w każdej z wydzielonych podsieci.
- Weryfikacja polityk bezpieczeństwa na urządzeniach zabezpieczających, w tym:
 - kontroli aplikacji,
 - inspekcji pakietów,
 - segmentacji stref bezpieczeństwa,
 - polityk głębokiej inspekcji ruchu, ochrony antywirusowej, systemu IPS oraz filtrowania treści.

7. Dokumentacja powdrożeniowa

- Opracowanie pełnej dokumentacji powdrożeniowej zawierającej:
 - aktualne konfiguracje urządzeń (przełączniki L2/L3, urządzenia zabezpieczające),
 - końcową mapę sieci VLAN wraz z opisem stref bezpieczeństwa,
 - zestawienie adresacji IP, rezerwacji DHCP oraz przypisań portów,
 - dokumentację dostępu administracyjnego (kont, ról oraz sposobu autoryzacji),
 - opis konfiguracji połączeń szkieletowych 10 Gb/s

8. Szkolenie techniczne administratorów

- Przeprowadzenie szkolenia technicznego (transferu wiedzy) dla administratorów Zamawiającego w zakresie:
 - zarządzania VLAN na przełącznikach,
 - administracji urządzeniami zabezpieczającymi,
 - modyfikacji reguł międzysegmentowych i polityk bezpieczeństwa,
 - diagnozowania i rozwiązywania problemów sieciowych związanych z segmentacją oraz szkieletowymi połączeniami 10 Gb/s.

Testy powdrożeniowe

Po dokonaniu całości wdrożenia należy:

- a) przeprowadzić testy poprawności działania całej infrastruktury
- b) przygotować dokumentację powykonawczą zawierającą listę dostarczonego sprzętu wraz z numerami seryjnymi i opisem konfiguracji poszczególnych elementów systemów
- c) Ze względu na krytyczne aplikacje które będą dostępne z sieci publicznej, Wykonawca przeprowadzi testy podatności systemów (testy penetracyjne). Testy będą polegały na zdalnej enumeracji otwartych portów oraz weryfikacji bezpieczeństwa oprogramowania na nich nasłuchującego. Skanowanie obejmie:

- urządzenia dedykowane (embedded), na przykład routery i przełączniki;
- punkty styku z sieciami obcymi
- zbadanie podatności systemów Zamawiającego na ataki przeprowadzane z zewnątrz
- Ponadto Wykonawca przeprowadzi badanie bezpieczeństwa sieci systemów komputerowych, które pozwoli na:
 - określenie błędów w konfiguracji skutkujących powstaniem podatności na atak;
 - wskazanie nadmiernych uprawnień, niezgodnych z zasadami dobrych praktyk;
 - Badaniu będą podlegały następujące systemy:

- ✓ rodzina Microsoft Windows Server (do poziomu weryfikacji poprawek Windows Update włącznie);
- ✓ Linux 2.4.x, 2.6.x, 3.x.x;
- ✓ IBM AIX;
- ✓ CISCO IOS;
- ✓ Microsoft SQL;
- ✓ MySQL;

Badanie zostanie zakończone raportem. Forma i zakres raportu musi być zaakceptowany przez dział informatyki Zamawiającego przed zakończeniem projektu.

18. UPS rackowy do podtrzymania i wygaszenia maszyn w momencie awarii (3 szt.)

PARAMETRY \ TYP	Wymagania minimalne
Moc wyjściowa (pozorna)	minimum 3000 VA
Moc wyjściowa (czynna)	minimum 3000 W
DANE OGÓLNE I ŚRODOWISKOWE	
Topologia	VI (lineinteractive)
Typ obudowy	Rack / Tower
Chłodzenie	Wymuszone, wewnętrzne wentylatory
WEJŚCIE	
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wejściowego (wartości skuteczne) i tolerancja	178 ÷ 281 V AC ± 2 %
Częstotliwość znamionowa napięcia wejściowego	50 Hz
Zakres częstotliwości i tolerancja	45 ÷ 55 Hz ± 1 Hz
Progi przełączania: sieć – UPS	178 ÷ 281 V AC ± 2 %
WYJŚCIE	
Napięcie znamionowe (wartość skuteczna)	230 V AC
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca sieciowa	195 ÷ 253 V AC ± 2 %
Zakres napięcia wyjściowego (wartości skuteczne) i tolerancja – praca rezerwowa	230 V AC ± 5 %
Automatyczna regulacja napięcia (AVR)	± 10 %
Kształt napięcia wyjściowego (przy pracy rezerwowej / sieciowej)	Sinusoidalny / Tak jak na wejściu
Częstotliwość znamionowa napięcia wyjściowego	50 Hz
Filtracja napięcia wyjściowego	Filtr przeciwzakłóceńowy RFI/EMI, tłumik warystorowy
Progi przełączania: UPS – sieć	183 ÷ 276 V AC ± 2 %
Czas przełączenia na pracę rezerwową	< 3 ms
Czas powrotu na pracę sieciową	0 ms
Przeciążalność	> 105% - 15 s (wyłączenie UPS)
AKUMULATORY I CZASY PODTRZYMANIA	
Akumulatory wewnętrzne	minimum 8 x 12 V / 7 Ah VRLA

Możliwość podłączenia zewnętrznego modułu bateryjnego	wymagane minimum 1szt.
Czas podtrzymania tylko z baterii wewnętrznych (100 % / 80 % / 50 % Pmax)	minimum 3 / 4 / 7min
Maksymalny czas ładowania baterii wewnętrznych UPS do 90% pojemności baterii - po uprzednim rozładowaniu obciążeniem równym 80% Pmax (do wyłączenia się zasilacza).	do 4 h
PARAMETRY MECHANICZNE	
Masa zasilacza	nie większa niż 45 kg
ZABEZPIECZENIA	
Zabezpieczenie wejściowe	Przeciwwzwarciowe – Bezpiecznik automatyczny 16 A / 250 V AC
	Przeciwpzepięciowe
Zabezpieczenie wyjściowe	Elektroniczne – przeciwwzwarciowe i przeciążeniowe
Zabezpieczenia wejścia DC (akumulatory wewnętrzne)	Zabezpieczenie nadprądowe
Zabezpieczenia DC (zewnętrzny moduł baterijny)	Zabezpieczenie nadprądowe
WYPOSAŻENIE I FUNKCJE DODATKOWE	
Przyłącza wyjściowe (liczba i typ gniazd)	minimum 3 x IEC320 C13 (10 A) - sterowalne
	minimum 3 x IEC320 C13 (10 A) - niesterowalne
	minimum 1 x IEC320 C19 (16 A)
	minimum 2 x PL (z bolcem uziemiającym)
Sygnalizacja	Akustycznie – optyczna; graficzny wyświetlacz LCD,
Interfejsy komunikacyjne	USB HID, SNMP/HTTP
Gniazdo na dodatkowe karty rozszerzeń	wymagane minimum 1 wolne gniazdo
Wsporniki do montażu w szafie RACK	wymagane na wyposażeniu
Oprogramowanie monitorująco-zarządzające	oprogramowanie w języku polskim tego samego producenta co UPS do zarządzania i monitorowania pracy UPS .
	możliwość zdalnego włączenia / wyłączenia UPSa (poprzez SNMP)
	możliwość zdalnego wyłączenia zarządzanej sekcji gniazd
	możliwość edycji nazw urządzeń na liście monitorowanych UPSów
	wymagane wsparcie producenta (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
	wsparcie dla systemów Linux, Windows oraz wirtualizacji Hyper-V, Vmware, XenServer
Możliwość aktualizacji oprogramowania firmware przez użytkownika	wymagane
Możliwość ustawienie minimalnego stopnia naładowania akumulatorów, przy którym zasilacz uruchomi się po rozładowaniu akumulatorów i powrocie	wymagane

napięcia sieciowego	
	Zasilacz wyprodukowany w Polsce / na terenie UE
GWARANCJA / SERWIS	
Gwarancja	min 36 miesięcy na elektronikę i 24 miesiące na akumulatory;
Serwis	autoryzowany serwis producenta zlokalizowany w Polsce.

Wycena szczegółowa:

Zakres rzeczowy	ilość	Cena netto	Wartość netto	Wartość VAT	Wartość brutto
Repozytorium danych dla środowiska wirtualnego – macierz dyskowa jako magazyn dla maszyn wirtualnych	1				
Serwery klastra wysokiej dostępności (2 szt.)	2				
Komputery dla administracji i obsługi środowiska wirtualnego – stacje robocze dla personelu odpowiedzialnego za zarządzanie i utrzymanie infrastruktury IT szpitala, UPS do komputera (20 szt.)	20				
Niezależny system backupu - serwer wraz z biblioteką taśmową, oprogramowaniem backupowym oraz urządzeniem typu NAS	1				
UPS rackowy do podtrzymania i wygaszenia maszyn w momencie awarii (3 szt.)	3				
System zarządzania urządzeniami końcowymi – centralna kontrola nad infrastrukturą IT, monitoring stacji roboczych i serwerów, wsparcie dla bezpieczeństwa środowiska IT	1				
Switch warstwy rdzeniowej (2 szt.)	2				
System NAC (kontrola dostępu do sieci) – zapewnienie bezpieczeństwa sieci poprzez segmentację, autoryzację urządzeń i użytkowników, ochrona przed nieautoryzowanym dostępem	1				
Oprogramowanie do przechowywania logów z urządzeń sieciowo/serwerowych	1				
Oprogramowanie do monitoringu infrastruktury	1				

Pakiet ochrony antywirusowej – zabezpieczenie serwerów, maszyn wirtualnych oraz urządzeń końcowych przed zagrożeniami malware, ransomware i innymi atakami	1				
Segmentacja sieci i zwiększenie przepustowości – dostosowanie sieci LAN do wymagań środowiska wirtualnego, podział na strefy bezpieczeństwa, podniesienie przepustowości łącza, rewitalizacja punktów dystrybucyjnych	1				
Szkolenia w zakresie dostarczonego sprzętu oraz technologii	1				
Wdrożenie infrastruktury IT – instalacja i konfiguracja klastra wirtualnego, usług katalogowych (AD), backupu, systemów bezpieczeństwa i segmentacji sieci	1				
Zakup małych switchy dostępowych w celu eliminacji obecnie pracujących urządzeń bez wsparcia (mini switchy) (10 szt.)	10				
Zintegrowana zapora sieciowa UTM – ochrona środowiska wirtualnego i systemów szpitala przed zagrożeniami z sieci publicznej, zarządzanie politykami bezpieczeństwa	1				
Switchy dostępne – rozbudowa infrastruktury LAN, zapewniająca bezpieczny dostęp do środowiska wirtualnego i usług IT dla użytkowników (10 szt.)					
System ochrony poczty elektronicznej zapewniający zaawansowane filtrowanie spamu, ochronę przed phishingiem, malware oraz złośliwymi załącznikami, archiwizacja	1				
RAZEM					