Załącznik nr 1
Szczegółowy opis przedmiotu zamówienia

Zatwierdzam:

WÓJT
mgr Bogusław Kręcisz

GMINA SKOŁYSZYN
38-242 Skołyszyn 12
tel./fax 13 44 910 62 (63) (64)
NIP 685-16-51-203 REGON 370440382
BS O/ Skołyszyn
76 8627 1037 2003 5000 0459 0001

Gmina Skołyszyn
Październik 2024

Spis treści

1. 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;

2. 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.

3. 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.

4. Zestawienie zakresu dostaw i usług.

Lp.	Nazwa	Wymagana minimalna długość gwarancji (m-ce)	Ilość	Jednostka miary	Uwagi
1.	Serwer backup	24	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. 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.
2.	Przełącznik sieci LAN IDF	Wieczysta (Life time)	8	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.
3.	Przełącznik sieci LAN CORE	Wieczysta (Life time)	2	Szt.	
4.	Licencje CAL	Nd.	20	Szt.	Pozwoli na instalacje oprogramowania – serwerów wirtualnych pod systemy cyberbezpieczństwa, dołączenie ich do centralnej bazy użytkowników -

					usługa katalogowa. Zapewni wykorzystanie mechanizmów kontroli dostępu do danych takich jak: uprawnienia użytkowników, grupy użytkowników i zarządzanie uprawnieniami, praca zdalna, regularne aktualizacje oprogramowania dla systemów klienckich.
5.	System EDR-XDR	24	130	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.
6.	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).
7.	Access Point	24	40	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.
8.	Kontroler sieci Wi-Fi	24	1	Szt.	
9.	UPS	24	1	Szt.	Urządzenie pozwoli na podłączenie zakupionych urządzeń w bezpieczny sposób do sieci elektrycznej zapewniając właściwe warunki pracy w momencie braku zasilania. Zwiększy poziom bezpieczeństwa przechowywanych danych, eliminując zagrożenie utarty danych w wyniku niewłaściwego, nagłego wyłączenia urządzeń.
10.	Instalacja, konfiguracja, wdrożenie.	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.

5. Szczegółów opis pozycji.

5.1. 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;
- 1 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;
        - 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

- 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.

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;
- Serwer musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w UE;
- Ogólnopolska, telefoniczna infolinia/linia techniczna producenta serwera;
- 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.

5.2. Przełącznik sieci LAN IDF – szt. 8 - wymagania minimalne

1. Typ i liczba portów:
   - 48 portów 10/100/1000BaseT RJ-45 PoE (802.3at PoE+, 802.3af) + uplink 4x10G SFP
   - Moc dostępna dla PoE: 375W (wsparcie dla wszystkich 48 portów jednocześnie),
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): 175 Gb/s (full duplex),

- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 130.00 Mpps
- Pamięć DRAM – 1 GB
- Pamięć flash – 512 MB
- Wielkość bufora pakietów - 1.5 MB
- Obsługa:
  - 4000 aktywnych sieci VLAN
  - 15000 adresów MAC
  - 900 statycznych tras IPv4
  - 16 statycznych tras IPv6
  - 128 interfejsów SVI L3
  - Obsługa ramek Ethernet Jumbo
  - 1024 grupy IGMP
  - 8 połączeń zagregowanych typu „port channel"
  - 8 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

6. Porty dostępowe przełącznika posiadają zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)
7. Obsługa protokołu NTP
8. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping
9. 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-MED
12. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC
10. Urządzenie wspiera połączenia link aggregation zgodnie z IEEE 802.3ad
11. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
12. Możliwość uruchomienia funkcji serwera DHCP
13. 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,

14. 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.
15. 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;
16. Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6,
17. 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,
18. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.),
19. 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,
20. 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;
21. Możliwość montażu w szafie rack 19".
22. Wysokość urządzenia 1 RU.

5.3. Przełącznik sieci LAN Core – szt. 2 - wymagania minimalne

Przełącznik wielowarstwowy L2/L3, zarządzany

Typ i liczba portów: 12 portów 10GBaseT i 12 portów SFP+ lub równoważnie 24 poty 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-C/RJ45
Porty dostępowe przełącznika zgodne ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet)

Parametry wydajnościowe:

- Przepustowość przełącznika (switching bandwidth) 480 Gb/s
- Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów 240 Mpps
- Pamięć DRAM – 512 MB
- Pamięć flash – 256 MB
- Procesor wbudowany 1,3 GHz
- Wielkość bufora pakietów - 3 MB
- 2 000 grup IGMP
- 8 grupy połączeń zagregowanych typu „port channel" LACP
- 8 linków w ramach jednego połączenia zagregowanego typu „port channel" LACP
- 1 000 wpisów w listach kontroli dostępu ACL
- 8 kolejek sprzętowych

Obsługa:

- 4 090 aktywnych sieci VLAN
- 16 000 adresów MAC
- 900 statycznych tras IPv4
- 128 interfejsów L3

Obsługa ramek Ethernet Jumbo 9 000 B

Możliwość łączenia do 4 jednostek w stos poprzez porty 10 GE, zarządzane jako jeden system z funkcją failover active/standby
Funkcjonalność cross-stack QoS, VLAN, LAG i port mirroring

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 126 instancji protokołu STP

Funkcje wirtualnej sieci LAN: Voice VLAN, Protocol based VLAN
Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego
Protokół 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 Ethernet

Obsługa protokołu NTP
Funkcje DHCP server, DHCP relay
Obsługa IGMPv1/2/3 i MLDv1/2 Snooping, DHCP snooping
Blokowanie Head of Line (HOL)

Zabezpieczenie przed wejściem w pętlę Unidirectional Link Detection (UDLD)
Zapobieganie atakom DoS

Obsługa mechanizmów routingu statycznego dla IPv4 i IPv6
Routing dynamiczny RIP v2

Zarządzanie

- 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 & Play
Przycisk reset
Certyfikaty: UL 60950, FCC 15 A, CSA 22.2, CE mark lub równoważne
Zasilanie 230V AC
Wysokość maksymalnie 1U, montowany w szafie typu RAC 19''

5.4. Licencje CAL – szt. 20 – wymagania minimalne

Licencje dostępowe do posiadanych systemów operacyjnych (Windows Serwer 2022) w ilości 20 szt.
Oferowane licencje muszą udostępnić możliwość korzystania z zasobów serwisów 20 użytkownikom.

5.5. System EDR-XDR – szt. 130 – 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.

17. 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.
18. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla rozwiązania i mogą stanowić zagrożenie bezpieczeństwa.
19. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
20. Rozwiązanie musi posiadać tylko jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
21. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
22. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
23. 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.

24. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
25. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.

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

9. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
10. Rozwiązanie musi posiadać system zapobiegania włamaniom działający na hoście (HIPS).
11. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
12. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
13. 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.
14. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
15. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
16. Rozwiązanie musi zapewniać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
17. Rozwiązanie musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.

Dodatkowe wymagania dla ochrony serwerów Linux:

18. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
19. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
20. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

21. 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.

6. Rozwiązanie musi zapewniać administratorowi podejrzenie listy zainstalowanych aplikacji.
7. 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.
13. 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.
14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. 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.

5.6. 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 100 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.
11. System musi posiadać funkcjonalność serwerów:
    - serwera RADIUS dla infrastruktury sieciowej,
    - serwera OTP dla infrastruktury VPN, Captive Portal, Tacacs+,
    - serwera SYSLOG,
    - serwera TACACS+,
    - serwera Monitoringu,
    - serwera DHCP,
    - serwera polityk uwierzytelniania i kontroli dostępu 802.1X,
    - serwera WWW (HTTP/HTTPS) dla uwierzytelnienia gościnnego.
12. System musi umożliwiać realizację wysokiej dostępności elementów funkcjonalnych, poprzez zapewnienie redundancji dla modułów realizujących dostępu do sieci i DHCP.
13. System musi umożliwiać uwierzytelnianie administratorów za pomocą wewnętrznej bazy użytkowników i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgreSQL, Oracle, ODBC.
14. System musi umożliwiać uwierzytelnianie tożsamości i urządzeń końcowych za pomocą wewnętrznej bazy i/lub zewnętrznych systemów autoryzacji w tym OpenLDAP, Microsoft ActiveDirectory, Google G Suite, WebServices/API, Radius, relacyjnych baz danych: min MySQL, MSSQL, MariaDB, PostgresSQL, Oracle, ODBC.
15. 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.
16. Podczas synchronizacji musi umożliwiać mapowanie grup lokalnych z grupami zdalnymi, atrybutami Active Directory, tworzenia lokalnych haseł, certyfikatów, wysłania konfiguracji dostępowych poprzez email.

17. System musi wspierać funkcjonalność API dla masowych operacji CRUD (Create, Read, Update, Delete) na obiektach systemu oraz procedur blokowania dostępu do sieci.
18. System musi mieć możliwość autoryzacji protokołem NTLM z wieloma serwerami Microsoft Active Directory, także nie połączonych relacjami zaufania.
19. System musi mieć możliwość obsługę wielu PKI dla różnych grup użytkowników.
20. System musi posiadać funkcjonalność tworzenia kont administracyjnych z konfigurowalnym dostępem do dowolnych spośród wszystkich funkcjonalności systemu oraz do dowolnych obiektów utworzonych i/lub zarządzanych w systemie.
21. System musi mieć możliwość zmiany parametrów kont Microsoft Active Directory (min. Login, Hasło, Imię, Nazwisko, Email, Status).
22. System musi posiadać funkcjonalność konfiguracji praw kontroli dostępu do poszczególnych elementów menu interfejsu oraz obiektów na poziomie ich dodawania, edycji, kasowania.
23. Interfejs graficzny systemu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim i polskim).
24. System musi umożliwiać kontrolę dostępu do interfejsu graficznego administratora na podstawie adresu IP lub podsieci.
25. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, mac adres, urządzenie końcowe, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony Vlan z przydzielonym adresem IP.
26. System musi zapewniać scentralizowane monitorowanie urządzeń sieciowych. W systemie musi być dostępny dedykowany interfejs graficzny, na którym dostępny jest podgląd wszystkich portów i modułów zarządzanego urządzenia.
27. System musi umożliwiać monitoring urządzeń sieciowych oraz końcowych za pomocą protokołu min. SNMP.
28. System musi umożliwiać zbieranie danych inwentaryzacyjnych, ich zmian oraz sprawdzanie kondycji urządzeń sieciowych oraz końcowych za pomocą min. protokołu SNMP.
29. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu, zapisu konfiguracji zmian, konfiguracji ustawień portu z zakresu min. VLANów, Autoryzacji, Statusu, Opisu.
30. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
31. System musi posiadać możliwość konfiguracji serwera DHCP dla stworzonych podsieci IP.
32. System musi umożliwiać konfigurację własnych szablonów przesyłanych wiadomości e-mail oraz wydruku poświadczeń dostępu do sieci.
33. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych oraz końcowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.
34. System musi posiadać funkcjonalność wysyłania zdarzeń np. do systemów SIEM minimum protokołem Syslog informacji z serwerów autoryzacji, DHCP, VPN, OTP.
35. System musi posiadać mechanizm tworzenia cyklicznej kopii bezpieczeństwa lokalnie lub na udziałach zewnętrznych.
36. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).
37. System musi posiadać możliwość logowania w oparciu o portale społecznościowe, minimum: Facebook i Google, LinkedIn.
38. System musi posiadać możliwość wysyłania danych rejestracyjnych poprzez email, bramkę SMS oraz zapasową bramkę SMS.
39. System musi posiadać funkcję personalizacji strony gościnnej.
40. Captive Portal musi się automatycznie dostosować formatem do podłączonego urządzenia końcowego min: komputer, tablet, telefon.
41. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor.
42. Captive Portal musi mieć możliwość włączenia dwuskładnikowego uwierzytelniania konta (OTP) minimum za pomocą tokenu wygenerowanego na Google Authenticatorze lub wysłanego przez bramkę SMS oraz zapasową bramkę SMS.
43. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.
44. Captive Portal musi posiadać możliwość zmiany hasła kont lokalnych oraz Microsoft Active Directory.
45. Captive Portal musi umożliwiać logowanie typu HotSpot za pomocą kodu dostępu.

46. Captive Portal musi umożliwiać tworzenie dynamicznych pól formularza rejestracyjnego, np.: pole tekstowe, lista wyboru.
47. Interfejs graficzny Captive Portalu musi być dostępnym w różnych wersjach językowych (min. w języku angielskim, polskim, niemieckim, hiszpańskim, francuskim i ukraińskim).
48. Captive Portal musi posiadać możliwość pobrania konfiguracji dla OTP.
49. Captive Portal powinien wspierać automatyczne kasowanie wygasłych kont gościnnych: na żądanie, okresowo wg zadanej liczbie dni.
50. Captive Portal powinien umożliwiać konfiguracje maksymalnej ilości nieudanych logowań.
51. System musi umożliwiać budowanie powiązań urządzeń sieciowych minimum za pomocą protokołów LLDP, CDP.
52. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą protokołu, min. Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego.
53. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.
54. System powinien posiadać mechanizm rozłączania sesji min SNMP, komend CLI, RADIUS CoA zgodnie z RFC 5176.
55. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.
56. System musi obsługiwać różne metody profilowania do wykrywania typu 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.
57. System musi umożliwiać integracje z zewnętrznymi rozwiązaniami typu MDM (min. AirWatch, IBM MaaS, MobileIron, Microsoft Intune, Google Workspace, Famoc).
58. System musi posiadać funkcjonalność dwuskładnikowego uwierzytelniania konta (OTP) realizowaną poprzez tworzenie tokenu w Google Authenticator i SMS, minumum na systemach: FortiGate, Pulse Secure, OpenVPN, Palo Alto, Cisco ASA.
59. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa co najmniej:
    - Czy system jest aktualny z możliwością automatycznego naprawienia niezgodności
    - Czy włączony jest firewall
    - Czy jest uruchomiony system antywirusowy i aktualna baza sygnatur
    - Czy jest włączone szyfrowanie dysku systemowego
    - Czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory
    - Czy na dysku znajdują się pliki lub katalogi wskazane przez administratora
    - Czy w systemie są uruchomione procesy wskazane przez administratora
    - Czy w systemie są uruchomione usługi wskazane przez administratora z możliwością automatycznego naprawienia niezgodności
    - Czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
        - Wartości klucza rejestru
        - Typu wartości: Number, String, Version
60. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.
61. System musi współpracować z serwerem tokenów.
62. System musi posiadać mechanizm autokonfiguracji sieci (autokonfiguratory sieci) urządzeń końcowych (sieci przewodowej i bezprzewodowej) bez potrzeby angażowania pracowników działo IT dla systemów co najmniej:
    - Microsoft Windows
    - Mac OS
    - iOS
    - Android
63. System musi posiadać możliwość instalacji certyfikatu końcowego użytkownika poprzez mechanizm autokonfiguracji sieci (autokonfiguratory sieci).
64. System musi wspierać protokół IPv6 min dla konsoli SSH, komunikacji RADIUS, NTP, SNMP, komunikację z Microsoft Active Directory.

Mechanizmy uwierzytelniania

1. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.
2. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
   - MAC,
   - PAP/ASCII,
   - CHAP,
   - SNMP,
   - 802.1X.
3. wraz z możliwością wyboru szczegółowego sposobu uwierzytelniania np. IEEE 802.1x (PEAP), IEEE 802.1x (EAP-TLS), IEEE 802.1x (EAP-TTLS), MAC (PAP), MAC (CHAP), MAC (MD5), TEAP, itp.
4. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.
5. System musi umożliwiać uwierzytelnianie SNMP Trap urządzeń końcowych.
6. System musi wspierać implementację protokołu 802.1X z różnymi suplikantami (min. Windows XP, Windows Vista, Windows 7, Windows 8 i 8.1, Windows 10, Windows 11, Apple Mac OS X Supplicant, Apple iOS Supplicant, Google Android Supplicant, Ubuntu Supplicant).
7. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
   - Tożsamość/Urządzenie końcowe,
   - Grupa tożsamości/urządzeń końcowych,
   - Parametry urządzeń końcowych, min: system operacyjny, wersja,
   - Atrybuty Active Directory,
   - Jednostka organizacyjna tożsamości/urządzeń końcowych,
   - Urządzenia sieciowe sieci przewodowej, bezprzewodowej,
   - Grupy urządzeń sieciowych,
   - Porty urządzeń sieciowych,
   - Grupy portów urządzeń sieciowych,
   - Jednostka organizacyjna portów,
   - Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID),
   - Data, czas ważności polityki,
   - Wewnętrzny Captive Portal,
   - Metoda autoryzacji.
8. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów: Cisco Networks, Aruba Networks, Extreme Networks, Hewlett Packard Enterprise, Juniper Networks, Ruckus Networks, MicroTik, Ubiquiti Networks.
9. System musi wspierać funkcjonalność *IP-to-ID Mapping*, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.
10. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.
11. System musi posiadać możliwość wdrażania polityk w całej sieci za pomocą jednej konsoli.
12. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.
13. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.
14. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.
15. System musi umożliwiać tworzenie hasła dnia, dla tożsamości zarejestrowanych przez wewnętrzny Captive portal.
16. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o urządzenie końcowe i/lub w postaci zbiorczego pliku w formacie CSV. Lokalna baza urządzeń końcowych musi być tworzona per urządzenie końcowe na podstawie unikalnego adresu MAC.
17. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.
18. System musi wspierać funkcjonalność różnych typów autoryzacji na pojedynczym porcie urządzenia sieciowego: min. autoryzację pojedynczą, autoryzację wielokrotną, uwierzytelnianie urządzeń typu Voice

VLAN, równoczesną obsługę różnych typów autoryzacji skonfigurowanych na porcie i/lub autoryzację poprzez portal www.

19. System musi 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.
20. System musi umożliwiać integrację z EDUROAM w zakresie autoryzacji użytkowników.
21. 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.
2. Alarmy mogą być generowane w sytuacjach, min:
    - Ilości obsługiwanych transakcji RADIUS,
    - Opóźnienie obsługi transkacji RADIUS,
    - Statusu krytycznego modułów.
3. System musi posiadać zestaw narzędzi diagnostycznych dla rozwiązywania problemów, w tym:
    - badanie łączności IP za pomocą ping, traceroute,
    - tcpdump protokołów RADIUS, TACACS+,
    - wyszukiwanie zdarzeń RADIUS z uwzględnieniem:
        - nazwy użytkownika,
        - adresu MAC,
        - statusu uwierzytelnienia (udana lub nieudana),
        - powodu, jeżeli uwierzytelnienie nieudane,
        - zakresu czasowego, co do dnia, godziny i minuty,
    - wykonanie zdalnego polecenia na urządzeniu sieciowym.

5.7. Access point – szt. 40 – wymagania minimalne

Punkty dostępowy	
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/s 5 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

5.8. Kontroler Wi-Fi – szt. 1 – wymagania minimalne

Kontroler zgodny z zaoferowanymi punktami dostępowymi	
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
Zasilanie	Min. 802.3af PoE,
Dostęp	Poprzez przeglądarkę internetową
Temperatura pracy	W zakresie nie mniejszym niż 0 do 35° C

5.9. UPS – szt.1 – wymagania minimalne.

Lp.	Opis wymagań techniczno-funkcjonalnych	Konfiguracja minimalna Zamawiającego
1.	Technologia	VFI (true on-line, podwójne przetwarzanie energii)
2.	Moc znamionowa	6 kVA / 6 kW
3.	Wyjściowy współczynnik mocy (PF)	1.0
4.	Napięcie wejściowe	230 Vac
5.	Tolerancja napięcia wejściowego przy obciążeniu 70-100%; bez przechodzenia na baterie	138– 299 Vac
6.	Tolerancja napięcia wejściowego przy obciążeniu mniejszym od 70%; bez przechodzenia na baterie	110 – 299 Vac
7.	Częstotliwość wejściowa	Wymagana 40-70 Hz
8.	Sprawność AC-AC w trybie pracy on-line z obciążeniem 100%	nie mniejsza niż 95%
9.	Sprawność AC-AC w trybie pracy Oszczędzania energii Eco Mode	nie mniejsza niż 99%
10.	Tryb pracy z konwersją częstotliwości	Wymagana praca ze stałą częstotliwością wyjściową 50Hz, przy zasilaniu 60Hz lub odwrotnie.
11.	Napięcie wyjściowe	230 Vac
12.	Częstotliwość wyjściowa	50/60Hz (programowalna)
13.	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem	Wymagane
14.	Czas podtrzymania	5min dla obc 6kW
15.	Baterie	Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 10-12 lat i pojemności minimalnej 2160 V*Ah.
16.	Szafa baterii	Moduł baterii Rack o wysokości 3U
17.	Stabilizacja napięcia wyjściowego w stanie ustalonym	± 1%

18.	Stabilizacja napięcia wyjściowego w stanie nieustalonym	± 3%
19.	Współczynnik szczytu	3:1
20.	Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD w języku polskim oraz sygnalizacją akustyczną	Wymagane
21.	Złącze interfejsów	RS232, USB, REPO
22.	Wyjściowa listwa do wpięcia UPS do instalacji stałej	Wymagana możliwość podłączenia przewodów o przekroju min 6mm2
23.	Karta sieciowa SNMP	Wymagana
24.	Interfejs EPO (do wyłącznika ppoż.)	Wymagane
25.	Szyny Rack	Wymagane do montażu UPS i modułu baterii
26.	Diagnostyka parametrów urządzenia UPS i baterii	Automatyczna diagnostyka parametrów urządzenia UPS i baterii na panelu UPS-a i z wykorzystaniem oprogramowania do zarządzania i monitorowania UPS
27.	Oprogramowanie zapewniające pełny monitoring, zarządzanie i automatyczny shut-down systemu operacyjnego	Wymagane
28.	Poziom hałasu w odległości 1m,	< 50 dBA Wentylatory o regulowanej prędkości obrotowej w zależności od obciążenia i temperatury
29.	Możliwość regulacji z panelu sterującego tolerancji napięcia wejściowego i częstotliwości wejściowej w linii bypassu	Wymagane
30.	Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa ,kompatybilności elektromagnetycznej potwierdzone deklaracją zgodności CE	Wymagane
31.	Producent zasilacza UPS z siedzibą w Polsce, posiadający biuro dystrybucji i serwisu na terenie kraju.	Wymagane
32.	Certyfikat ISO 9001 oraz 14001 producenta zasilacza UPS	Wymagane
33.	Wymiary zasilacza UPS i baterii w szafie rack 19''	Maks 5U
34.	Instrukcja w języku polskim	Wymagane

5.10. Instalacja, konfiguracja, wdrożenie. – szt. 1 – wymagania minimalne

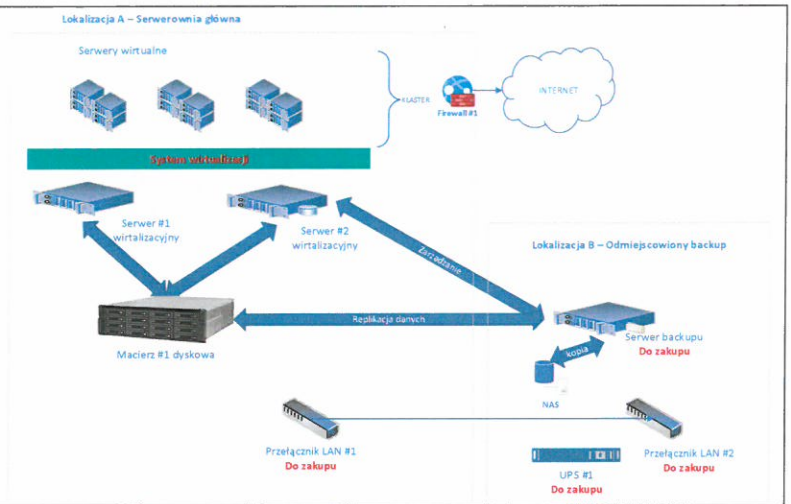
Usługi informatyczne w zakresie wdrożenia, konserwacji i serwisu sprzętu informatycznego oraz oprogramowania.		
1.	**Usługi**	Celem prac jest przygotowanie środowiska teleinformatycznego, na potrzeby realizacji elementów cyberbezpieczeństwa, zbudowanego w oparciu o dostarczone urządzenia sprzętowe i 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: a) Sporządzenia Planu Wdrożenia uwzględniającego fakt wykonania wdrożenia bez przerywania bieżącej działalności Zamawiającego oraz przewidującego rozwiązania dla sytuacji kryzysowych wdrożenia. b) Sporządzenia Dokumentacji Systemu według której nastąpi realizacja. Dokumentacja Systemu musi być uzgodniona z Zamawiającym i zawierać wszystkie aspekty wdrożenia. W szczególności: i. koncepcję techniczną projektu, która powinna zawierać opis mechanizmów działania systemu z wykorzystaniem dostarczonych i rozbudowywanych elementów sprzętowych. ii. schematy połączeń iii. mechanizmy działania głównych elementów sprzętowych: • sieć LAN - przełączniki sieciowe • klaster wirtualizacyjny • system backupu i archiwizacji danych • system serwerowy • system macierzowy • firewall/UTM iv. iii. mechanizmy działania głównych elementów programowych: • system EDR • system NAC • system domenowy/wirtualizacyjny • system backupu v. testy systemu uwzględniające sprawdzenie wymaganych niniejszą specyfikacją funkcjonalności vi. sposób odbioru uzgodniony z Zamawiającym vii. listę i opisy procedur, wypełnianie których gwarantuje Zamawiającemu prawidłowe działanie systemu viii. opis przypadków, w których projekt dopuszcza niedziałanie systemu ix. realizacja wdrożenia nastąpi według Planu Wdrożenia po zakończeniu którego Wykonawca sporządzi Dokumentację Powykonawczą Odbiór wdrożenia nastąpi na podstawie zgodności stanu faktycznego z Planem Wdrożenia.
2.	**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: a. Stworzenia połączeń sieci LAN pomiędzy przełącznikami. b. Podłączenia urządzeń serwerowo-macierzowych (serwery, macierze) do przełączników sieci LAN. c. Połączenia powinny być zrealizowane z zachowaniem redundancji i agregacji połączeń na poziomie co najmniej n+1. d. Połączenia musza wykorzystywać dostępną, największą przepustowość portu pomiędzy łączonymi urządzeniami.
3.	**Instalacja i konfiguracja oprogramowania**	1. Konfiguracja oprogramowania do wirtualizacji wraz z wykreowaniem odpowiedniej liczby wirtualnych maszyn na potrzeby tworzonego rozwiązania IT z zachowaniem zgodności z ilością dostarczonych licencji. 2. Konfiguracja oprogramowania do systemu wykonywania backupu i archiwizacji danych działającego na serwerze backupu. 3. Instalacja i konfiguracja 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 systemów operacyjnych dla serwerów wirtualnych. 5. Instalacja i konfiguracja oprogramowania EDR. 6. Instalacja i konfiguracja oprogramowania NAC.
4.	**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: a. Przeprowadzenie audytu obecnej topologii oraz konfiguracji. b. Aktualizacja oprogramowania układowego do najnowszej stabilnej wersji oferowanej przez producenta urządzenia. c. Stworzenia odpowiednich konfiguracji STACK z wykorzystaniem dedykowanych modułów. d. Konfiguracja sieci wirtualnych VLAN – taka liczba sieci wirtualnych aby odseparować różne typy ruchu (ilość sieci VLAN należy określić w uzgodnieniu z Zamawiającym). e. Wymagane jest wydzielenie i skonfigurowanie co najmniej stref: • SERWERY • UŻYTKOWNICY WEWNĘTRZNI • UŻYTKOWNICY ZEWNĘTRZNI • MANAGEMENT f. Jeśli jest to konieczne – Zamawiający oczekuje rekonfiguracji adresacji IP w danych strefach (readresacja urządzeń, serwerów, komputerów leży po stronie Wykonawcy) g. Zamawiający wymaga skonfigurowania polityk ruchu pomiędzy strefami na urządzeniach firewall. h. Konfiguracja połączeń pomiędzy przełącznikami sieci LAN. i. Rozpięcie połączeń przełączników IDF na centralne przełączniki CORE z zachowaniem nadmiarowości z wykorzystaniem wszystkich dostępnych portów uplink. ii. Z wykorzystaniem połączeń światłowodowych oraz miedzianych. iii. Agregacja połączeń celem uzyskania pasma nx10Gbps w obu kierunkach ruchu. iv. 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. i. Konfiguracja sieci VLAN na wszystkich przełącznikach – konfiguracja propagacji sieci VLAN. j. Konfiguracja routingu pomiędzy sieciami VLAN na centralnym urządzeniu firewall - klaster; k. Zamawiający wymaga aby wszystkie sieci VLAN (L2) zostały rozpięte na warstwie L2 na urządzeniu firewall – (połączenie TRUNK). l. 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.

		m. Ustawienie serwera czasu dla urządzeń sieci LAN – przełączników sieciowych - na klaster firewall. n. Zamawiający wymaga instalacji i konfiguracji serwera logów dla urządzeń sieci LAN (maszyna wirtualna) – przełączników sieciowych, z graficznym interfejsem przeszukiwania. Zamawiający dopuszcza rozwiązania Open Source. o. 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. p. Wykonawcza skonfiguruje urządzenia aby raportowały, przesyłały dane do zainstalowanego serwera logów i monitorowania sieci. q. Testowanie obsługi ruchu sieciowego. r. Testowanie skuteczności zabezpieczeń.
5.	**Serwer backupu**	W ramach projektu przewiduje się wykorzystanie dostarczonego 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.

		
6.	**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.
7.	**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.
8.	**Aktualizacja/Uruchomienie środowiska wirtualizacyjnego.**	Zamawiający wymaga aktualizacji środowiska wirtualizacyjnego, co najmniej w zakresie: 1. Instalacja oprogramowania wirtualizacyjnego na dostarczonych serwerach. 2. Instalacja najnowszych poprawek do środowiska wirtualizacyjnego oferowanych przez producenta oprogramowania wirtualizacyjnego oraz przez producenta serwerów.

		3. 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. 4. 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. 5. Konfiguracja sieci w infrastrukturze wirtualnej - konieczna jest konfiguracja wspierająca wirtualne sieci LAN w oparciu o protokół 802.1q. 6. Przygotowanie koncepcji wirtualizacji fizycznych maszyn. 7. Instalacja i konfiguracja oprogramowania zarządzającego środowiskiem wirtualnym. 8. Konfiguracja klastra wysokiej dostępności: a. 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. b. Konfiguracja mechanizmów przenoszenia uruchomionych wirtualnych maszyn pomiędzy węzłami klastra bez utraty dostępu do zasobów wirtualnych maszyn. c. Konfiguracja mechanizmów ochrony wirtualnych maszyn przed awarią fizycznego serwera. 9. Weryfikacja działania klastra wysokiej dostępności. 10. Migracja istniejącej infrastruktury do środowiska wirtualnego. 11. Konfiguracja uprawnień w środowisku wirtualizacyjnym – integracja z usługą katalogową 12. Konfiguracja powiadomień o krytycznych zdarzeniach (email).
9.	**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:

		a. kopie wirtualnych maszyn muszą być wykonywane przy użyciu mechanizmów oferowanych przez dostarczone środowisko wirtualizujące; b. kopie wirtualnych maszyn muszą być wykonywane na dedykowany zasób dyskowy; c. kopie wirtualnych maszyn muszą być wykonywane automatycznie wg zadanego harmonogramu; d. kopie zapasowe muszą być wykonywane z zastosowaniem mechanizmów deduplikacji danych w celu zapewnienia inteligentnego zarządzania przestrzenią dyskową; e. musi istnieć możliwość odtworzenia: i. całej wirtualnej maszyny; ii. dysku wirtualnej maszyny; iii. 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: a. Nazwę zadania backupu b. Status zakończenia zadania backupu /Powodzenie, niepowodzenie/ c. Długość trwania zadania backupu d. Ilość zapisanych na taśmie danych 7. Zdefiniowanie powiadomień na wskazany adres email o zdarzeniach: a. Błąd urządzenia b. Uszkodzenie wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi c. Brak miejsca w wewnętrznej bazie danych systemu zarządzania kopiami zapasowymi d. Konieczność przeprowadzenia oczyszczania wewnętrznej bazy danych systemu zarządzania kopiami zapasowymi e. Zdarzenia dotyczące licencji f. 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: a. serwer backupu. b. 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.
10.	**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.
11.	**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 instalacji wymagane jest przeszkolenie administratora z całości systemu.
12.	**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; a. Definicja punktów dostępowych sieci WLAN na urządzeniach; b. Konfiguracja interfejsu radiowego punktów dostępowych sieci WLAN: i. Wybór i konfiguracja kanałów radiowych na poszczególnych punktach dostępowych tak, aby zminimalizować interferencje pomiędzy poszczególnymi punktami dostępowymi sieci WLAN; ii. Wybór i konfiguracja odpowiednich SSID na poszczególnych punkach dostępowych; c. Konfiguracja kont administratora oraz ograniczenie dostępu do urządzenia jedynie ze stacji zarządzającej; d. Konfiguracja stacji zarządzającej pracą sieci WLAN: i. Logowanie zdarzeń występujących w sieci WLAN do stacji zarządzającej; e. Konfiguracja zaawansowanych mechanizmów bezpieczeństwa (autentykacja użytkowników korzystających z sieci WLAN oraz szyfrowanie ruchu transmitowanego przez sieć WLAN, w powiązaniu z dostarczanym serwerem uwierzytelniającym); f. Konfiguracja mechanizmu dostępu do wydzielonych sieci WLAN: i. Zabezpieczenie dostępu do gościnnej sieci WLAN (SSID Guest) poprzez autentykację na wewnętrznym serwerze WWW urządzenia zarządzającego pracą sieci WLAN; ii. Zabezpieczenie dostępu do wybranych sieci WLAN poprzez autentykację na zewnętrznym serwerze z wykorzystaniem kont z systemu domenowego; iii. Zabezpieczenie dostępu do wybranych sieci WLAN poprzez autentykację na zewnętrznym serwerze z wykorzystaniem certyfikatów;

		iv. Zezwolenie na dostęp sieci WLAN tylko w określonych porach dnia; v. Określenie rodzaju ruchu, jaki może być transmitowany w ramach sieci WLAN (np. dostęp do Internetu dla usług WWW, vpn, itp.); vi. Dla sieci WLAN pracowniczej (SSID Pracownik) zdefiniować politykę dostępu, która przypisze odpowiednią sieć VLAN na podstawie przynależności do grup w systemie domenowym; vii. Konfiguracja mechanizmów QoS w sieci WLAN (transmisja danych oraz głosu);
13.	**UPS**	W ramach niniejszego postępowania Zamawiający wymaga podłączenia, skonfigurowania i uruchomienia zaoferowanego urządzenia UPS 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.
14.	**Usługa Katalogowa /Aktualizacja.**	**Instalacja, aktualizacja usługi katalogowej wraz z dodatkowymi komponentami w taki sposób, aby spełnione były poniższe wymagania celem świadczenia e-usług publicznych:**
14.1.	**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.
14.2.	**Wersja systemu operacyjnego serwerów**	Zastosowany system operacyjny musi zapewniać, co najmniej: a) możliwość uruchomienia usługi katalogowej w trybie usługi b) możliwość skonfigurowania różnych polityk haseł dla różnych grup zabezpieczeń c) możliwość łatwego odzyskania usuniętego obiektu usługi katalogowej wraz ze wszystkimi danymi, jakie były z nimi związane przed usunięciem (w tym przynależność do grup zabezpieczeń) d) możliwość zarządzania usługą katalogową poprzez interfejs graficzny oraz CLI e) możliwość zainstalowania lokalnego Centrum Certyfikacji zapewniającego wydawanie niekwalifikowanych certyfikatów X.509 umożliwiających uwierzytelnianie na stacjach roboczych i serwerach z wykorzystaniem kart kryptograficznych, szyfrowanie danych
14.3.	**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.
14.4.	**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: a) Resetowania haseł użytkowników b) Odblokowywania kont użytkowników c) Zmiany atrybutów „Display Name" oraz „Last name" Zamawiający wymaga skonfigurowania parametrów audytu dla usługi katalogowej umożliwiających między innymi: a) Śledzenie zmian obiektów usługi katalogowej z dostępem do informacji o dotychczasowej wartości b) 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).
14.5.	**Konfiguracja polityki haseł oraz polityki blokowania kont**	Konfiguracja globalnej polityki haseł dla domeny: a) Hasło musi zawierać minimum 8 znaków b) Maksymalny czas ważności hasła: do ustalenia z Zamawiającym c) Minimalny czas, po którym możliwa jest zmiana hasła: do ustalenia z Zamawiającym d) Hasło musi spełniać zasady złożoności Konfiguracja polityki haseł dla kadry zarządzającej: a) Hasło musi zawierać minimum 10 znaków b) Maksymalny czas ważności hasła: 30 dni c) Minimalny czas, po którym możliwa jest zmiana hasła: 240 dni d) 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.
14.6.	**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: a) ścieżki i nazwy pliku wejściowego b) ścieżki i nazwy pliku logującego c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu) d) nazwy FQDN domeny e) nazwy NetBIOS domeny

		f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty g) 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: a) \\DOMENA\Public\SHARE1 b) \\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. 6. Skrypt tworzy podkatalogi: \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej oraz \\DOMENA\Public\SHARE2\Nazwa_Jednostki_Organizacyjnej 7. Skrypt nadaje uprawnienia do utworzonych podkatalogów według założeń: a) \\DOMENA\Public\SHARE1\Nazwa_Jednostki_Organizacyjnej: i. Administratorzy Domeny – Pełna kontrola ii. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej iii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu iv. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze a) \\DOMENA\Public\Share2\Nazwa_Jednostki_Organizacyjnej: v. Administratorzy Domeny – Pełna kontrola vi. Grupa G_Nazwa_Jednostki_Organizacyjnej – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu Nazwa_Jednostki_Organizacyjnej vii. Użytkownicy Uwierzytelnieni - Odczyt viii. Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu ix. Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 8. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 9. 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: a) ścieżki i nazwy pliku wejściowego b) ścieżki i nazwy pliku logującego c) ścieżki i nazwy pliku wyjściowego (właściwego skryptu) d) nazwy FQDN domeny e) nazwy NetBIOS domeny f) nadrzędnej jednostki organizacyjnej, w której będą tworzone nowe obiekty g) ścieżki do udziału sieciowego HOME h) litery dysku katalogu domowego 2. Skrypt ma pobierać z pliku wejściowego listę kont użytkowników w formacie: NazwaUzytkownika;Imie;Nazwisko:Haslo;Dzial;NumerTelefonu 3. Skrypt tworzy nowe konta użytkowników w jednostce organizacyjnej nadrzędnej zdefiniowanej w części konfiguracyjnej skryptu pobierając wszystkie niezbędne dane z pliku wejściowego 4. Nowo utworzone konta użytkowników muszą mieć jednorazowo ustawione hasła – użytkownik musi zmienić hasło podczas pierwszego logowania 5. Skrypt tworzy katalog \\DOMENA\HOME\NazwaUzytkownika 6. Skrypt nadaje uprawnienia do utworzonych katalogów użytkowników według założeń: a) Administratorzy Domeny – Pełna kontrola b) Użytkownik – Pełna kontrola z wyłączeniem uprawnień: Zmiana uprawnień, Przejęcie na własność, usuwanie katalogu NazwaUzytkownika c) Wyłączenie dziedziczenia uprawnień z katalogu nadrzędnego poziomu d) Włączenie propagacji uprawnień do katalogów i plików znajdujących się poniżej w strukturze 10. Skrypt ma ustawić dla każdego konta użytkownika literę dysku domowego oraz poprawną ścieżkę sieciową 11. Każde uruchomienie skryptu ma skutkować odczytaniem pliku wejściowego i wygenerowaniem właściwego skryptu (na końcu nazwy właściwego skryptu musi być dołączona bieżąca data i godzina) 12. Działanie skryptu właściwego musi być w całości logowane do pliku tekstowego, opatrzonego bieżącą datą i godziną w celu umożliwienia każdorazowego zweryfikowania poprawności działania 13. 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.
14.7.	**Skonfigurowanie mapowania zasobów sieciowych**	Skonfigurowanie mechanizmów mapowania dysków sieciowych dla systemów klienckich Windows. Mapowane mają być między innymi zasoby: \\DOMENA\Public\SHARE1 \\DOMENA\Public\SHARE2 Oraz 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).
14.8.	**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: a) Określenie daty, czasu, nazwy użytkownika, który usunął / próbował usunąć plik/folder b) Określenie daty, czasu, nazwy użytkownika, który zapisał / próbował zapisać plik/folder c) 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.
14.9.	**Serwery uwierzytelniające**	1. Zamawiający wymaga uruchomienia serwerów uwierzytelniających współpracujących z infrastrukturą AD, realizujących funkcję uwierzytelniania na dostarczanych przełącznikach sieciowych. 2. Zamawiający wymaga uruchomienia co najmniej dwóch instancji serwera uwierzytelniania w celu zachowania redundancji na dwóch niezależnych serwerach. 3. 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. 4. Zamawiający wymaga skonfigurowania odpowiednich polityk bezpieczeństwa na zainstalowanych serwerach uwierzytelniających bazujących na utworzonych w strukturze usługi katalogowej Zamawiającego grupach. 5. Jeżeli jest potrzebna, Zamawiający wymaga dostarczenia licencji na instalowane serwery uwierzytelniające oraz ujęcia ich ceny w ofercie.
14.10.	**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)
14.11.	**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.
15.	**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
16.	**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.
17.	**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: a) zastosowanej technologii serwerów b) zastosowanej technologii pamięci masowej c) firewall/UTM d) sieci LAN e) sieci Wi-Fi f) systemu wirtualizacji/domeny (usługi katalogowej) g) systemu backupu h) 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.
18.	**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.
19.	**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.