**Załącznik nr 1**

**Szczegółowy opis przedmiotu zamówienia**

 Gmina Wiejska Jarosław

Kwiecień 2024

Spis treści

[1. Wymagania ogólne dla urządzeń i oprogramowania sieciowego. 3](#_Toc164146402)

[2. Wymagania gwarancyjne. 3](#_Toc164146403)

[3. Miejsce instalacji sprzętu i oprogramowania/systemu. 3](#_Toc164146404)

[4. Zestawienie zakresu dostaw i usług. 4](#_Toc164146405)

[5. Szczegółów opis pozycji. 7](#_Toc164146406)

[5.1. Serwer z oprogramowaniem – szt. 1 – wymagania minimalne 7](#_Toc164146407)

[5.2. Oprogramowanie bazy danych – szt. 1 - wymagania minimalne 9](#_Toc164146408)

[5.3. Oprogramowanie do backupu – szt. 1 – wymagania minimalne 13](#_Toc164146409)

[5.4. Firewall – szt. 2 – wymagania minimalne 17](#_Toc164146410)

[5.5. Centralny system logów – szt. 1 – wymagania minimalne 22](#_Toc164146411)

[5.6. Serwer backup – szt. 1 – wymagania minimalne 23](#_Toc164146412)

[5.7. Przełącznik sieci LAN Core – szt. 3 - wymagania minimalne 26](#_Toc164146413)

[5.8. Przełącznik sieci LAN IDF – szt. 2 - wymagania minimalne 28](#_Toc164146414)

[5.9. Serwerowy system operacyjny – szt. 3 – wymagania minimalne 30](#_Toc164146415)

[5.10. System Operacyjny CAL – szt. 70 - wymagania minimalne 32](#_Toc164146416)

[5.11. System EDR-XDR – szt. 90 – wymagania minimalne 32](#_Toc164146417)

[5.12. System NAC – szt. 1 – wymagania minimalne 37](#_Toc164146418)

[5.13. Punkt dostępowy sieci WIFI Access Point – szt. 1 – wymagania minimalne 42](#_Toc164146419)

[5.14. UPS – szt. 1 – wymagania minimalne 43](#_Toc164146420)

[5.15. Agregat – szt. 1 – wymagania minimalne 45](#_Toc164146421)

[5.16. Instalacja, konfiguracja, wdrożenie, utrzymanie – szt. 1 – wymagania minimalne 47](#_Toc164146422)

## Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

* całość sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów;
* całość sprzętu musi być nowa (wyprodukowana nie wcześniej niż 6 miesięcy przed dostawą), nie używana wcześniej;

## Wymagania gwarancyjne.

**Sprzęt**

* o ile wymagania szczegółowe nie specyfikują inaczej, na dostarczany sprzęt musi być udzielona gwarancja oparta na gwarancji producenta rozwiązanie; serwis gwarancyjny świadczony ma być w miejscu instalacji sprzętu; czas reakcji na zgłoszony problem (rozumiany jako podjęcie działań diagnostycznych i kontakt ze zgłaszającym) nie może przekroczyć jednego dnia roboczego;
* Wykonawca ma obowiązek przyjmowania zgłoszeń serwisowych przez telefon (w godzinach pracy Wnioskodawcy), fax, e-mail lub WWW (przez całą dobę); Wykonawca ma udostępnić pojedynczy punkt przyjmowania zgłoszeń dla dostarczanych rozwiązań. Każde zgłoszenie należy potwierdzić drogą pisemną lub elektroniczną w postaci potwierdzenia przyjęcia zgłoszenia;
* Gwarantowany czas naprawy nie może być dłuższy niż 10 dni roboczych. W przypadku sprzętu, dla którego jest wymagany dłuższy czas na naprawę sprzętu, Zamawiający wymaga podstawienia na czas naprawy Sprzętu o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 31 dni roboczych od momentu zgłoszenia usterki;
* Zamawiający otrzyma dostęp do pomocy technicznej (telefon, e-mail lub WWW) w zakresie rozwiązywania problemów związanych z bieżącą eksploatacją dostarczonych rozwiązań w godzinach pracy Wnioskodawcy;
* wszystkie dostarczane moduły muszą pochodzić od producenta urządzeń i być objęte serwisem gwarancyjnym opartym na świadczeniach producenta sprzętu;

**Oprogramowanie**

* oprogramowanie powinno posiadać gwarancję obejmującą swoim zakresem poprawność działania w zakresie wdrożonych funkcjonalności wg stanu na dzień podpisania stosownego protokołu odbioru (chyba że zapisy szczegółowe stanowią inaczej);

UWAGA. Powyższe zapisy gwarancyjne znajdują zastosowanie w każdym przypadku i podlegają modyfikacji o uregulowania szczególne znajdujące w dalszej części SOPZ.

## Miejsce instalacji sprzętu i oprogramowania/systemu.

* Dostarczony sprzęt i oprogramowanie powinny zostać zamontowane, zainstalowane i skonfigurowane zgodnie z wymaganiami opisanymi w dalszej części dokumentu, w budynkach urzędu lub budynkach jednostek podległych, w miejscach wskazanych przez Zamawiającego.

## Zestawienie zakresu dostaw i usług.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa** | **Wymagana minimalna długość gwarancji (m-ce)** | **Ilość** | **Jednostka miary** | **Uwagi** |
|  | Serwer z oprogramowaniem | 36 | 1 | Szt. | Pozycja dotyczy stworzenie klastra niezawodnościowego HA, chmury prywatnej z dwóch fizycznych serwerów.  |
|  | Oprogramowanie bazy danych | Nd. | 1 | Szt. | Silnik bazy do przechowywania i gromadzenia danych z systemu zarządzania infrastrukturą IT oraz zapisu konfiguracji i parametryzacji urządzeń sieciowych w tym logów systemowych element składowy, systemów cyberbezpieczeństwa. |
|  | Oprogramowanie do backupu | 24 | 1 | Szt. | Na dedykowanym serwerze zostanie zainstalowane oprogramowanie do backupu i archiwizacji danych. System zostanie podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych. Miejscem przechowywania danych backupu będą dyski serwer. Połowa zasobów zostanie wykorzystana do przechowywanych plików off-line. Natomiast druga część zasobu zostanie wykorzystana do wykonywania replikacji asynchronicznej on-lina maszyn wirtualnych na lokalna platformę wirtualizacyjną na serwerze backupu. |
|  | Firewall  | 24 | 2 | Szt. | Pozycja dotyczy stworzenie klastra firewall, który  zabezpieczy punkt styku z Internetem, będzie terminował połączenia VPN z lokalizacji zdalnych, zapewni dostęp do zasobów sieciowych zgromadzonych w oprogramowani dziedzinowym oraz modułach świadczących e-usługi publiczne (wydzielenie sieci DMZ). Ruch z sieci VLAN zostanie zagregowany na tym urządzeniu. W ramach projektu zostaną opracowane polityki bezpieczeństwa dla ruchu sieciowego.  |
|  | Centralny system logów | 24 | 1 | Szt. | Pozycja pozwoli na zapisywanie i raportowanie zdarzeń w ruchu sieciowym z klastra firewall. |
|  | Serwer backup | 36 | 1 | Szt. | Pozycja dotyczy elementu systemu kopii zapasowych. Obecny system nie pozwala na łatwe odzyskanie środowiska produkcyjnego oraz na utrzymanie ciągłości pracy. Konieczne jest zatem stworzenie dedykowanego systemu odmiejscowionej kopii zapasowej pozwalającego na odtworzenie kompletnego systemu.  |
|  | Przełącznik sieci LAN CORE | Wieczysta (Live time) | 3 | Szt. | Urządzenia pozwolą na stworzenie rozległej sieci szkieletowej 10G. Będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI–L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokoły STP (protokół drzewa rozpinającego). Na przełącznikach zostanie zrealizowany mechanizm sieci wirtualnych VLAN (separacji ruchu sieciowego na warstwie L2 modelu ISO/OSI).   Przełączniki zostaną połączone pomiędzy sobą z wykorzystaniem portów 10G SFP (w tym druga lokalizacja dla odmiejscowionego backupu) do lokalizacji głównej. |
|  | Przełącznik sieci LAN IDF | Wieczysta (Live time) | 2 | Szt. |
|  | Serwerowy system operacyjny | Nd. | 3 | Szt. | Pozwoli na instalacje systemów NAC i EDR, dołączenie ich do centralnej bazy użytkowników - usługa katalogowa. Zapewni wykorzystanie mechanizmów kontroli dostępu do danych takich jak: uprawnienia użytkowników, grupy użytkowników i zarządzanie uprawnieniami, regularne aktualizacje oprogramowania dla systemów klienckich. |
|  | System operacyjny - CAL | Nd. | 70 | Szt. |
|  | System EDR-XDR | 24 | 90 | Szt. | Zakup pozwoli na zabezpieczenie punktów końcowych sieci. Będzie monitorował i gromadził dane z punktów końcowych sieci, a następnie używał tych informacji do wykrywania, badania i reagowania na różne zagrożenia bezpieczeństwa.  |
|  | System NAC | 24 | 1 | Szt. | Zakup pozwali na implementację protokołu 802.1x na przełącznikach sieci LAN i stacjach roboczych wraz integracją z usługa katalogową (domeną AD).  |
|  | Punktdostępowysieci WIFIAccess Point | 24 | 1 | Szt. | Punkty dostępowe sieci bezprzewodowej będą to urządzenia zarządzalne, pozwolą na rozszerzenie dostępu do sieci LAN i zapewnią bezpieczny do niej dostęp (Wireless Security) poprzez szyfrowanie transmisji danych oraz uwierzytelnienie użytkowników w centralnej bazie danych usługi katalogowej Active Director tak aby żadna nieupoważniona osoba nie mogła się połączyć. Punkty dostępowe będą ogłaszały kilka identyfikatorów sieci bezprzewodowych SSID z różnym poziomem dostępu do danych i przypisaną siecią VLAN. |
|  | UPS | 24 | 1 | Szt. | Urządzenia pozwolą na podłączenie zakupionych urządzeń w bezpieczny sposób do sieci elektrycznej zapewniając właściwe warunki pracy w momencie braku zasilania. Zwiększą poziom bezpieczeństwa przechowywanych danych, eliminując zagrożenie utarty danych w wyniku niewłaściwego, nagłego wyłączenia urządzeń. |
|  | Agregat | 24 | 1 | Szt. |
|  | Instalacja, konfiguracja, wdrożenie, utrzymanie | 24 | 1 | Szt. | Pozycja dotyczy pełnej instalacji i konfiguracji dostarczonych elementów projektu (sprzętowo-programowych) wraz z migracja danych, przeszkoleniem administratorów urzędu oraz zapewnieniem wsparcia powdrożeniowego na okres trwania projektu. |

## Szczegółów opis pozycji.

## Serwer z oprogramowaniem – szt. 1 – wymagania minimalne

|  |
| --- |
| **Obudowa*** Typu RACK, wysokość 2U;
* Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
* Możliwość zainstalowania 16 dysków twardych hot plug 2,5”;
* Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
* Zainstalowane 2 szt. dysków SSD 240GB skonfigurowane w RAID podpięte do sprzętowego kontrolera;
* Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;
* Możliwość zainstalowania dedykowanego wewnętrznego napędu blu-ray.
* Możliwość zainstalowania dedykowanego wewnętrznego napędu LTO-8.

**Płyta główna*** Dwuprocesorowa;
* Wyprodukowana i zaprojektowana przez producenta serwera;
* Możliwość instalacji procesorów 60-rdzeniowych;
* Zainstalowany moduł TPM 2.0;
* 6 złącz PCI Express generacji 5 w tym:
	+ 4 fizyczne złącza o prędkości x16;
	+ 2 fizyczne złącza o prędkości x8;
	+ Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
	+ Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
* 32 gniazda pamięci RAM;
* Obsługa minimum 8 TB pamięci RAM DDR5;
* Wsparcie dla technologii:
	+ Memory Scrubbing;
	+ SDDC;
	+ ECC;
	+ Memory Mirroring;
	+ ADDDC;
* Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  dyski nie mogą zajmować klatek dla dysków hot-plug.

**Procesory*** Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86\_64;
* Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 246 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany w konfiguracji dwuprocesorowej dla dowolnego producenta serwera na stronie <http://spec.org/cpu2017/results/cpu2017.html>.

**Pamięć RAM*** 256 GB pamięci RAM;
* DDR5 Registered 4800MT/s;
* Pamięci obsadzone w sposób gwarantujący najwyższa możliwość wydajność;

**Kontrolery LAN**Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:* 1x 1Gbit Base-T;
* 2x 10Gbit SFP+ obsadzone wkładkami MMF LC.
* Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

**Kontrolery I/O*** Kontroler FC 2 x 16Gb

**Porty*** Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
* 2 porty USB 3.0 wewnętrzne;
* 2 porty USB 3.0 dostępne z tyłu serwera;
* 2 porty USB 3.0 na panelu przednim;
* Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
* Ilość dostępnych złącz 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 900W;
* Redundantne wentylatory hotplug.

**Zarządzanie*** Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
	+ informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
		- karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express;
		- procesory CPU;
		- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
		- wbudowany na płycie głównej nośnik pamięci M.2 SSD;
		- status karty zarządzającej serwera;
		- wentylatory;
		- bateria podtrzymująca ustawienia BIOS płyty głównej;
		- zasilacze;
		- system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
* Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
	+ Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
	+ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	+ Dostęp poprzez przeglądarkę Web, SSH;
	+ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	+ Zarządzanie alarmami (zdarzenia poprzez SNMP);
	+ Możliwość przejęcia konsoli tekstowej;
	+ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
	+ Obsługa serwerów proxy (autentykacja);
	+ Obsługa VLAN;
	+ Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
	+ Wsparcie dla protokołu SSDP;
	+ Obsługa protokołów TLS 1.2, SSL v3;
	+ Obsługa protokołu LDAP;
	+ Integracja z HP SIM;
	+ Synchronizacja czasu poprzez protokół NTP;
	+ Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
* Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
* Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
* Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

**Wspierane OS*** Microsoft Windows Server 2022, 2019;
* VMWare vSphere 8.0;
* Suse Linux Enterprise Server 15;
* Red Hat Enterprise Linux 9, 8;
* Microsoft Hyper-V Server 2019.

**Gwarancja*** 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis.
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
* Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
* Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

**Dokumentacja, inne*** Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
* Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
* Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
* W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
* Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
* Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
* Zgodność z normami: CB, RoHS, WEEE  oraz CE.
 |

## Oprogramowanie bazy danych – szt. 1 - wymagania minimalne

|  |
| --- |
| System bazodanowy (SBD) typ I licencjonowany na rdzenie procesora musi spełniać następujące wymagania poprzez wbudowane mechanizmy:1. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do: definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL.
2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania.
3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem.
4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów.
5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania).
6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych.
7. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech:
* bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD),
* niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe),
* klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach,
1. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (*backup*) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych.
2. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych.
3. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory.
4. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw. Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność.
5. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń:
* odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system),
* wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur),
* para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy).
1. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci.
2. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków” obiektu, „rodzica” itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji.
3. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi:
* udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli,
* udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD,
* udostępniać język zapytań do struktur XML,
* udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML),
* udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań.
1. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności:
* zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów,
* oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,
* obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD,
* typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.).
1. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania.
2. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny.
3. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania.
4. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych.
5. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera.
6. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.:
* mechanizm debuggowania tworzonego rozwiązania,
* mechanizm stawiania „pułapek” (breakpoints),
* mechanizm logowania do pliku wykonywanych przez transformację operacji,
* możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu),
* możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)
* mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli),
* mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach),
* mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego,
* mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych.
1. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina.
2. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail).
3. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki).
4. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych.
5. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta).
6. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli.
7. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu.
8. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać:
* raporty parametryzowane,
* cache raportów (generacja raportów bez dostępu do źródła danych),
* cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów),
* współdzielenie predefiniowanych zapytań do źródeł danych,
* wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File),
* możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport,
* możliwość wizualizacji wskaźników KPI,
* możliwość wizualizacji danych w postaci obiektów sparkline.
1. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services).
2. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach.
3. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów.
4. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja).
5. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT.
6. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache’u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD.
7. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań.
8. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).

Licencje dostępowe:Wymaga się aby oferowane licencje dla systemu bazodanowego umożliwiały korzystanie z zasobów dla 10 użytkowników (10 licencji dostępowych). |

## Oprogramowanie do backupu – szt. 1 – wymagania minimalne

|  |
| --- |
| **Wymagania ogólne*** Minimalna ilość licencji musi umożliwiać backup środowiska wirtualnego z co najmniej dwóch serwerów 2-procesorowych obejmującego co najmniej 20 VM oraz 3 serwerach fizycznych.
* Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 oraz Microsoft Hyper-V 2008R2SP1, 2012, 2012 R2, 2019 i 2022. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej
* Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.
* Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.
* Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

**Całkowite koszty posiadania*** Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej
* Oprogramowanie musi tworzyć “samowystarczalne” archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków
* Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental)
* Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji
* Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.
* Oprogramowanie musi pozwalać na rozszerzenie lokalnej przestrzeni backupowej poprzez integrację z Microsoft Azure Blob, Amazon S3 oraz z innymi kompatybilnymi z S3 macierzami obiektowymi. Proces migracji danych powinien być zautomatyzowany. Jedynie unikalne bloki mogą być przesyłane w celu oszczędności pasma oraz przestrzeni na przechowywane dane. Funkcjonalność ta nie może mieć wpływu na możliwości odtwarzania danych.
* Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania
* Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.
* Oprogramowanie musi oferować portal samoobsługowy, umożliwiający odtwarzanie użytkownikom wirtualnych maszyn, obiektów MS Exchange i baz danych MS SQL oraz Oracle (w tym odtwarzanie point-in-time)
* Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji
* Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej. Włączenie szyfrowania nie może skutkować utratą jakiejkolwiek funkcjonalności wymienionej w tej specyfikacji
* Oprogramowanie musi posiadać mechanizmy chroniące przed utratą hasła szyfrowania
* Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX)
* Oprogramowanie musi posiadać architekturę klient/serwer z możliwością instalacji wielu instancji konsoli administracyjnych.

**Wymagania RPO*** Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej
* Oprogramowanie musi wykorzystywanać mechnizmy śledzenia zmienionych plików przy zabezpieczaniu udziałów plikowych.
* Oprogramowanie musi oferować możliwość sterowania obciążeniem storage'u produkcyjnego tak aby nie przekraczane były skonfigurowane przez administratora backupu poziomy latencji. Funkcjonalność ta musi być dostępna na wszystkich wspieranych platformach wirtualizacyjnych
* Oprogramowanie musi automatycznie wykrywać i usuwać snapshoty-sieroty (orphaned snapshots), które mogą zakłócić poprawne wykonanie backupu. Proces ten nie może wymagać interakcji administratora
* Oprogramowanie musi posiadać wsparcie dla VMware vSAN potwierdzone odpowiednią certyfikacją VMware.
* Oprogramowanie musi wspierać kopiowanie backupów na taśmy wraz z pełnym śledzeniem wirtualnych maszyn
* Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son)
* Oprogramowanie musi umieć korzystać z protokołu DDBOOST w przypadku, gdy repozytorium backupów jest umiejscowione na Dell EMC DataDomain. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi umieć korzystać z protokołu Catalyst (w tym Catalyst Copy) w przypadku, gdy repozytorium backupów jest umiejscowione na HPE StoreOnce. Funkcjonalność powinna wspierać łącze sieciowe lub FC.
* Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016, 2019 lub 2022 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.
* Repozytoria oparte o XFS muszą pozwalać na zmiezmienność danych przez określoną ilość czasu (tzw Immutability)
* Oprogramowanie musi mieć możliwość replikacji asynchronicznej włączonych wirtualnych maszyn bezpośrednio z infrastruktury VMware vSphere pomiędzy hostami ESXi oraz pomiędzy hostami Hyper-V. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.
* Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik
* Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding)
* Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN)

**Wymagania RTO*** Oprogramowanie musi umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage’u użytego do przechowywania kopii zapasowych.
* Dodatkowo dla środowiska vSphere i Hyper-V powyższa funkcjonalność powinna umożliwiać uruchomianie backupu z innych platform (inne wirtualizatory, maszyny fizyczne oraz chmura publiczna)
* Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami
* Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków
* Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny bezpośrednio do Microsoft Azure, Microsoft Azure Stack oraz Amazon EC2.
* Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików
* Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy VIX API dla platformy VMware i PowerShell Direct dla platformy Hyper-V.
* Oprogramowanie musi wspierać odtwarzanie pojedynczych plików z następujących systemów plików:
* Linux: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs
* BSD: UFS, UFS2
* Solaris: ZFS, UFS
* Mac: HFS, HFS+
* Windows: NTFS, FAT, FAT32, ReFS
* Novell OES: NSS
* Oprogramowanie musi wspierać przywracanie plików z partycji Linux LVM oraz Windows Storage Spaces.
* Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.
* Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.
* Oprogramowanie musi wspierać granularne odtwarzanie dowolnych atrybutów, rekordów DNS zintegrowanych z AD, Microsoft System Objects, certyfikatów CA oraz elementów AD Sites.
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Exchange 2010 i nowszych (dowolny obiekt w tym obiekty w folderze "Permanently Deleted Objects"),
* Oprogramowanie musi wspierać przywracanie danych Exchange do oryginalnego środowiska
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft SQL 2005 i nowszych
* Oprogramowanie musi wspierać odtworzenie point-in-time wraz z możliwością przywrócenia bazy do oryginalnego środowiska
* Oprogramowanie musi wspierać granularne odtwarzanie Microsoft Sharepoint 2010 i nowszych
* Oprogramowanie musi wspierać odtworzenia elementów, witryn, uprawnień dla witryn Sharepoint.
* Oprogramowanie musi wspierać granularne odtwarzanie baz danych Oracle z opcją odtwarzanie point-in-time wraz z włączonym Oracle DataGuard. Funkcjonalność ta musi być dostępna dla baz uruchomionych w środowiskach Windows oraz Linux.
* Oprogramowanie musi pozwalać na zaprezentowanie oraz migrację online baz MS SQL oraz Oracle bezpośrednio z pliku kopii zapasowej do działającego serwera bazodanowego
* Oprogramowanie musi wspierać także specyficzne metody odtwarzania w tym "reverse CBT" oraz odtwarzanie z wykorzystaniem sieci SAN

**Ograniczenie ryzyka*** Oprogramowanie musi dawać możliwość stworzenia laboratorium (izolowane środowisko) dla vSphere i Hyper-V używając wirtualnych maszyn uruchamianych bezpośrednio z plików backupu.
* Oprogramowanie musi umożliwiać weryfikację odtwarzalności wielu wirtualnych maszyn jednocześnie z dowolnego backupu według własnego harmonogramu w izolowanym środowisku. Testy powinny uwzględniać możliwość uruchomienia dowolnego skryptu testującego również aplikację uruchomioną na wirtualnej maszynie. Testy muszą być przeprowadzone bez interakcji z administratorem
* Oprogramowanie musi mieć podobne mechanizmy dla replik w środowisku vSphere
* Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, Symantec Protection Engine oraz ESET NOD32.
* Oprogramowanie musi umożliwiać dwuetapowe, automatyczne, odtwarzanie maszyn wirtualnych z możliwością wstrzyknięcia dowolnego skryptu przed odtworzeniem danych do środowiska produkcyjnego.

**Monitoring*** System musi zapewnić możliwość monitorowania środowiska wirtualizacyjnego opartego na VMware vSphere i Microsoft Hyper-V bez potrzeby korzystania z narzędzi firm trzecich
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego VMware w wersji 5.5, 6.0, 6.5, 6.7 and 7.0 – zarówno w bezpłatnej wersji ESXi jak i w pełnej wersji ESX/ESXi zarządzane przez konsole vCenter Server lub pracujące samodzielnie
* System musi umożliwiać monitorowanie środowiska wirtualizacyjnego Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022 zarówno w wersji darmowej jak i zawartej w płatnej licencji Microsoft Windows Server zarządzane poprzez System Center Virtual Machine Manager lub pracujące samodzielnie.
* System musi mieć status „VMware Ready” i być przetestowany i certyfikowany przez VMware
* System musi umożliwiać kategoryzacje obiektów infrastruktury wirtualnej niezależnie od hierarchii stworzonej w vCenter
* System musi umożliwiać tworzenie alarmów dla całych grup wirtualnych maszyn jak i pojedynczych wirtualnych maszyn
* System musi dawać możliwość układania terminarza raportów i wysyłania tych raportów przy pomocy poczty elektronicznej w formacie HTML oraz Excel
* System musi dawać możliwość podłączenia się do kilku instancji vCenter Server i serwerów Hyper-V jednocześnie, w celu centralnego monitorowania wielu środowisk
* System musi mieć wbudowane predefiniowane zestawy alarmów wraz z możliwością tworzenia własnych alarmów i zdarzeń przez administratora
* System musi mieć wbudowane połączenie z bazą wiedzy opisującą problemy z predefiniowanych alarmów
* System musi mieć centralną konsolę z sumarycznym podglądem wszystkich obiektów infrastruktury wirtualnej (ang. Dashboard)
* System musi mieć możliwość monitorowania platformy sprzętowej, na której jest zainstalowana infrastruktura wirtualna
* System musi zapewnić możliwość podłączenia się do wirtualnej maszyny (tryb konsoli) bezpośrednio z narzędzia monitorującego
* System musi mieć możliwość integracji z oprogramowaniem do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość monitorowania obciążenia serwerów backupowych, ilości zabezpieczanych danych oraz statusu zadań kopii zapasowych, replikacji oraz weryfikacji odzyskiwalności maszyn wirtualnych.
* System musi oferować inteligentną diagnostykę rozwiązania backupowego poprzez monitorowanie logów celem wykrycia znanych problemów oraz błędów konfiguracyjnych w celu wskazania rozwiązania bez potrzeby otwierania zgłoszenia suportowego oraz bez potrzeby wysyłania jakichkolwiek danych diagnostycznych do producenta oprogramowania backupu.
* System musi mieć możliwość granularnego monitorowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość monitorowania instancji VMware vCloud Director w wersji 9.x i 10.x

**Raportowanie*** System raportowania musi umożliwić tworzenie raportów z infrastruktury wirtualnej bazującej na VMware ESX/ESXi 5.5, 6.0, 6.5, 6.7 and 7.0 vCenter Server 5.x oraz 6.x jak również Microsoft Hyper-V 2008 R2 SP1, 2012, 2012 R2, 2016, 2019 oraz 2022
* System musi wspierać wiele instancji vCenter Server i Microsoft Hyper-V jednocześnie bez konieczności instalowania dodatkowych modułów.
* System musi być certyfikowany przez VMware i posiadać status „VMware Ready”
* System musi być systemem bezagentowym. Nie dopuszcza się możliwości instalowania przez system agentów na monitorowanych hostach ESXi i Hyper-V
* System musi mieć możliwość eksportowania raportów do formatów Microsoft Word, Microsoft Excel, Microsoft Visio, Adobe PDF
* System musi mieć możliwość ustawienia harmonogramu kolekcji danych z monitorowanych systemów jak również możliwość tworzenia zadań kolekcjonowania danych ad-hoc
* System musi mieć możliwość ustawienia harmonogramu generowania raportów i dostarczania ich do odbiorców w określonych przez administratora interwałach
* System w raportach musi mieć możliwość uwzględniania informacji o zmianach konfiguracji monitorowanych systemów
* System musi mieć możliwość generowania raportów z dowolnego punktu w czasie zakładając, że informacje z tego czasu nie zostały usunięte z bazy danych
* System musi posiadać predefiniowane szablony z możliwością tworzenia nowych jak i modyfikacji wbudowanych
* System musi mieć możliwość analizowania „przeszacowanych” wirtualnych maszyn wraz z sugestią zmian w celu optymalnego wykorzystania fizycznej infrastruktury
* System musi mieć możliwość generowania raportów na podstawie danych uzyskanych z oprogramowania do tworzenia kopii zapasowych tego samego producenta
* System musi mieć możliwość generowania raportu dotyczącego zabezpieczanych maszyn, zdefiniowanych zadań tworzenia kopii zapasowych oraz replikacji jak również wykorzystania zasobów serwerów backupowych.
* System musi mieć możliwość generowania raportu planowania pojemności (capacity planning) bazującego na scenariuszach ‘what-if’.
* System musi mieć możliwość granularnego raportowania infrastruktury, zależnego od uprawnień nadanym użytkownikom dla platformy VMware
* System musi mieć możliwość generowania raportów dotyczących tzw. migawek-sierot (orphaned snapshots)
* System musi mieć możliwość generowania personalizowanych raportów zawierających informacje z dowolnych predefiniowanych raportów w pojedynczym dokumencie
 |

## Firewall – szt. 2 – wymagania minimalne

|  |
| --- |
| Wymagania OgólneSystem bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.System wspiera protokoły IPv4 oraz IPv6 w zakresie:* Firewall.
* Ochrony w warstwie aplikacji.
* Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
* 16 portami Gigabit Ethernet RJ-45.
* 8 gniazdami SFP 1 Gbps.
* 4 gniazdami SFP+ 10 Gbps.
1. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
2. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
3. System realizujący funkcję Firewall jest wyposażony w lokalną przestrzeń dyskową o pojemności minimum 480 GB.
4. System jest wyposażony w zasilanie AC.
5. Parametry wydajnościowe:
6. W zakresie Firewall’a obsługa nie mniej niż 2.8 mln. jednoczesnych połączeń oraz 120 tys. nowych połączeń na sekundę.
7. Przepustowość Stateful Firewall: nie mniej niż 38 Gbps dla pakietów 512 B.
8. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 6.5 Gbps.
9. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 30 Gbps.
10. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 5 Gbps.
11. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 2.5 Gbps.
12. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 3 Gbps.

Funkcje Systemu Bezpieczeństwa:W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

Polityki, Firewall1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
* Translację jeden do jeden oraz jeden do wielu.
* Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
1. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
2. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
3. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
4. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
5. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
* Amazon Web Services (AWS).
* Microsoft Azure.
* Cisco ACI.
* Google Cloud Platform (GCP).
* OpenStack.
* VMware NSX.
* Kubernetes.

Połączenia VPN1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
* Wsparcie dla IKE v1 oraz v2.
* Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
* Obsługa protokołu Diffie-Hellman grup 19, 20.
* Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
* Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
* Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
* Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
* Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
* Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
* Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
* Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
* Mechanizm „Split tunneling” dla połączeń Client-to-Site.
1. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
* Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
* Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
* Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.

Routing i obsługa łączy WANW zakresie routingu rozwiązanie zapewnia obsługę:1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

Funkcje SD-WAN1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).

Zarządzanie pasmem1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

Ochrona przed atakami1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

Kontrola aplikacji1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

Kontrola WWW1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
* Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
* Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
* Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
1. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
2. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
3. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

Logowanie1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

Testy wydajnościowe oraz funkcjonalne1. Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

Serwisy i licencjeW ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:a)     Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen. Gwarancja oraz wsparcie1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Opisy do wymagań ogólnych1. Zaleca się, aby w przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), został uzyskany dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Zaleca się, aby został uzyskany dokument - oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż produkt pochodzi z autoryzowanego kanału sprzedaży, np. poprzez oświadczenie o posiadanym statusie autoryzacyjnym.
 |

## Centralny system logów – szt. 1 – wymagania minimalne

|  |
| --- |
| **Wymagania Ogólne**W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).**Interfejsy, Dysk:**1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 500 GB

Parametry wydajnościowe:1. System musi być w stanie przyjmować minimum 1 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:**Logowanie**1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.b. Listę najbardziej aktywnych użytkowników.c. Listę najczęściej wykorzystywanych aplikacji.d. Listę najczęściej odwiedzanych stron www.e. Listę krajów , do których nawiązywane są połączenia.f. Listę najczęściej wykorzystywanych polityk Firewall.g. Informacje o realizowanych połączeniach IPSec.1. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
2. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
3. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

**Raportowanie**W zakresie raportowania system musi zapewniać:1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

**Korelacja logów**W zakresie korelacji zdarzeń system musi zapewniać:1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
* Malware.
* Aplikacje sieciowe.
* Email.
* IPS.
* Traffic.
* Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

**Zarządzanie**1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.1. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy i licencje1. Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
 |

## Serwer backup – szt. 1 – wymagania minimalne

|  |
| --- |
| **Obudowa*** Typu RACK, wysokość 2U;
* Szyny umożliwiające wysunięcie serwera z szafy stelażowej;
* Możliwość zainstalowania 12 dysków twardych hot plug 3,5”;
* Zainstalowane fizyczne zabezpieczenie (np. na klucz lub elektrozamek) uniemożliwiające fizyczny dostęp do dysków twardych;
* Zainstalowane 2 szt. dysków SSD 1,92TB Hot-Plug DWPD>2
* Zainstalowane 10 szt. dysków SAS lub NL-SAS 12G 12TB Hot-Plug skonfigurowane w RAID podpięte do sprzętowego kontrolera;
* Możliwość zainstalowania dysku M.2 NVMe PCIe4.0 x4;

**Płyta główna*** Dwuprocesorowa;
* Wyprodukowana i zaprojektowana przez producenta serwera;
* Możliwość instalacji procesorów 60-rdzeniowych;
* Zainstalowany moduł TPM 2.0;
* 6 złącz PCI Express generacji 5 w tym:
	+ 4 fizyczne złącza o prędkości x16;
	+ 2 fizyczne złącza o prędkości x8;
	+ Opcjonalnie możliwość uzyskania 2 złącz typu pełnej wysokości;
	+ Opcjonalnie możliwość uzyskania 9 aktywnych interfejsów PCI-e;
* 32 gniazda pamięci RAM;
* Obsługa minimum 8 TB pamięci RAM DDR5;
* Wsparcie dla technologii:
	+ Memory Scrubbing;
	+ SDDC;
	+ ECC;
	+ Memory Mirroring;
	+ ADDDC;
* Możliwość instalacji 2 dysków M.2 na płycie głównej (lub dedykowanej karcie PCI Express)  dyski nie mogą zajmować klatek dla dysków hot-plug.

**Procesory*** Dwa procesory 8-rdzeniowe, taktowanie bazowe 2,6 GHz, architektura x86\_64;
* Osiągające w teście SPEC CPU2017 Floating Point wynik SPECrate2017\_fp\_base 246 pkt (wynik osiągnięty dla zainstalowanych dla dwóch procesorów). Wynik musi być opublikowany w konfiguracji dwuprocesorowej dla dowolnego producenta serwera na stronie <http://spec.org/cpu2017/results/cpu2017.html>.

**Pamięć RAM*** 256 GB pamięci RAM;
* DDR5 Registered 4800MT/s;

**Kontrolery LAN**Interfejsy LAN, nie zajmujące żadnego z dostępnych slotów PCI Express:* 1x 1Gbit Base-T;
* 2x 10Gbit SFP+, wszystkie porty obsadzone modułami MMF LC;
* Możliwość uzyskania dwóch interfejsów 100Gbit QSFP28 bez konieczności instalacji kart w slotach PCIe;

**Kontrolery I/O*** Kontroler SAS RAID dla dysków wewnętrznych posiadający 4GB pamięci cache, obsługujący poziomy RAID: 0,1,10,5,50,6,60 z podtrzymaniem pamięci cache w przypadku utraty zasilania;

**Porty*** Zintegrowana karta graficzna ze złączem VGA z tyłu serwera;
* 2 porty USB 3.0 wewnętrzne;
* 2 porty USB 3.0 dostępne z tyłu serwera;
* 2 porty USB 3.0 na panelu przednim;
* Opcjonalny port serial, możliwość wykorzystania portu serial do zarządzania serwerem;
* Ilość dostępnych złącz 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 900W;
* Redundantne wentylatory hotplug.

**Zarządzanie*** Wbudowane diody informacyjne lub wyświetlacz informujące o stanie serwera - system przewidywania, rozpoznawania awarii;
	+ informacja o statusie pracy (poprawny, przewidywana usterka lub usterka) następujących komponentów:
		- karty rozszerzeń zainstalowane w dowolnym  slocie PCI Express;
		- procesory CPU;
		- pamięć RAM z dokładnością umożliwiającą jednoznaczną identyfikację uszkodzonego modułu pamięci RAM;
		- wbudowany na płycie głównej nośnik pamięci M.2 SSD;
		- status karty zarządzającej serwera;
		- wentylatory;
		- bateria podtrzymująca ustawienia BIOS płyty głównej;
		- zasilacze;
		- system przewidywania/rozpoznawania awarii musi być niezależny i działać w przypadku odłączenia kabli zasilających serwera (podtrzymywany kondensatorowo lub bateryjnie w celu uruchomienia przy odłączonym zasilaniu sieciowym);
* Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:
	+ Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
	+ Dedykowana karta LAN 1 Gb/s, dedykowane złącze RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
	+ Dostęp poprzez przeglądarkę Web, SSH;
	+ Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii;
	+ Zarządzanie alarmami (zdarzenia poprzez SNMP);
	+ Możliwość przejęcia konsoli tekstowej;
	+ Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM);
	+ Obsługa serwerów proxy (autentykacja);
	+ Obsługa VLAN;
	+ Możliwość konfiguracji parametru Max. Transmission Unit (MTU);
	+ Wsparcie dla protokołu SSDP;
	+ Obsługa protokołów TLS 1.2, SSL v3;
	+ Obsługa protokołu LDAP;
	+ Integracja z HP SIM;
	+ Synchronizacja czasu poprzez protokół NTP;
	+ Możliwość backupu i odtwarzania ustawień bios serwera oraz ustawień karty zarządzającej;
* Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna);
* Dedykowana, do wbudowania w kartę zarządzającą (lub zainstalowana) pamięć flash o pojemności minimum 16 GB;
* Możliwość zdalnej reinstalacji systemu lub aplikacji z obrazów zainstalowanych w obrębie dedykowanej pamięci flash bez użytkowania zewnętrznych nośników lub kopiowania danych poprzez sieć LAN;
* Serwer posiada możliwość konfiguracji i wykonania aktualizacji BIOS, Firmware, sterowników serwera bezpośrednio z GUI (graficzny interfejs) karty zarządzającej serwera bez pośrednictwa innych nośników zewnętrznych i wewnętrznych poza obrębem karty zarządzającej.

**Wspierane OS*** Microsoft Windows Server 2022, 2019;
* VMWare vSphere 8.0;
* Suse Linux Enterprise Server 15;
* Red Hat Enterprise Linux 9, 8;
* Microsoft Hyper-V Server 2019.

**Gwarancja*** 3 lata gwarancji producenta serwera w trybie on-site z gwarantowaną skuteczną naprawą do końca następnego dnia od zgłoszenia. Naprawa realizowana przez producenta serwera lub autoryzowany przez producenta serwis. Dyski twarde nie podlegają zwrotowi organizacji serwisowej;
* Funkcja zgłaszania usterek i awarii sprzętowych poprzez automatyczne założenie zgłoszenia w systemie helpdesk/servicedesk producenta sprzętu;
* Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych;
* Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera – jeżeli funkcjonalność ta wymaga dodatkowego serwisu lub licencji producenta serwera, takowy element musi być uwzględniona w ofercie;
* Możliwość odpłatnego wydłużenia gwarancji producenta do 7 lat w trybie onsite z gwarantowanym skutecznym zakończeniem naprawy serwera najpóźniej w następnym dniu roboczym od zgłoszenia usterki (podać koszt na dzień składania oferty).

**Dokumentacja, inne*** Elementy, z których zbudowane są serwery muszą być produktami producenta tych serwerów lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA – wymagane oświadczenie wykonawcy lub producenta;
* Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE – wymagane oświadczenie wykonawcy lub producenta;
* Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera, w ofercie należy podać link do strony producenta na której znajduje się nr telefonu oraz maila na który można zgłaszać usterki;
* W czasie obowiązywania gwarancji na sprzęt, możliwość po podaniu na infolinii numeru seryjnego urządzenia weryfikacji pierwotnej konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;
* Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www producenta serwera;
* Możliwość pracy w pomieszczeniach o wilgotności w zawierającej się w przedziale 8 - 85 %;
* Zgodność z normami: CB, RoHS, WEEE  oraz CE.
 |

## Przełącznik sieci LAN Core – szt. 3 - wymagania minimalne

|  |
| --- |
| Przełącznik wielowarstwowy L2/L3, zarządzanyTyp i liczba portów: 12 portów 10GBaseT i 12 portów SFP+Porty SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:* Gigabit Ethernet 1000Base-SX
* Gigabit Ethernet 1000Base-LX/LH
* 10Gigabit Ethernet 10GBase-SR
* 10Gigabit Ethernet 10GBase-LR
* 10Gigabit Ethernet typu twinax

Port konsoli USB Type-B/RJ45Porty dostępowe przełącznika zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)Parametry wydajnościowe:* Przepustowość przełącznika (switching bandwidth) 238 Gb/s
* Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 320 Mpps
* Pamięć DRAM – 512 MB
* Pamięć flash – 256 MB
* Procesor wbudowany 1,3 GHz
* Wielkość bufora pakietów - 3 MB
* 4 000 grup IGMP
* 32 grupy połączeń zagregowanych typu „port channel” LACP
* 8 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP
* 2 000 wpisów w listach kontroli dostępu ACL
* 8 kolejek sprzętowych

Obsługa:* 4 096 aktywnych sieci VLAN
* 32 000 adresów MAC
* 7 100 statycznych tras IPv4
* 256 interfejsów L3

Obsługa ramek Ethernet Jumbo 9 000 BMożliwość łączenia do 8 jednostek w stos poprzez porty 10 GE, zarządzane jako jeden system z funkcją failover active/standbyFunkcjonalność cross-stack QoS, VLAN, LAG i port mirroringPrzełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:* IEEE 802.1w Rapid Spanning Tree
* Per-VLAN Rapid Spanning Tree (PVRST+)
* IEEE 802.1s Multi-Instance Spanning Tree
* Obsługa 126 instancji protokołu STP

Funkcje wirtualnej sieci LAN: Voice VLAN, Protocol based VLANObsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowegoProtokół rejestracji GARP VLAN (GVRP)Mechanizmy związane z bezpieczeństwem sieci:* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level)
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN
* Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X
* Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC
* Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X
* Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
* Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,\
* Obsługa HTTPS, SSH, SSL
* Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP)

Mechanizmy związane z zapewnieniem jakości usług w sieci:* Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi
* Implementacja algorytmu Weighted Round Robin dla obsługi kolejek
* Możliwość obsługi jednej z kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority)
* Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP
* Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi,
* Kontrola sztormów dla ruchu broadcast/multicast/unicast
* Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP

Obsługa standardów komunikacyjnych: IEEE 802.3 10BASE-T Ethernet, IEEE 802.3u 100BASE-TX Fast Ethernet, IEEE 802.3ab 1000BASE-T Gigabit Ethernet, IEEE 802.3ad Link Aggregation Control Protocol, IEEE 802.3z Gigabit Ethernet, IEEE 802.3ae 10 Gbit/s Ethernet over fiber for LAN, IEEE 802.3an 10GBase-T 10 Gbit/s Ethernet over copper twisted pair cable, IEEE 802.3x Flow Control, IEEE 802.1D (STP, GARP, and GVRP), IEEE 802.1Q/p VLAN, IEEE 802.1w Rapid STP, IEEE 802.1s Multiple STP, IEEE 802.1X Port Access Authentication, IEEE 802.1AB Link Layer Discovery Protocol, IEEE 802.3az Energy Efficient EthernetObsługa protokołu NTPFunkcje DHCP server, DHCP relayObsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snoopingBlokowanie Head of Line (HOL)Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)Zapobieganie atakom DoSObsługa mechanizmów routingu statycznego dla IPv4 i IPv6Routing dynamiczny RIP v2Zarządzanie* Port konsoli
* Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją
* Obsługa protokołów SNMPv3, SSHv2, https, syslog
* Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia
* Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki
* Obsługa protokołu LLDP i LLDP-MED

Obsługa funkcji Plug & PlayPrzycisk resetCertyfikaty: UL 60950, FCC 15 A, CSA 22.2, CE mark lub równoważne Zasilanie 230V AC Wysokość maksymalnie 1U, montowany w szafie typu RAC 19’’  |

## Przełącznik sieci LAN IDF – szt. 2 - wymagania minimalne

|  |
| --- |
| 1. Typ i liczba portów:
	* 48 portów 10/100/1000BaseT RJ-45 + uplink 4x10G SFP
2. Porty SFP/SFP+ możliwe do obsadzenia następującymi rodzajami wkładek:
	* Gigabit Ethernet 1000Base-SX,
	* Gigabit Ethernet 1000Base-LX/LH,
	* 10Gigabit Ethernet 10GBase-SR,
	* 10Gigabit Ethernet 10GBase-LR,
	* 10Gigabit Ethernet typu twinax (SFP+ - SFP+)
3. Urządzenie musi posiadać funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi,
4. Zasilanie i chłodzenie:
	* Urządzenie wyposażone jest w wbudowany zasilacz AC230V,
5. Parametry wydajnościowe:
	* Przepustowość przełącznika (switching bandwidth): 176 Gb/s (full duplex),
	* Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 130.94 Mpps
	* Pamięć DRAM – 512 MB
	* Pamięć flash – 256 MB
	* Wielkość bufora pakietów - 1.5 MB
	* Obsługa:
* 256 aktywnych sieci VLAN
* 15000 adresów MAC
* 16 statycznych tras IPv4
* 16 statycznych tras IPv6
* 64 interfejsów SVI L3
* Obsługa MTU-L3 9198B
* Obsługa ramek Ethernet Jumbo 10240B
* 1024 grupy IGMP
* 6 połączeń zagregowanych typu „port channel”
* 16 linków w ramach jednego połączenia zagregowanego typu „portchannel” LACP
* Ilość wpisów w listach kontroli dostępu Security ACL – 600
* Ilość wpisów w listach kontroli dostępu QoS ACL – 600
1. Porty dostępowe przełącznika posiadają zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
2. Obsługa protokołu NTP
3. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
4. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
* IEEE 802.1w Rapid Spanning Tree
* Per-VLAN Rapid Spanning Tree (PVRST+)
* IEEE 802.1s Multi-Instance Spanning Tree
* Obsługa 64 instancji protokołu STP

11. Obsługa protokołu LLDP i LLDP-MED12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC1. Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad
2. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
3. Możliwość uruchomienia funkcji serwera DHCP
4. Mechanizmy związane z bezpieczeństwem sieci:
* Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik
* umożliwia zalogowanie się administratora z konkretnym poziomem dostępu
* zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
* Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
* Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
* Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
* Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
* Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication),
* Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176,
* Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www),
* Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
* Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+,
* Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP),
* Funkcja Private VLAN,
1. Obsługa mechanizmów zapewaniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
* sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
* bezpieczna sekwencja uruchamiania,
* sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
1. Mechanizmy związane z zapewnieniem jakości usług w sieci:
* Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
* Implementacja algorytmu Shaped Round Robin dla obsługi kolejek,
* Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
* Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
* Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń,
* Kontrola sztormów dla ruchu broadcast/multicast/unicast,
* Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP;
1. Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6,
2. Przełącznik umożliwia lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących,
3. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),
4. Obsługa protokołu sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow,
5. Zarządzanie
* Port konsoli,
* Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika,
* Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją,
* Obsługa protokołów SNMPv3, SSHv2, https, syslog,
* Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia,
* Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki;
1. Możliwość montażu w szafie rack 19”.
2. Wysokość urządzenia 1 RU.
 |

## Serwerowy system operacyjny – szt. 3 – wymagania minimalne

|  |
| --- |
| Licencja na serwerowy system operacyjny musi uprawniać do zainstalowania serwerowego systemu operacyjnego w środowisku fizycznym oraz umożliwiać zainstalowanie minimum 1000 instancji wirtualnych tego serwerowego systemu operacyjnego. Licencja musi zostać tak dobrana aby była zgodna z zasadami licencjonowania producenta oraz pozwalała na legalne używanie na oferowanym serwerze.Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania 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  7000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
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:
10. pozwalają na zmianę rozmiaru w czasie pracy systemu,
11. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
12. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
13. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
14. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
15. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
16. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
17. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
18. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
19. Dostępne dwa rodzaje graficznego interfejsu użytkownika:
20. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
21. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
22. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
23. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
24. Mechanizmy logowania w oparciu o:
25. Login i hasło,
26. Karty z certyfikatami (smartcard),
27. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
28. Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla grup użytkowników praw do wykorzystywania szyfrowanych danych..
29. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
30. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
31. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
32. Pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
33. Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
34. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
35. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
36. 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:
	* Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
	* Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
	* Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
	* Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1.
37. Zdalna dystrybucja oprogramowania na stacje robocze.
38. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
39. 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,
	* Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
40. Szyfrowanie plików i folderów.
41. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
42. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
43. Serwis udostępniania stron WWW.
44. Wsparcie dla protokołu IP w wersji 6 (IPv6),
45. Wsparcie dla algorytmów Suite B (RFC 4869),
46. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
47. 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)
48. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
49. Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
50. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
51. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
52. Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
53. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.
 |

## System Operacyjny CAL – szt. 70 - wymagania minimalne

|  |
| --- |
| Licencje dostępowe do oferowanych systemów operacyjnych w ilości 70 szt. Oferowane licencje muszą udostępnić możliwość korzystania z zasobów serwisów 70 użytkownikom. |

## System EDR-XDR – szt. 90 – wymagania minimalne

|  |
| --- |
| **Administracja zdalna** 1. Rozwiązanie musi wspierać instalację na systemach Windows Server (od 2012), Linux oraz w postaci maszyny wirtualnej w formacie OVA lub dysku wirtualnego w formacie VHD.
2. Rozwiązanie musi zapewniać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. Rozwiązanie musi zapewniać pobranie wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
4. Rozwiązanie musi zapewniać dostęp do konsoli centralnego zarządzania w języku polskim z poziomu interfejsu WWW zabezpieczony za pośrednictwem protokołu SSL.
5. Rozwiązanie musi zapewniać zabezpieczoną komunikację pomiędzy poszczególnymi modułami serwera za pomocą certyfikatów.
6. Rozwiązanie musi zapewniać utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
7. Rozwiązanie musi zapewniać centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, które działają na stacjach roboczych w sieci.
8. Rozwiązanie musi zapewniać weryfikację podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe).
9. Rozwiązanie musi zapewniać instalowanie i odinstalowywanie oprogramowania firm trzecich dla systemów Windows oraz MacOS oraz odinstalowywanie oprogramowania zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
10. Rozwiązanie musi zapewniać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
11. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
12. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
13. Rozwiązanie musi zapewniać korzystanie z minimum 100 szablonów raportów, przygotowanych przez producenta oraz musi zapewniać tworzenie własnych raportów przez administratora.
14. Rozwiązanie musi zapewniać wysłanie powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
15. Rozwiązanie musi zapewniać podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.

**Ochrona stacji roboczych** 1. Rozwiązanie musi wspierać systemy operacyjne Windows (Windows 10/Windows 11).
2. Rozwiązanie musi wspierać architekturę ARM64.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
4. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami oraz podłączeniem komputera do sieci botnet.
5. Rozwiązanie musi zapewniać wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Rozwiązanie musi zapewniać skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Rozwiązanie musi zapewniać skanowanie całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
8. Rozwiązanie musi zapewniać skanowanie plików spakowanych i skompresowanych oraz dysków sieciowych i dysków przenośnych.
9. Rozwiązanie musi posiadać opcję umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików na podstawie rozszerzenia, nazwy, sumy kontrolnej (SHA1) oraz lokalizacji pliku.
10. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
11. 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).
12. Rozwiązanie musi zapewniać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
13. Rozwiązanie musi posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
14. Rozwiązanie musi zapewniać blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
15. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
16. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
* tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
* tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
* tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
* tryb uczenia się, w którym rozwiązanie uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
* tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
1. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
2. 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.
3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
5. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
6. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
7. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
* tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
* tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
* tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
* tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
1. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
2. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
3. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.
4. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
5. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
6. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
7. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

**Ochrona serwera**1. Rozwiązanie musi wspierać systemy Microsoft Windows Server 2012 i nowszych oraz Linux w tym co najmniej: RedHat Enterprise Linux (RHEL) 7,8 i 9, CentOS 7, Ubuntu Server 18.04 LTS i nowsze, Debian 10, Debian 11 i Debian 12, SUSE Linux Enterprise Server (SLES) 15, Oracle Linux 8 oraz Amazon Linux.
2. Rozwiązanie musi zapewniać ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, 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 możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.

Dodatkowe wymagania dla ochrony serwerów Windows: 1. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
2. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
3. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
4. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
5. Rozwiązanie musi zapewniać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
6. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
7. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
8. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
9. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux: 1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
3. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.
4. 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.

**Szyfrowanie** 1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10 32-bit i 64-bit.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.

**Ochrona urządzeń mobilnych opartych o system Android** 1. Rozwiązanie musi zapewniać skanowanie wszystkich typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
2. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
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 skonfigurowania zaufanej karty SIM.
5. Rozwiązanie musi zapewniać wysłanie na urządzenie komendy z konsoli centralnego zarządzania, która umożliwi:
* usunięcie zawartości urządzenia,
* przywrócenie urządzenie do ustawień fabrycznych,
* zablokowania urządzenia,
* uruchomienie sygnału dźwiękowego,
* lokalizację GPS.
1. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
2. Rozwiązanie musi posiadać blokowanie aplikacji w oparciu o:
* nazwę aplikacji,
* nazwę pakietu,
* kategorię sklepu Google Play,
* uprawnienia aplikacji,
* pochodzenie aplikacji z nieznanego źródła.

**Sandbox w chmurze** 1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
* Czysty,
* Podejrzany,
* Bardzo podejrzany,
* Szkodliwy.
1. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.
2. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
3. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.

**Moduł XDR** 1. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
2. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
3. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
4. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
5. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
6. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
7. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
8. Serwer musi posiadać ponad 900 wbudowanych reguł, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
9. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
10. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
11. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
12. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
13. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej.
14. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
15. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
16. Konsola administracyjna musi mieć możliwość tagowania obiektów.
17. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
 |

## System NAC – szt. 1 – wymagania minimalne

|  |
| --- |
| **Podstawowa funkcjonalność systemu:**1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników i urządzeń końcowych.
2. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor)
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 50000 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 (Bring Your Own 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, Citrix XenServer w wersji min 4.x
* Maszyny fizyczne - serwery wspierane przez producenta.
1. 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.
1. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
2. 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.
3. 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, PostgresSQL, Oracle, ODBC.
4. System musi umożliwiać synchronizację danych (tożsamości, urządzenia końcowe, jednostki organizacyjne, konta administracyjne, adresy MAC) z zewnętrznych systemów (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc, Microsoft Active Directory, Radius, OpenLDAP, relacyjnych baz danych (jak MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC), CheckPoint, Service Now.
5. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.
6. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
7. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
8. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
9. 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.
10. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
11. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
12. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
13. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
14. 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.
15. 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.
16. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
17. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
18. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
19. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
20. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
21. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
22. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
23. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.
24. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
25. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
26. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
27. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
28. System musi posiadać funkcję personalizacji strony gościnnej.
29. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
30. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
31. 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.
32. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
33. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
34. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.
35. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
36. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
37. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
38. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
39. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
40. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
41. 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.
42. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
43. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
44. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
45. System musi obsługiwać różne metody profilowania do wykrywania typu urządzeniu, 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.
46. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
47. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
48. 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
1. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
2. System musi współpracować z serwerem tokenów.
3. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
* Microsoft Windows
* Mac OS
* iOS
* Android
1. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
2. 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.
1. 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.
2. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
3. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
4. 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).
5. 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.
1. 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, MicroTik, Ubiquiti Networks.
2. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
3. 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.
4. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
5. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
6. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
7. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
8. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
9. 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.
10. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
11. 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.
12. 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.
13. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
14. System musi umożliwiać przesyłanie 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 dostępów 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.

**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 nadam 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 wpierać 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.
1. Alarmy mogą być generowane w sytuacjach, min:
* Ilości obsługiwanych transakcji RADIUS,
* Opóźnienie obsługi transkacji RADIUS,
* Statusu krytycznego modułów.
1. 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.
 |

## Punkt dostępowy sieci WIFI Access Point – szt. 1 – wymagania minimalne

|  |
| --- |
| **Punkty dostępowy – komplet (sztuk 6)**  |
| Nazwa atrybutu | Wymagane parametry techniczne |
| Typ | Punkt dostępowy/Access Point |
| Obsługa protokołów | IEEE 802.11a, IEEE 802.11ac, IEEE 802.11ax, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.1Q, IEEE 802.3at |
| Częstotliwość pracy | 2,4 GHz i 5 GHz |
| Prędkość transmisji | 2,4 GHz: 573.5 Mb/s5 GHz: 4800 Mb/s |
| Bezpieczeństwo | Min. WPA, WPA-Enterprise, WPA-PSK, WPA2, WPA3 |
| Zasilanie | 802.3at PoE+ |
| MIMO | 2,4 GHz: 2x2 (UL MU-MIMO)5 GHz: 4x4 (DL/UL MU-MIMO) |
| Zysk anteny bezprzewodowej | Min. 3 dBi |
| Maksymalne zużycie energii | Nie więcej niż 15W |
| Porty LAN | Min. 1 szt. 10/100/1000 |
| Temperatura pracy | W zakresie nie mniejszym niż ‑10 do 60° C |
| Możliwości montażu | Montaż wewnątrz i na zewnątrz budynków |
| Akcesoria zawarte w zestawie | Zestaw montażowy |
| Gwarancja | Min. 2 lata |
| Kontroler – 1 szt. |
| Nazwa atrybutu | Wymagane parametry techniczne |
| Typ | Kontroler pozwalający na zarządzanie i konfigurację punktów dostępowych |
| Porty wejścia/wyjścia | Min. 1 x 10/100/1000 Mbit/s, min. 1 x micro USB |
| Zasilanie | Min. 802.3af PoE,  |
| Dostęp | Poprzez przeglądarkę internetową |
| Temperatura pracy | W zakresie nie mniejszym niż 0 do 35° C |

## UPS – szt. 1 – wymagania minimalne

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis wymagań techniczno-funkcjonalnych** | **Wartość minimalna** |
|  | Technologia | VFI (true on-line, podwójne przetwarzanie energii) |
|  | Budowa | Beztransformatorowa, prostownik IGBT.UPS musi być wyposażony w podwójny tor zasilający niezależny dla prostownika i Bypassu.  |
|  | Moc znamionowa | 30 kVA / 30kW |
|  | Wyjściowy współczynnik mocy (PF) | 1,0 |
|  | Współczynnik mocy wejściowej 0.99.  | 0,99 |
|  | Napięcie wejściowe trójfazowe | 400 VAC 3F + N |
|  | Tolerancja napięcia wejściowego przy obciążeniu 100%; bez przechodzenia na baterie | 172 – 287 Vac (L-N) |
|  | Zakres częstotliwości wejściowej | Wymagana 40-70 Hz |
|  | Sprawność AC-AC w trybie pracyon-line z obciążeniem 100%  | nie mniejsza niż 96% |
|  | Tryb pracy ECO mode, zapewniający podwyższoną sprawność zasilacza | Wymagany |
|  | Możliwość rozbudowy mocy wokresie eksploatacji  | Do minimum 8 sztuk w układzie pracy równoległej |
|  | Montażu modułu pracy równoległej w oferowanej jednostce | Wymagane – pozwala na dołączenie kolejnej jednostki. |
|  | Napięcie wyjściowe trójfazowe | 400 VAC 3F + N |
|  | Częstotliwość wyjściowa | 50/60Hz (programowalna) |
|  | Zintegrowane bezprzerwoweprzełączniki obejściowe (by-pass) | Statyczny przełącznik (SCR) orazręczny rozłącznik serwisowy |
|  | Zewnętrzny bezprzerwowy Bypass serwisowy | Wymagany Bypass bezprzerwowy w postaci jednego przełącznika, z informacją o położeniu dla zabezpieczenia falownika UPS przed uszkodzeniem w przypadku nieprawidłowego użycia. |
|  | Wejście komunikacyjne na UPS do podłączenia sygnalizacji położenia przełącznika zewnętrznego Bypassu serwisowego, dla ochrony falownika UPS przed przypadkowym przełączeniem | Wymagane |
|  | Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczeniechroniące baterie przed głębokim rozładowaniem. | Wymagane, wraz z funkcją restingu baterii |
|  | Możliwość regulacji prądu ładowania baterii z poziomu panelu LCD w UPS-ie.  | Wymagane – podać maksymalną wartość prądu ładowania baterii |
|  | Czas podtrzymania | 6 minut przy obciążeniu 30kW |
|  | Minimalna pojemność zainstalowanych akumulatorów liczona jako: Ilosc akumulatorów \* pojemność pojedynczego akumulatora \* napięcie pojedynczego akumulatora [V\*Ah] | 8 640 Ah\*V |
|  | Moduł baterii | Baterie muszą być umieszczone w obudowie UPS. Należy stosować baterie szczelne AGM VRLA o żywotności 10-12 lat. Każdy łańcuch baterii zabezpieczony niezależnym rozłącznikiem bezpiecznikowym. |
|  | Autonomia pracy zasilacza UPS przy pracy z baterii podawana w minutach na panelu LCD zasilacza | Wymagane |
|  | W przypadku uszkodzenia pojedynczychakumulatorów w stosie, wymaganapoprawna praca urządzenia ze zmniejszonym łańcuchem baterii | Wymagane, poprzez konfigurację, zmianę długości łańcucha baterii 30-40 sztuk |
|  | Stabilizacja napięcia wyjściowego wstanie ustalonym | ± 1% |
|  | Stabilizacja napięcia wyjściowego w stanie nieustalonym | ± 3% |
|  | Stabilność częstotliwościwyjściowej: | bez synchronizacji: ± 0,05 Hz |
|  | Współczynnik szczytu | 3:1 |
|  | Minimalne przeciążenie falownika w trybie pracy normalnej | 115% przez 60 minut130% przez 10 minut150% przez 1 minutę>150% - 0,2 sek |
|  | Panel sterujący z wyświetlaczem dotykowym oraz sygnalizacją diodową i akustyczną | Wymagane |
|  | Złącze interfejsów | SNMP, Dry Contact In/OUT, Modbus RTU, RS485 |
|  | Karta sieciowa SNMP wbudowana w UPS. | Wymagane |
|  | Interfejs EPO (do wyłącznika ppoż.) | Wymagane – zestyk NO oraz NC. UPS zintegrowany z systemem ppoż budynku. |
|  | Diagnostyka parametrów urządzeniaUPS i baterii | Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS |
|  | Dedykowane oprogramowanie do wysyłania SMS | Wymagane |
|  | Poziom hałasu w odległości 1m | < 50 dBA |
|  | Rejestr zdarzeń | Dziennik zdarzeń w UPS-ie+ komunikaty serwisowe |
|  | Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu | Wymagane |
|  | Monitorowanie stanu baterii i czasu autonomii  | Stan baterii + dostępna autonomia mierzona w czasie rzeczywistym  |
|  | UPS wyposażony w dotykowy, kolorowy wyświetlacz zabezpieczony hasłem przed ingerencją osób postronnych | Wymagane |
|  | UPS wyposażony w programowany tryb pracy ECO mode o podwyższonej sprawności z możliwością zaprogramowania dni tygodnia oraz godzin w jakich UPS przechodzi automatycznie w tryb oszczędnej pracy o podwyższonej sprawności. | Wymagane |
|  | UPS wyposażony w funkcję automatycznego czyszczenia z możliwością zaplanowania okresowego samoczynnego załączenia się tej funkcji. | Wymagane |
|  | UPS wyposażony w zdalny wyłącznik REPO | Wymagane – dostawa po stronie dostawcy UPS. |
|  | Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE | Wymagane zarówno dla zasilacza UPS jak i baterii |
|  | Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju. | Wymagane |
|  | Certyfikat ISO 9001 i 14001 dystrybutora i producenta sprzętu | Wymagane |
|  | Rozłączniki manewrowe | Zasilacz UPS powinien być wyposażony w komplet rozłączników pozwalających na bezpieczne włączenie i wyłączenie UPSa. Wymaga się co najmniej czterech rozłączników zamontowanych na UPS: zasilanie prostownika, zasilanie bypass, bypass serwisowy, rozłącznik wyjściowy z UPS. |
|  | Podłączenie zasilania i odbiorów | Podłączenie okablowania z tyłu zasilacza, z możliwością podłączenia dwóch oddzielnych torów do zasilania prostownika i bypassu wewnętrznego. |
|  | UPS powinien posiadać funkcję umożliwiającą samo dociążenie bez podłączania dodatkowych odbiorników w celu przetestowania podzespołów pod pełnym obciążeniem w trakcie każdej wizyty serwisu. | Wymagane |
|  | Zasilacz wyposażony w kółka transportowe pozwalające na łatwe przemieszczanie w czasie konserwacji | Wymagane  |
|  | Wymiary UPS nie większe niż (S x G x W) | 300 x 850 x 1250 mm (+/-5%) |
|  | Instrukcja w języku polskim | Wymagane |

## Agregat – szt. 1 – wymagania minimalne

|  |
| --- |
| * Agregat prądotwórczy stacjonarny w wersji zabudowanej z silnikiem diesla – paliwo: olej napędowy
* Moc wg PN-ISO 8528: PRP min. 100 kVA / 80 kW
* Poziom, do którego można przeciążyć agregat przez jedną godzinę raz na dwanaście godzin pracy min. 110 kVA / 88 kW
* Napięcie wyjściowe 400/230V, 50Hz
* Konstrukcja agregatu na ramie wykonanej z blachy stalowej zabezpieczona przed korozją i pomalowana
* Wymiary nie przekraczające: długość 2500 mm x szerokość 1100 mm x wysokość 1800 mm
* Ciężar nie przekraczający 1.700 kg
* Obudowa dźwiękochłonna odporna na warunki atmosferyczne, o gwarantowanym przez producenta poziomie mocy akustycznej nie większym niż LwA 96 dB
* Pojemność zbiornika zainstalowanego w ramie agregatu, min. 200 litrów i wystarczającym na ok. 8 h pracy pod pełnym obciążeniem dla mocy ciągłej PRP.
* Podgrzewany blok silnika umożliwiający uruchomienie zespołu przy niskich temperaturach:
* zewnętrzny (montowany poza silnikiem) układ podgrzewania cieczy chłodzącej wyposażony w termostat oraz zawory odcinające umożliwiające wymianę podgrzewacza bez konieczności spuszczania płynu chłodzącego - umożliwia start zespołu w niskich temperaturach
* Tłumiki antywibracyjne pomiędzy ramą, a zespołem silnik-prądnica
* Podejście kablowe od spodu szafy wyłącznika głównego
* Bateria rozruchowa 24 V (2x12V)
* Rozłącznik baterii akumulatorów zamontowany na ramie agregatu
* Prostownik zasilający panel, ładujący i konserwujący baterię rozruchową
* Szafa wyłącznika głównego prądnicy z zabezpieczeniem zwarciowym i przeciążeniowym zainstalowana na agregacie
* Panel sterowniczy (szafa sterownicza wyposażona m.in. w sterownik kontroli i nadzoru pracy agregatu) zainstalowana na agregacie
* Agregat musi posiadać znak CE (lub równoważny) obejmujący następujące Dyrektywy:
* 2006/42/CE Bezpieczeństwo Maszyn (lub równoważny)
* 2006/95/CE Nisko Napięciowa (lub równoważny)
* 2004/108/CE Kompatybilność Elektromagnetyczna (lub równoważny)
* 2000/14/CE Emisja Hałasu (dotyczy wyłącznie urządzeń pracujących na wolnym powietrzu)
* 97/68/CE Emisja gazów i cząstek zanieczyszczających z maszyn ruchomych nie drogowych (zgodnie z Aneksem 1 Punkt 1). (dotyczy wyłącznie urządzeń pracujących na wolnym powietrzu i przemieszczających się np. agregaty na podwoziu jezdnym) (lub równoważny)

**Minimalne wymagania dotyczące silnika (parametry do oceny równoważności):** * Silnik wysokoprężny (diesel) chłodzony cieczą, turbodoładowany
* Układ cylindrów: rzędowy (L) , liczba cylindrów nie większa niż 4
* Rodzaj wtrysku paliwa: bezpośredni
* Rodzaj sterowania wtryskiem: common rail
* Regulator obrotów silnika – elektroniczny
* Klasa regulacji obrotów wg ISO8528-5 – minimum G3
* Napięcie instalacji : 24V DC

**Minimalne wymagania dotyczące prądnicy** * Napięcie 3x400V + N, 50Hz
* Moc nominalna przy 400V/50Hz/Klasa H nie mniejsza niż 110 kVA/88 kW
* Konstrukcja: synchroniczna, samowzbudna, samoregulująca, bezszczotkowa
* Automatyczny regulator napięcia – AVR o stabilizacji napięcia +/- 1,0%
* Całkowita zawartość harmonicznych w przebiegu napięcia generowanego pod stałym obciążeniem: < 2 %
* Klasa izolacji H
* Stopień ochrony nie mniejszy niż IP23
* Sprawność (4/4) nie mniejsza niż 88,2 %
* Zdolność zwarciowa: >300%

**Minimalne wymagania dotyczące automatyki – sterownika****Możliwości standardowe:*** Stopień ochrony płyty czołowej sterownika nie mniejszy niż IP65
* Wyświetlacz LCD
* Napięcie zasilania zakres nie gorszy niż 8–36 V
* Ilość wejść binarnych – nie mniej niż 7
* Ilość wyjść binarnych – nie mniej niż 7
* Ilość wejść analogowych – nie mniej niż 3
* Odczyt obrotów z czujnika magnetycznego obrotów (przy regulacji elektronicznej obrotów)
* Możliwość zaprogramowania funkcji AMF/MRS w sterowniku tzn. możliwość pracy w trybach: AMF - nadzoru sieci i sterowania SZR-em lub MRS – zdalnego startu na sygnał z zewnątrz bez sterowania SZR-em
* Programowane wejścia/wyjścia
* Pomiar 3 fazowy napięcia sieci / generatora
* Pomiar 3 fazowy prądu generatora
* Pomiar kW i kVA, współczynnika mocy
* 3-fazowa funkcja AMF (nadzoru sieci przy sterowaniu SZR-em):

- Zabezpieczenie nadczęstotliwościowe/podczęstotliwościowe- Zabezpieczenie nadnapięciowe/podnapięciowe- Zabezpieczenie od asymetrii napięciowej* Odczyty parametrów silnika: ciśnienia oleju, temperatury chłodziwa, obrotów silnika, napięcia akumulatorów, poziomu paliwa
* Zabezpieczenia silnika: zbyt niskie ciśnienie oleju, zbyt wysoka temperatura chłodziwa, błąd rozruchu, niskie/wysokie napięcie akumulatora, niskie/wysokie obroty silnika
* Programowane wejścia/wyjścia
* Zabezpieczenia generatora 3-fazowego:

- Zabezpieczenie nadczęstotliwościowe /podczęstotliwościowe- Zabezpieczenie nadnapięciowe/podnapięciowe- Zabezpieczenie od asymetrii prądowej/napięciowej- Zabezpieczenie nadprądowe/od przeciążeń* Licznik godzin pracy
* Rejestracja historii zdarzeń
* Zacisk wzbudzenia wstępnego D+
* Programowany autotest agregatu
* Menu w języku polskim
* Bezpłatne oprogramowanie komunikacyjne dostępne na stronie producenta

**Możliwości opcjonalne (możliwe do zainstalowania) :*** RS232/RS485/USB
* MODBUS RTU/TCP
* Obsługa Internetu z serwerem sieciowym przez LAN/WAN/SNMP
* Obsługa Internetu przez GPRS
* Obsługa GPS (lokalizacja)
* Komunikacja SMS, e-mail
 |

## Instalacja, konfiguracja, wdrożenie, utrzymanie – szt. 1 – wymagania minimalne

|  |
| --- |
| Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania. |
|  | **Usługi** | Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji elementów cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i oprogramowanie opisane w podmiotowym dokumencie.Część sprzętowa powinna zostać oparta na systemie wirtualizacji zasobów IT. Zamawiający umożliwi Wykonawcy dostęp do infrastruktury w ustalonym wcześniej terminie w celu dokonania analizy i przygotowania procedur wdrożenia, migracji do nowego środowiska. Dostęp do infrastruktury będzie możliwy pod nadzorem Zamawiającego i po spełnieniu warunków wynikających z Polityki Bezpieczeństwa i wymagań Zamawiającego.Zamawiający udzieli Wykonawcy wszelkich niezbędnych informacji niezbędnych do przeprowadzenia wdrożenia.**W ramach oferty Zamawiający wymaga przeprowadzenia wdrożenia na zasadach projektowych z pełną dokumentacją wdrożeniową**. Zamawiający wymaga następującego zakresu usług realizowanego w porozumieniu z Zamawiającym:* 1. Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia.
	2. Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności:
		1. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych.
		2. schematy połączeń
		3. mechanizmy działania głównych elementów sprzętowych:
* klaster wirtualizacyjny
* sieć LAN - przełączniki sieciowe
* system backupu i archiwizacji danych
* firewall/UTM
* centralny system logów
* zasilanie awaryjne
* sieć WiFi
	+ 1. iii. mechanizmy działania głównych elementów programowych:
* system EDR
* system NAC
* system domenowy/wirtualizacyjny
* system backupu
* Oprogramowanie bazy danych
	+ 1. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności
		2. sposób odbioru uzgodniony z Zamawiającym
		3. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu
		4. opis przypadków, w których projekt dopuszcza niedziałanie systemu
		5. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą

Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia. |
|  | **Montaż i fizyczne uruchomienie systemu** | **Zamawiający wymaga, aby Wykonawca zainstalował całości dostarczonego rozwiązania w pomieszczeniu serwerowni, jak i innych wskazanych miejscach co najmniej w zakresie:**1. Wniesienie, ustawienie i fizyczny montaż wszystkich dostarczonych urządzeń w szafach rack w pomieszczeniach (miejscach) wskazanych przez Zamawiającego z uwzględnieniem wszystkich lokalizacji.
2. Rozbudowa istniejących zasobów sprzętowych.
3. Urządzenia, które nie są montowane w szafach teleinformatycznych, powinny zostać zamontowane w miejscach wskazanych przez Zamawiającego, oraz skonfigurowane i dołączone do infrastruktury Zamawiającego.
4. Usunięcie opakowań i innych zbędnych pozostałości po procesie instalacji urządzeń.
5. Podłączenie całości rozwiązania do infrastruktury Zamawiającego.
6. Wykonanie procedury aktualizacji firmware dostarczonych elementów do najnowszej wersji oferowanej przez producenta sprzętu.
7. Dla urządzeń modularnych wymagany jest montaż i instalacja wszystkich podzespołów.
8. Wykonanie połączeń kablowych pomiędzy dostarczonymi urządzeniami w celu zapewnienia komunikacji – Wykonawca musi zapewnić niezbędne okablowanie (np.: patchordy miedziane min. kat. 6 UTP lub światłowodowe uwzględniające typ i model interfejsu w urządzeniu sieciowym).
9. Wykonawca musi zapewnić niezbędne okablowanie potrzebne do podłączenia urządzeń aktywnych do sieci elektrycznej (np.: listwy zasilające).
10. Wykonawca musi zapewnić niezbędne wkładki dla dostarczonych urządzeń np.: SFP, SFP+ miedzy innymi celem:
	1. Stworzenia połączeń sieci LAN pomiędzy przełącznikami.
	2. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN.
	3. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1.
	4. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
 |
|  | **Instalacja i konfiguracja oprogramowania** | 1. Instalacja i konfiguracja dostarczonego oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji.
2. Instalacja i konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu.
3. Instalacja dostarczonego oprogramowania systemu serwerowego wraz z niezbędnymi usługami oraz instalacja wszystkich niezbędnych kodów dostępowych oraz licencji (wszelkie procedury rejestracyjne powinno zostać wykonane na danych dostarczonych przez Zamawiającego).
4. Instalacja i konfiguracja dostarczonych systemów operacyjnych dla serwerów wirtualnych.
5. Instalacja i konfiguracja oprogramowania EDR.
6. Instalacja i konfiguracja oprogramowania NAC.
7. Instalacja i konfiguracja oprogramowania bazy danych
 |
|  | **Konfiguracja przełączników/sieci LAN:** | Zamawiający wymaga stworzenia połączeń sieciowych pomiędzy wszystkimi lokalizacjami występującymi w projekcie według topologii gwiazdy. Centralnym punktem będzie serwerownia zlokalizowana w Urzędzie.Dostarczone przełączniki urządzaniami będą stanowiły centralny punkt wymiany danych sieciowych z punktu widzenia warstwy drugiej modelu ISO/OSI – L2 (warstwa łącza danych) oraz zapewnią wsparcie dla protokołu STP (protokół drzewa rozpinającego).Konfiguracja przełączników w zakresie:* 1. Przeprowadzenie audytu obecnej topologii oraz konfiguracji.
	2. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
	3. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów.
	4. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym).
	5. Wymagane jest wydzielenie i skonfigurowanie co najmniej stref:
* SERWERY
* UŻYTKOWNICY WEWNĘTRZNI
* UŻYTKOWNICY ZEWNĘTRZNI
* MANAGEMENT
	1. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy)
	2. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall.
	3. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN.
		1. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink.
		2. Z wykorzystaniem połączeń światłowodowych oraz miedzianych.
		3. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu.
		4. Należy wykorzystać wkładki o najwyższej możliwej przepustowości dla danego połączenia np.: dla portu o możliwej przepustowości 1/10Gbs (wkładka: SFP/SFP+), należy wykorzystać wkładki SFP+ o przepustowości 10Gbps.
	4. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN.
	5. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster;
	6. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK).
	7. Zamawiający wymaga skonfigurowania mechanizmów bezpieczeństwa na dostarczonych przełącznikach LAN co najmniej w zakresie:
* Konfiguracja mechanizmów DHCP Snooping
* Konfiguracja mechanizmów Dynamic ARP Inspection
* Konfiguracja mechanizmów Port Security na wskazanych portach przełączników
* Konfiguracja mechanizmów 802.1x na wskazanych portach przełączników w oparciu o certyfikaty komputerów (konfiguracja Centrum Certyfikacji oraz polityk leży po stronie Wykonawcy) z wykorzystaniem dostarczonego oprogramowania NAC.
	1. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall.
	2. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source.
	3. Zamawiający wymaga instalacji i konfiguracji dedykowanego serwera monitorowania pracy urządzeń sieciowych z graficznym interfejsem przeszukiwania (maszyna wirtualna): przełączniki sieciowe, drukarki, UTM. Zamawiający dopuszcza rozwiązania Open Source.
	4. Wykonawcza skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci.
	5. Testowanie obsługi ruchu sieciowego.
	6. Testowanie skuteczności zabezpieczeń.
 |
|  | **Konfiguracja elementów bezpieczeństwa sieciowego.**  | Urządzenia firewall/modernizacja konfiguracji UTM w zakresie.1. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia.
2. Aktywacja (jeśli wymagana) urządzenia na stronie internetowej producenta.
3. Aktywacja (jeśli wymagana) funkcjonalności oferowanych przez urządzenia (AV, IPS, Kontrola Aplikacji, Filtrowanie WWW, Filtrowanie Email)
4. Przygotowanie projektu włączenia urządzenia do sieci LAN urzędu.
5. Konfiguracja dostarczonych systemów Firewall:
	1. Konfiguracja podstawowych parametrów
	2. Konfiguracja translacji adresów NAT
	3. Konfiguracja mechanizmów ochrony wybranych sieci VLAN, do których przyłączone zostaną np. serwery, macierze, itp.
	4. Konfiguracja inspekcji określonych protokołów sieciowych;
	5. Konfiguracja reguł dostępu do określonych podsieci, chronionych przez moduł Firewall;
	6. Konfiguracja zarządzania Firewall przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
	7. Testowanie działania bramy
6. Konfiguracja modułów należących do systemu wykrywania włamań IPS:
	1. Konfiguracja podstawowych parametrów
	2. Konfiguracja mechanizmów ochrony określonych sieci VLAN przez moduł wykrywania włamań;
	3. Konfiguracja reguł kontroli ruchu sieciowego przez moduły oraz sposobów reakcji na pojawienie się niepożądanego ruchu sieciowego;
	4. Konfiguracja zarządzania modułami przez dedykowaną stację zarządzającą bezpieczeństwem sieciowym;
	5. Testowanie działania ochrony IPS
7. Konfiguracja modułu ochrony antywirusowej, antyspyware, blokowania transferu plików, antyspamowa, filtrowania i blokowania odwołań do niepożądanych adresów URL.
	1. Przypisanie adresu IP do zarządzania.
	2. Konfiguracja inspekcji protokołów HTTP, HTTPS; SMTP, FTP, POP3
	3. Definicja reguł filtrowania/blokowania
	4. Integracja z systemem domenowym w celu weryfikacji nawiązywania połączenia poprzez nazwę użytkownika z domeny.
8. Konfiguracja tuneli SSL VPN celem zapewnienia bezpiecznego dostępu do sieci wewnętrznej.
9. Konfiguracja uwierzytelniania w oparciu o dostarczony moduł uwierzytelnienia.
10. Uruchomienie i skonfigurowanie dedykowanych oddzielnych instancji systemów bezpieczeństwa dla: dedykowanych, stworzonych na przelaniach sieci VLAN.
11. W miarę możliwości polityki dostępu powinny być budowane w oparciu o poświadczenia użytkowników (moduł uwierzytelnienia), nie zaś o adresy IP, czy MAC
12. W każdej instancji systemu bezpieczeństwa należy skonfigurować co najmniej 3 profile (wytyczne przekaże Zamawiający) dla każdej z poniższych funkcjonalności:
	1. kontrola dostępu - zapora ogniowa klasy Stateful Inspection
	2. ochrona przed wirusami – antywirus [AV] (dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS) umożliwiający skanowanie wszystkich rodzajów plików, w tym zip, rar
	3. ochrona przed atakami - Intrusion Prevention System [IPS/IDS]
	4. kontrola stron internetowych pod kątem rozpoznawania witryn potencjalnie niebezpiecznych: zawierających złośliwe oprogramowanie, stron szpiegujących oraz udostępniających treści typu SPAM.
	5. kontrola zawartości poczty – antyspam [AS] (dla protokołów SMTP, POP3, IMAP)
	6. kontrola pasma oraz ruchu [QoS, Traffic shaping]
	7. Kontrola aplikacji oraz rozpoznawanie ruchu P2P
	8. Ochrona przed wyciekiem poufnej informacji (DLP)
	9. Filtra WWW (w oparciu o kategorie stron WWW oraz własną bazę URL)
	10. Inspekcja ruchu SSL
	11. Ochrony przez atakami na stacje klienckie
	12. Kontrola pasma
13. Konfiguracja szyfrowanych tuneli VPN (IPSec) pomiędzy lokalizacjami zdalnymi.
14. Konfiguracja logowania i raportowania.
15. Podłączenie klastra firewall do dostarczonego centralnego sytemu logów.
 |
|  | **Serwery pod wirtualizację** | Zamawiający wymaga instalacji i konfiguracji dostarczonych serwerów celem stworzenia bazy sprzętowej dla klastra niezawodnościowego i wydajnościowego stworzonego na bazie dostarczonych serwerów i oprogramowania do wirtualizacji. |
|  | **Serwer backupu** | W ramach projektu przewiduje się wykorzystanie urządzenia - serwera na backupu - miejsce przechowywanie backupu. Na serwerze należy zainstalować oprogramowanie do wirtualizacji – zarządzane z jednego centralnego miejsca, tego samego jak dla serwerów wirtualizacyjnych. System musi zostać podłączony do macierzy produkcyjnej, musie posiadać lokalne repozytoria danych na przestrzeni dyskowej, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na połowie zasobu dyskowego. Natomiast druga część zasobu musi zostać wykorzystana do wykonywania replikacji on-line maszyn wirtualnych na lokalna platformę wirtualizacyjną – na serwerze backupu. Takie podejście ma gwarantować zabezpieczenie kluczowych węzłów sieciowych (serwerów wirtualnych) na dwa sposoby tj. plik off-line maszyny wirtualnej oraz kopia on-line replikowania asynchronicznie według harmonogramu. Wykonywanie backupu musi być powiązane z procedurą sprawdzania poprawności jego wykonania oraz automatycznym raportowaniem do jednostki administracyjnej. Mechanizm podłączenia 1. Konfiguracja i podłączenie serwera backupu do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
2. Konfiguracja i podłączenie serwera backupu do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
3. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.

Logiczny schemat rozbudowywanego systemu backup – stan docelowy. |
|  | **Macierz****dyskowa** | Istniejąca macierz musi być wykorzystywana do gromadzenia i przechowywania „danych produkcyjnych” – wykorzystywanych przez oprogramowanie dziedzinowe. Musi zostać podłączona do środowiska wirtualizacyjnego (klaster serwerów).Ilość i wielkość udziałów dyskowych udostępnionych dla serwerów np.: wirtualizacyjnych zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej. |
|  | **Sieć Wi-Fi** | 1. Przeprowadzenie pomiarów propagacji sygnału WLAN (site survey) w budynkach w celu określenia miejsc, w których należy zainstalować punktu dostępowe sieci bezprzewodowej, tak aby zapewnić optymalne pokrycie budynku sygnałem WLAN. W przypadku wyznaczenia innych punktów zmiany należy uzgodnić w Zamawiającym.
2. Montaż i instalacja dostarczonego kontrolera.
3. Dostawa i montaż bezprzewodowych punktów dostępowych – Wykonawca musi zapewnić wykonanie okablowania strukturalnego sieci LAN dla doręczonych punktów dostępowych – skrętka min. kat 6 U/UTP. Okablowanie musi zostać zakończone na patchpanelu w szafie sererowej.
4. Przeprowadzenie pomiarów propagacji sygnału WLAN (revised site survey) w budynku, w którym zainstalowano sieć WLAN, w celu weryfikacji pokrycia.
5. Konfiguracja urządzeń zarządzających pracą punktów dostępowych sieci WLAN;
	1. Definicja punktów dostępowych sieci WLAN na urządzeniach;
	2. Konfiguracja interfejsu radiowego punktów dostępowych sieci WLAN:
		1. Wybór i konfiguracja kanałów radiowych na poszczególnych punktach dostępowych tak, aby zminimalizować interferencje pomiędzy poszczególnymi punktami dostępowymi sieci WLAN;
		2. Wybór i konfiguracja odpowiednich SSID na poszczególnych punkach dostępowych;
	3. Konfiguracja kont administratora oraz ograniczenie dostępu do urządzenia jedynie ze stacji zarządzającej;
	4. Konfiguracja stacji zarządzającej pracą sieci WLAN:
		1. Logowanie zdarzeń występujących w sieci WLAN do stacji zarządzającej;
	5. Konfiguracja zaawansowanych mechanizmów bezpieczeństwa (autentykacja użytkowników korzystających z sieci WLAN oraz szyfrowanie ruchu transmitowanego przez sieć WLAN, w powiązaniu z dostarczanym serwerem uwierzytelniającym);
	6. Konfiguracja mechanizmu dostępu do wydzielonych sieci WLAN:
		1. Zabezpieczenie dostępu do gościnnej sieci WLAN (SSID Guest) poprzez autentykację na wewnętrznym serwerze WWW urządzenia zarządzającego pracą sieci WLAN;
		2. Zabezpieczenie dostępu do wybranych sieci WLAN poprzez autentykację na zewnętrznym serwerze z wykorzystaniem kont z systemu domenowego;
		3. Zabezpieczenie dostępu do wybranych sieci WLAN poprzez autentykację na zewnętrznym serwerze z wykorzystaniem certyfikatów;
		4. Zezwolenie na dostęp sieci WLAN tylko w określonych porach dnia;
		5. Określenie rodzaju ruchu, jaki może być transmitowany w ramach sieci WLAN (np. dostęp do Internetu dla usług WWW, vpn, itp.);
		6. Dla sieci WLAN pracowniczej (SSID Pracownik) zdefiniować politykę dostępu, która przypisze odpowiednią sieć VLAN na podstawie przynależności do grup w systemie domenowym
		7. Konfiguracja mechanizmów QoS w sieci WLAN (transmisja danych oraz głosu);
 |
|  | **UPS, Agregat** | W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanych urządzeń UPS i Agregat do sieci elektrycznej Urzędu celem zabezpieczenia pomieszczenia serwerowni. Wszystkie koszty z tym związane np.: modernizacji istniejącej instalacji elektrycznej muszą zostać przewidziane i uwzględnione w ofercie Wykonawcy. |
|  | **Migracja danych** | Dotyczy przeniesienia obecnie wykorzystywanych i rozbudowywanych systemów informatycznych na nowe dostarczone rozwiązanie sprzętowe z wykorzystaniem wirtualizacji zasobów.Dane (systemy dziedzinowe) musza zostać przeniesione na nowe zasoby serwerowo-macierzowe. Zakres migracji zostanie ustalona z Zamawiającym na etapie analizy przedwdrożeniowej.Migracja danych musi uwzględniać uwspólnianie zasobów oraz weryfikacji ich poprawności i jakości technicznej min. w pełnym zakresie danych i rejestrów systemów dziedzinowych. |
|  | **Serwer SMTP** | Zamawiający wymaga zainstalowania oraz uruchomienia i skonfigurowania dedykowanego serwera SMTP. Serwer SMTP powinien być uruchomiony na dedykowanym wirtualnym serwerze pracującym pod kontrolą systemu Linux.Serwer SMTP będzie wykorzystywany na potrzeby wysyłania powiadomień systemowych między innymi z:* Urządzeń sieciowych
* Serwerów
* Macierzy dyskowej
* Systemu zarządzania kopiami zapasowymi
* Systemu wirtualizacji serwerów
* Aplikacji

Zamawiający wymaga zabezpieczenia serwera w taki sposób, aby uniemożliwić przesyłanie wiadomości z nieautoryzowanych źródeł. Zamawiający wymaga, aby wysyłane powiadomienia były poprawnie dostarczane na zewnętrzne konta email. |
|  | **Instalacja i konfiguracja serwera kopii zapasowych konfiguracji urządzeń sieciowych.** | 1. Zamawiający wymaga, aby wraz z uruchomieniem dostarczanych urządzeń sieciowych uruchomić serwer – repozytorium konfiguracji z dostarczanych urządzeń np.; przełączników sieciowych oraz innych urządzeń wspierających wykonywanie kopii zapasowych konfiguracji na zasób sieciowy.
2. Serwer musi być uruchomiony na dedykowanej maszynie (dopuszcza się maszynę wirtualną uruchomioną na infrastrukturze wirtualizującej Zamawiającego).
3. Serwer może działać w oparciu o dowolny system operacyjny, Zamawiający powinien uwzględnić cenę licencji w ofercie i dostarczyć ją we własnym zakresie.
4. Serwer może działać w oparciu o dowolne oprogramowanie bądź rozwiązanie autorskie Wykonawcy. Jeżeli takowa jest potrzebna, Zamawiający wymaga dostarczenia licencji. Cena licencji powinna być wliczona w cenę oferty.
 |
|  | **Uruchomienie środowiska wirtualizacyjnego.** | Zamawiający wymaga zaplanowania, uruchomienia oraz przetestowania środowiska wirtualizacyjnego, co najmniej w zakresie:1. Aktywacja licencji oprogramowania wirtualizacyjnego na stronie producenta.
2. Przygotowanie serwerów do instalacji oprogramowania wirtualizacyjnego – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
3. Przygotowanie macierzy do podłączenia do systemu wirtualizacji – aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta.
4. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach.
5. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.
6. Konfiguracja i podłączenie serwerów wirtualizacyjnych do zasobu dyskowego. Zamawiający wymaga takiego skonfigurowania dostępu do zasobu dyskowego, aby każdy wolumen dyskowy zasobu dyskowego był widziany przez każdy z serwerów wirtualizacyjnych poprzez wszystkie ścieżki (porty) udostępniane przez zasób dyskowy. Każdy wolumen dyskowy musi być dostępny dla każdego serwera wirtualizacyjnego w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) udostępnianych przez zasób dyskowy.
7. Konfiguracja i podłączenie serwerów wirtualizacyjnych do sieci LAN Wnioskodawcy. Zamawiający wymaga, aby każdy z serwerów wirtualizacyjnych był podłączony do sieci LAN, co najmniej taką liczbą portów, by w przypadku niedostępności (awarii) n-(n-1) ścieżek, gdzie n oznacza liczbę wszystkich dostępnych ścieżek (portów) był zachowany dostęp do sieci LAN.
8. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q.
9. Przygotowanie koncepcji wirtualizacji fizycznych maszyn.
10. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym.
11. Konfiguracja klastra wysokiej dostępności:
	1. Konfiguracja mechanizmów HA – w przypadku awarii węzła klastra wirtualne maszyny, które są na nim uruchomione muszą zostać przeniesione na sprawny węzeł klastra bez ingerencji użytkownika.
	2. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn.
	3. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera.
12. Weryfikacja działania klastra wysokiej dostępności.
13. Migracja istniejącej infrastruktury do środowiska wirtualnego.
14. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową
15. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
 |
|  | **System backupu** | 1. Instalacja i rekonfiguracja oprogramowania zarządzającego wykonywaniem kopii zapasowych na dostarczonym serwerze.
2. Aktywacja oraz instalacja niezbędnych licencji.
3. Konfiguracja stacji zarządzającej.
4. Dołączenie klientów do system backupu.
5. Zdefiniowanie zadań backupu oraz przypisanie do nich harmonogramu automatycznego wykonywania:
	1. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące;
	2. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy;
	3. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu;
	4. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową;
	5. musi istnieć możliwość odtworzenia:
		1. całej wirtualnej maszyny;
		2. dysku wirtualnej maszyny;
		3. pojedynczych plików wirtualnej maszyny (zamontowanie pliku z kopią zapasową w systemie operacyjnym gościa);
6. Zdefiniowanie powiadomień o przebiegu zadania (Zamawiający wymaga skonfigurowania powiadomień na wskazany adres email zawierających, co najmniej:
	1. Nazwę zadania backupu
	2. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/
	3. Długość trwania zadania backupu
	4. Ilość zapisanych na taśmie danych
7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach:
	1. Błąd urządzenia
	2. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi
	3. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi
	4. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi
	5. Zdarzenia dotyczące licencji
	6. Zapełnienia mail-slotu
8. Uruchomienie testowych zadań backupu
9. Weryfikacja poprawności wykonania kopii zapasowej / weryfikacja działania powiadomień email
10. Uruchomienie testowych zadań odtworzenia danych
11. Miejscem przechowywania kopii zapasowych jest:
	1. serwer backupu.
	2. NAS
12. na etapie wdrożenia należy ustalić czasy RPO (okresu czasu przez jaki dane mogą być utracone w wyniku awarii) i RTO (okresu czasu w ciągu którego system, który uległ awarii powinien zostać przewrócony) z Zamawiającym
13. System musi zostać podłączony do klastra wirtualizacyjnego, celem wykonywania backupu pełnych maszyn wirtualnych – przechowywanych na serwerze backupu.
 |
|  | **System EDR** | Zamawiający wymaga podniesienia wersji aktualnie posiadanego oprogramowania antywirusowego do wersji posiadającej moduł XDR.System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem.Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.  |
|  | **System NAC** | System należy skonfigurować według zaproponowanych wytycznych przez Wykonawcę z uwzględnieniem wymagań Urzędu. Zakres konfiguracji musi zostać zaakceptowany i ustalony z administratorem.Po przeprowadzanej aktualizacji wymagane jest przeszkolenie administratora z całości systemu ze szczególnym uwzględnieniem nowych funkcjonalności.  |
|  | **Usługa katalogowa.** | **Instalacja, aktualizacja usługi katalogowej wraz z dodatkowymi komponentami w taki sposób, aby spełnione były poniższe wymagania celem świadczenia e-usług publicznych:** |
| * 1.
 | **Zaplanowanie liczby serwerów na potrzeby usługi katalogowej oraz serwerów plików** | Taka liczba serwerów, aby w przypadku awarii pojedynczego serwera był zapewniony ciągły dostęp do usługi katalogowej, a w szczególności mechanizmy uwierzytelniania oraz rozwiązywania nazw oraz serwera plików. Zamawiający dopuszcza wykorzystanie serwerów wirtualnych uruchomionych na dostarczonym środowisku wirtualizacyjnym. |
| * 1.
 | **Wersja systemu operacyjnego serwerów** | Zastosowany system operacyjny musi zapewniać, co najmniej:1. możliwość uruchomienia usługi katalogowej w trybie usługi
2. możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń
3. możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń)
4. możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI
5. możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych
 |
| * 1.
 | **Instalacja systemu operacyjnego serwerów** | Instalacja systemu operacyjnego serwerów w taki sposób, aby w łatwy sposób możliwe było włączenie funkcji szyfrowania partycji systemowej za pomocą wbudowanych w system operacyjny mechanizmów. Po instalacji systemy operacyjne muszą zostać prawidłowo aktywowane. Następnie należy zainstalować niezbędne aktualizacje oraz poprawki związane z bezpieczeństwem udostępnione przez producenta systemu operacyjnego. |
| * 1.
 | **Uruchomienie usługi katalogowej oraz niezbędnych komponentów, migracja danych do/z obecnej usługi katalogowej** | Uruchomienie usługi katalogowej, komponentów odpowiedzialnych za rozwiązywanie nazw. Usługa katalogowa musi być uruchomiona na wszystkich serwerach przewidzianych do rozbudowy. Na wszystkich serwerach muszą być uruchomione także komponenty odpowiedzialne za rozwiązywanie nazw. Należy szczególną uwagę zwrócić na poprawne funkcjonowanie mechanizmów replikacji. Usługę katalogową należy skonfigurować w taki sposób, aby możliwe było wykorzystanie możliwie wszystkich funkcjonalności oferowanych przez zastosowane systemy operacyjne, a w szczególności możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń, możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem.Utworzenie struktury jednostek organizacyjnych na podstawie schematu organizacyjnego dostarczonego przez Zamawiającego.Zamawiający wymaga skonfigurowania delegacji uprawnień do zadanych jednostek organizacyjnych dla administratorów niższego poziomu. Administratorzy niższego poziomu powinni mieć uprawnienia do:1. Resetowania haseł użytkowników
2. Odblokowywania kont użytkowników
3. Zmiany atrybutów „Display Name” oraz „Last name”

Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi:1. Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości
2. Śledzenie zmian dotyczących tworzenia, usuwania obiektów

Zamawiający wymaga skonfigurowania dwóch stacji zarządzających. Zarządzanie środowiskiem będzie się odbywać z poziomu stacji zarządzających (usługa katalogowa, wszystkie możliwe do zarządzania z poziomu stacji zarządzającej komponenty serwerów). |
| * 1.
 | **Konfiguracja polityki haseł oraz polityki blokowania kont** | Konfiguracja globalnej polityki haseł dla domeny:1. Hasło musi zawierać minimum 8 znaków
2. Maksymalny czas ważności hasła: do ustalenia z Zamawiającym
3. Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym
4. Hasło musi spełniać zasady złożoności

Konfiguracja polityki haseł dla kadry zarządzającej:1. Hasło musi zawierać minimum 10 znaków
2. Maksymalny czas ważności hasła: 30 dni
3. Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni
4. Hasło musi spełniać zasady złożoności

Po 3 nieudanych próbach uwierzytelniania konto powinno być blokowane na 30 minut. Automatyczne anulowanie blokady ma następować po 480 minutach.Szczegółowe dane zostaną przekazane na etapie konfiguracji. |
| * 1.
 | **Stworzenie skryptów służących do tworzenia struktury usługi katalogowej** | Po oddaniu wdrożonego systemu do eksploatacji konieczne będzie tworzenie nowych kont użytkowników, grup zabezpieczeń oraz jednostek organizacyjnych. Zamawiający oczekuje stworzenia przez Wykonawcę skryptów ułatwiających te zadania.**Założenia skryptu tworzącego nowe jednostki organizacyjne oraz grupy:**1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie, co najmniej:
	1. ścieżki i nazwy pliku wejściowego
	2. ścieżki i nazwy pliku logującego
	3. ścieżki i nazwy pliku wyjściowego (właściwego skryptu)
	4. nazwy FQDN domeny
	5. nazwy NetBIOS domeny
	6. nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty
	7. ścieżek do udziałów dyskowych SHARE1 oraz SHARE2
2. Skrypt ma pobierać z pliku wejściowego listę jednostek organizacyjnych
3. Skrypt tworzy nowe jednostki organizacyjne w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu
4. Skrypt tworzy nowe grupy zabezpieczeń o nazwie G\_Nazwa\_Jednoski\_Organizacyjnej
5. Skrypt tworzy foldery:
	1. \\DOMENA\Public\SHARE1
	2. \\DOMENA\Public\SHARE2

 Foldery muszą posiadać tak ustawione parametry zabezpieczeń, aby użytkownicy nie mogli samodzielnie tworzyć nowych katalogów ani plików w lokalizacjach \\DOMENA\SHARE1 oraz \\DOMENA\SHARE2.1. Skrypt tworzy podkatalogi: [\\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE1/Nazwa_Jednostki_Organizacyjnej) oraz [\\DOMENA\Public\SHARE2\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE2/Nazwa_Jednostki_Organizacyjnej)
2. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń:
	1. [\\DOMENA\Public\SHARE1\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/SHARE1/Nazwa_Jednostki_Organizacyjnej):
		1. Administratorzy Domeny – Pełna kontrola
		2. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej
		3. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu
		4. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze
	2. [\\DOMENA\Public\Share2\Nazwa\_Jednostki\_Organizacyjnej](file://DOMENA/Public/Share2/Nazwa_Jednostki_Organizacyjnej):
		1. Administratorzy Domeny – Pełna kontrola
		2. Grupa G\_Nazwa\_Jednostki\_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa\_Jednostki\_Organizacyjnej
		3. Użytkownicy Uwierzytelnieni - Odczyt
		4. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu
		5. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze
3. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina)
4. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania

**Założenia skryptu tworzącego nowe konta użytkowników:**1. Możliwość skonfigurowania za pomocą zmiennych w skrypcie co najmniej:
	1. ścieżki i nazwy pliku wejściowego
	2. ścieżki i nazwy pliku logującego
	3. ścieżki i nazwy pliku wyjściowego (właściwego skryptu)
	4. nazwy FQDN domeny
	5. nazwy NetBIOS domeny
	6. nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty
	7. ścieżki do udziału sieciowego HOME
	8. litery dysku katalogu domowego
2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie:

 NazwaUzytkownika;Imie;Nazwisko:Haslo;Dzial;NumerTelefonu1. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego
2. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania
3. Skrypt tworzy katalog [\\DOMENA\HOME\NazwaUzytkownika](file://DOMENA/HOME/NazwaUzytkownika)
4. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń:
	1. Administratorzy Domeny – Pełna kontrola
	2. Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika
	3. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu
	4. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze
5. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową
6. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina)
7. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania
8. Skrypt ma wygenerować dla każdego zakładanego konta osobny plik tekstowy zawierający między innymi: Nazwę użytkownika, Imię, Nazwisko, Hasło do pierwszego zalogowania. Tak utworzone pliki mogą zostać wydrukowane i przekazane użytkownikom.

Powyżej opisane skrypty muszą posiadać w treści kodu stosowne komentarze opisujące działanie skryptów. Skrypty zostanę przekazane Zamawiającemu w wieczyste użytkowanie bez dodatkowych opłat wraz ze stosowną dokumentacją użytkownika oraz szczegółową instrukcja obsługi.Zamawiający wymaga wygenerowania kont użytkowników, katalogów domowych użytkowników, jednostek organizacyjnych, grup zabezpieczeń za pomocą opracowanych skryptów. |
| * 1.
 | **Skonfigurowanie mapowania zasobów sieciowych** | Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows.Mapowane mają być między innymi zasoby:\\DOMENA\Public\SHARE1\\DOMENA\Public\SHARE2Oraz określone przez Zamawiającego drukarki sieciowe.Zamawiający wymaga skonfigurowanie mapowania dysków sieciowych za pomocą zasad grup na dwa sposoby:1. Z wykorzystaniem skryptów logowania
2. Z wykorzystaniem mechanizmów zaimplementowanych w systemach Microsoft Windows Vista i nowszych (Wymagane jest także skonfigurowanie automatycznej instalacji niezbędnych składników na stacjach klienckich. Zamawiający nie dopuszcza instalacji wymaganych składników ręcznie).
 |
| * 1.
 | **Uruchomienie i skonfigurowanie serwera plików oraz wydruków** | Zamawiający wymaga uruchomienie oraz skonfigurowanie serwerów plików oraz serwerów wydruków tak, aby były spełnione poniższe założenia:Serwery plików muszą być skonfigurowane z wykorzystaniem dostępnych w zaoferowanych systemach operacyjnych serwerów mechanizmów zwiększających dostępność danych poprzez zastosowanie technologii replikacji systemu plików. Konieczność taka podyktowana jest zapewnieniem ciągłości dostępu do krytycznych danych Wnioskodawcy w przypadku awarii jednego z serwera plików. Zastosowane mechanizmy replikacji systemu plików muszą zapewniać:* Replikację multi-master z rozwiązywaniem konfliktów
* Wykorzystanie algorytmów kompresji danych wykrywających zmiany na poziomie bloków danych w obrębie plików – replikacji podlegają tylko zmienione bloki danych, a nie całe pliki.

Serwery plików muszą być skonfigurowane w taki sposób, aby ograniczać ekspozycję danych dla użytkowników oraz grup, które nie mają do nich dostępu.Na serwerach plików muszą być skonfigurowana przydziały dyskowe dla użytkowników i grup. Zamawiający wymaga także skonfigurowania przydziałów dyskowych dla wskazanych folderów.Zamawiający wymaga włączenia i skonfigurowania mechanizmów uniemożliwiających przechowywanie niedozwolonych typów plików. Konieczne jest także skonfigurowanie mechanizmów raportujących.Zamawiający wymaga skonfigurowania mechanizmów przekierowania lokalnych folderów „Moje Dokumenty” oraz „Pulpit” ze stacji roboczych na serwery plików. Funkcjonalność ta musi poprawnie działać dla systemów klienckich Zamawiającego.Zamawiający wymaga stworzenie domyślnego, obowiązującego profilu wędrującego dla klienckich systemów operacyjnych. Domyślny profil ma uwzględniać opracowanie i wykonanie grafiki na pulpit komputera klienta. Grafika będzie akceptowana przez Zamawiającego. Zamawiający wymaga stworzenia i przypisania odpowiednich polityk globalnych dla wymuszenia stosowania obowiązkowych (niemodyfikowalnych) profili mobilnych.Zamawiający wymaga opracowania koszyka dozwolonych aplikacji wraz z implementacją polityk globalnych ograniczających dostęp do aplikacji z wykorzystaniem np.: dedykowanych ustawień związanych z polityką kontroli uruchomienia aplikacji.Zamawiający wymaga skonfigurowania parametrów audytu dla serwerów plików umożliwiających między innymi:1. Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder
2. Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder
3. Określenia daty, czasu, nazwy użytkownika, który próbował uzyskać nieuprawniony dostęp do zasobów, do których nie ma uprawnień.

Zamawiający wymaga uruchomienia serwera wydruków oraz podłączenia i skonfigurowania drukarek sieciowych. Zamawiający wymaga opracowania i skonfigurowania odpowiednich polityk globalnych mapujących odpowiednie drukarki użytkownikom. Niedopuszczalne jest przyłączenie wszystkim użytkownikom wszystkich dostępnych drukarek. Użytkownicy powinni mieć przyłączone drukarki znajdujące się najbliżej jego komputera. |
| * 1.
 | **Serwery uwierzytelniające** | Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych.Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach.Instancja serwera może być uruchomiona na serwerach domenowych z zastrzeżeniem, że będzie ona kompatybilna z usługami uruchomionymi na tych serwerach i nie będzie wpływać negatywnie na ich pracę.Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach.Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie. |
|  | **Uruchomienie usług umożliwiającą instalację i zarządzanie aktualizacjami stacji roboczych Windows** | Zamawiający wymaga uruchomienia i skonfigurowania usług dostępnych w dostarczonych systemach operacyjnych serwerów umożliwiających zarządzanie aktualizacjami stacji roboczych i serwerów Windows według założeń:1. Aktualizacje i poprawki mają być pobierane na serwer instalacyjny za pośrednictwem sieci Internet
2. Administrator zatwierdza aktualizacje do instalacji
3. Stacje robocze i serwery pobierają i automatycznie instalują zatwierdzone przez Administratora aktualizacje według określonego harmonogramu

Zamawiający wymaga skonfigurowania co najmniej następujących parametrów:1. Systemów operacyjnych, aplikacji oraz wersji językowych, dla których będą pobierane aktualizacje
2. Kategorii aktualizacji
3. Grup komputerów (KOMPUTERY, SERWERY, KOMPUTERY-TEST, SERWERY-TEST)
4. Polityk globalnych przypisujących komputery znajdujące się w określonych jednostkach organizacyjnych do odpowiednich grup komputerów
5. Zasad automatycznego zatwierdzania nowych aktualizacji.
6. Mechanizmów raportowania (email)
 |
|  | **Przygotowanie infrastruktury PKI** | Zamawiający wymaga przygotowania i uruchomienia wewnętrznej infrastruktury PKI. Zamawiający posiada stacje robocze pracujące w oparciu o następujące systemy operacyjne: Windows 10, 11. Wymagana przez Zamawiającego konfiguracja zawiera co najmniej:1. Zaplanowanie i uruchomienie wewnętrznej struktury CA
2. Konfiguracja szablonów certyfikatów
3. Wydanie certyfikatów dla serwerów oraz stacji roboczych
4. Zastosowanie mechanizmów bezpieczeństwa poprzez możliwość backupu archiwizacji kluczy prywatnych wydawanych certyfikatów.
5. Wskazanie wszystkich możliwych dróg publikacji list CRL
6. Instalacji i konfiguracji stacji (komputer PC) do wydania kart – stacja do personalizacji.
 |
|  | **Testowanie i modyfikacja parametrów infrastruktury sieciowej.** | 1. Testowanie mechanizmów bezpieczeństwa klastra wirtualizacyjnego.
2. Testowanie wydajności przesyłu i zapisu danych do środowiska LAN.
3. Testowanie mechanizmów replikacji danych.
4. Testowanie dostępu publicznego do zasobów.
5. Testy wydajnościowe połączeń pochodzących z Internetu i wychodzących z zasobów lokalnych do Internetu
6. Testowanie autoryzowanego dostępu do wewnętrznych zasobów.
7. Wprowadzanie koniecznych modyfikacji konfiguracji urządzeń sieciowych po przeprowadzonych testach
 |
|  | **Asysty stanowiskowe** | Asysta stanowiskowa ma obejmować 16 godzin szkoleniowych w ujęciu 8 godzin na jeden dzień. Całość powinna się zamknąć w okresie 2 dni i ma dotyczyć autorskiego rozwiązania zrealizowanego w ramach podmiotowego wdrożenia.Asysta musi być warunkiem dopuszczający do przekazania rozwiązania technicznego do wykorzystania produkcyjnego. Asysta stanowiskowa musi zostać odebrana i zatwierdzona protokołem odbioru sygnowanym przez obie strony projektu tj. wykonawcę oraz użytkownika końcowego. |
|  | **Termin wykonania prac instalacyjno-wdrożeniowych. Oddanie systemu do eksploatacji.** | Wszystkie wymienione prace wdrożeniowe muszą zostać wykonane wspólnie z przedstawicielem Zamawiającego, z każdego etapu prac powinien zostać sporządzony protokół. Powyższe czynności należy wykonać w okresie realizacji Zamówienia po wcześniejszym uzgodnieniu harmonogramu wdrożenia z Wnioskodawcą. **Wykonawca jest zobowiązany do zapewnienia wsparcia technicznego w postaci jednej osoby w siedzibie Zamawiającego w ciągu pierwszego dnia roboczego następującego po pracach wdrożeniowo – instalacyjnych w godzinach od 8.00 do 15.30.** W tym czasie przedstawiciel Wykonawcy:* zobowiązany jest do rozwiązywania problemów technicznych, które wystąpią na etapie oddawania systemu do eksploatacji.
* dokona prezentacji działania sytemu dla pracowników Zamawiającego z zakresu zastosowanych technologii oraz poprawnej eksploatacji wdrożonych rozwiązań, a w szczególności:
1. zastosowanej technologii serwerów
2. zastosowanej technologii pamięci masowej
3. wirtualizacji
4. systemu backupu
5. sieci WiFi
6. Firewall z centralnym systemem logów
7. zastosowanych rozwiązań aplikacyjnych

Wykonawca zapewni również wparcie techniczne ze strony inżynierów w okresie trwania realizacji projektu. Wsparcie polegałoby na pomocy zdalnej lub telefonicznej przy rozwiązaniu problemów, które ewentualnie pojawią się podczas eksploatacji ww. rozwiązania. |
|  | **Opracowanie dokumentacji powykonawczej** | Zamawiający wymaga opracowania szczegółowej dokumentacji technicznej użytkownika (w formie papierowej i elektronicznej) obejmującej wszystkie etapy wdrożenia całości systemu. Wykonawca jest zobowiązany do przygotowania w formie papierowej i elektronicznej procedur eksploatacyjnych systemu.1. Wszelkie zmiany w stosunku do Dokumentacji systemu z podaniem ich powodów.
2. Konfiguracje urządzeń (lub opisy konfiguracji w przypadku sprzętu lub oprogramowania nieumożliwiającego eksportu konfiguracji do pliku tekstowego bądź posiadające rozproszoną konfigurację).
3. Dyski instalacyjne dostarczonego oprogramowania, jeżeli takowe występowały.
4. Kody dostępowe oraz klucze licencyjne, jeżeli takowe występowały.
5. Opis typowych czynności, prac administracyjnych, które pozwalają na codzienną obsługę dostarczonego sprzętu, systemów.
 |
|  | **Opieka serwisowa** | Zamawiający wymaga świadczenia opieki serwisowej przez okres 12 miesięcy z czasem reakcji na zaistniałe problemy wynoszącym 4 godziny. Czas reakcji jest rozumiany jako podjęcie działań mających na celu rozwiązanie zaistniałych problemów technicznych. |