**ZAŁĄCZNIK NR 1 do SWZ**

# OPIS PRZEDMIOTU ZAMÓWIENIA

## dla zamówienia pn.:

# Zakup sprzętu oraz usług szkoleniowych w ramach programu „Cyfrowa Gmina” dla Gminy Lubań

Lubań, grudzień 2022

# Spis treści

# 1 Ogólne informacje

Niniejsze Zamówienie jest częścią programu pn.: **„Cyfrowa Gmina”**, który jest realizowany przez Gminę Lubań. Głównym miejscem realizacji Zamówienia będzie siedziba Urzędu Gminy Lubań.

W celu podniesienia poziomu cyfryzacji Urzędu Gminy Lubań konieczny jest zakup nowego sprzętu IT. Infrastruktura informatyczna Urzędu powinna zapewnić efektywne i bezpieczne korzystanie z posiadanych systemów dziedzinowych oraz wspierających obsługę interesariuszy on-line, jak również wysoki poziom zabezpieczenia posiadanych danych.

OGÓLNE ZASADY RÓWNOWAŻNOŚCI ROZWIĄZAŃ:

1. W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.
2. Dodatkowo, wszędzie tam, gdzie zostało wskazane pochodzenie (marka, znak towarowy, producent, dostawca itp.) materiałów lub normy, aprobaty, specyfikacje i systemy, o których mowa w ustawie Prawo Zamówień Publicznych, Zamawiający dopuszcza oferowanie sprzętu lub rozwiązań równoważnych pod warunkiem, że zapewnią uzyskanie parametrów technicznych nie gorszych niż wymagane przez Zamawiającego w dokumentacji przetargowej. Zamawiający informuje, że w takiej sytuacji przedmiotowe zapisy są jedynie przykładowe i stanowią wskazanie dla Wykonawcy, jakie cechy powinny posiadać składniki użyte do realizacji przedmiotu

zamówienia. Zamawiający zgodnie z art. 99 ust. 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych, zwanej dalej ustawą, dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe i cechy użytkowe, a także jakościowe (m.in.: wymiary, skład, zastosowany materiał, kolor, odcień, przeznaczenie materiałów i urządzeń, estetyka itp.), jakim muszą odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby zostały spełnione wymagania stawiane przez Zamawiającego. Operowanie przykładowymi nazwami producenta ma jedynie na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami producentów/produktów ma wyłącznie charakter przykładowy. Zamawiający, wskazując oznaczenie konkretnego producenta (dostawcy), konkretny produkt lub materiały przy opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach jakościowych i cechach użytkowych, co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.

3. Zamawiający opisując przedmiot zamówienia przy pomocy określonych norm, aprobat czy specyfikacji technicznych i systemów odniesienia, o których mowa w art. 101 ust. 1-3 ustawy, zgodnie z art. 101 ust.4 ustawy dopuszcza rozwiązania równoważne opisywanym. Zgodnie z art. 101 ust. 5 ustawy – Zamawiający nie może odrzucić oferty tylko dlatego, że oferowane roboty budowlane, dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.

## 1.1 Miejsce realizacji dostaw i usług

Dostawy i usługi będą realizowane w siedzibie Urzędu Gminy Lubań.

**Dokładny adres realizacji Przedmiotu Zamówienia:**

Urząd Gminy Lubań

ul. Dąbrowskiego 18

59-800 Lubań

Szczegółowy zakres dostaw zostanie przedstawiony w dalszej części niniejszego załącznika.

## 1.2 Termin i Harmonogram Wykonania Zamówienia

Wymagany termin wykonania Zamówienia – **60 dni kalendarzowych od dnia podpisania umowy**.

## 1.3 Ogólne informacje dotyczące zamówienia

W tabeli poniżej przedstawiono wykaz sprzętu i licencji (oprogramowania), jakie mają zostać dostarczone w ramach przedmiotowego zamówienia oraz okres minimalnej gwarancji lub okres na jaki ma zostać udzielona licencja.

W przypadku sprzętu w pozycjach w których wpisano przedział czasowy od 24 do 36 miesięcy Wykonawca ma możliwość w formularzu oferty zaoferować okres gwarancji o długości od 24 do 36 miesięcy (w przypadku serwera do 60 miesięcy).

1. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (t.j. Dz.U. z 2022, poz. 1666 ze zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.
2. Opis przedmiotu zamówienia (tylko ogólny): Oferent winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

Są to kryteria punktowe opisane w Specyfikacji Warunków Zamówienia.

| Nazwa usługi i produktu | jednostka | ilość | Rozdział OPZ | Gwarancja / licencja min. |
|---|---|---|---|---|
| Switch typ I | 1 | szt. | 2.1 | 24 m-ce – 36 m-cy |
| Switch typ II | 4 | szt. | 2.2 | 24 m-ce – 36 m-cy |
| Serwer | 1 | szt. | 2.3 | 24 m-ce – 36 m-cy |
| Serwer NAS | 1 | szt. | 2.4 | 24 m-ce – 36 m-cy |
| UTM | 2 | szt. | 2.5 | 12 m-cy |
| Szkolenia UTM | 1 | kpl. | 2.6 | n/d |
| Wdrożenie i konfiguracja sprzętu oraz sieci wraz z uruchomieniem domeny AD | 1 | kpl. | 2.7 | n/d |

# 2 Szczegółowy opis zamówienia

W ramach zamówienia należy dostarczyć opisany poniżej sprzęt i oprogramowanie oraz wykonać następujące prace:

- Analiza przedwdrożeniowa;
- Fizyczna instalacja sprzętu serwerowego (serwer, macierz);
- Konfiguracja sieci dla serwera, macierzy i stacji roboczych;
- Konfiguracja serwera i macierzy (aktualizacja firmware, ustawienia sieciowe, konfiguracja);
- Instalacja oprogramowania serwera;
- Podłączenie komputerów do domeny;
- Instalacja i konfiguracja systemu Exchange;
- Konfiguracja polityk na firewall dla całego środowiska;
- Instalacja i uruchomienie radiolinii;
- Warsztat dla administratorów.

Ponadto:

1. Dostarczony sprzęt musi być fabrycznie nowy, wcześniej nie używany, być wolny od wad fizycznych i prawnych.
2. Wykonawca zobowiązany jest do instalacji sprzętu informatycznego w lokalizacjach określonych przez Zamawiającego.
3. Wykonawca zobowiązany jest do skonfigurowania zamawianego sprzętu w uzgodnieniu z Zamawiającym.
4. Dostawy i montaż należy realizować w dni robocze w godzinach od 8.00-15.00.
5. Wykonawca jest zobowiązany do złożenia dokumentacji powykonawczej, zawierającej w szczególności wszystkie dane dostępu do urządzeń i systemów, które będą wykorzystywane podczas instalacji i konfiguracji sprzętu i systemów.
6. Wykonawca jest zobowiązany do przeprowadzenia min. 5 godzin instruktażu dla administratora sprzętu i oprogramowania w siedzibie Zamawiającego w zakresie obsługi dostarczanych urządzeń.

## 2.1 Switch typ I - 1 szt.

**Porty przełącznika**: minimum 48x10/100/1000Base-T RJ45 oraz minimum 4x1/10GBase-X SFP+

**Port konsolowy:** RJ45 (RS-232)

**Port USB:** minimum 1 port co najmniej w standardzie 2.0

**Szybkość przełączania:** minimum 175Gb/s

**Przepustowość:** minimum 130Mp/s (dla pakietów 64Kb)

**Bufor pakietów:** minimum 1,5MB

**Ramki Jumbo:** minimum 10k

**Tablica adresów MAC:** minimum 16k

**Adresy MAC – Multicast:** minimum 1k

**Tablica ACL:** minimum 384

**Tablica VLAN:** minimum 4094

**Taktowanie procesora:** minimum 800MHz

**Pamięć Flash:** minimum 32MB

**Pamięć RAM:** minimum 128MB

**Temperatura pracy:** zakres minimum 0°C - 50°C

**Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji)

**Zasilanie:** zabudowany zasilacz 230V AC

**Pobór mocy:** maksymalnie 21W

**Zabezpieczenie przeciwprzepięciowe:** minimum 6kV

**Wymiary:** maksymalna: szerokość 440 mm, wysokość 45mm , głębokość 210mm

**Certyfikaty bezpieczeństwa**: CE, RoHS

**Algorytm:** Store and Forward

**VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ

**DHCP:** IPv4/IPv6 DHCP Client, IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping, IPv4/IPv6 DHCP Server

**Spanning tree:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding

**Protekcja ringowa:** ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection

**Agregacja łączy:** IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance

**Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing, Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,

**Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication

**QoS:** 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay

**Lista kontroli dostępu:** IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN

**Diagnostyka:** sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP

**Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking

**Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług

**Gwarancja: minimum 24 miesiące** lub dłużej zgodnie ze złożoną ofertą gwarancji producenta.

## 2.2 Switch typ II – 4 szt.

**Porty przełącznika**: minimum 24x 10/100/1000Base-T RJ45 oraz minimum 4x 1/10GBase-X SFP+

**Port konsolowy:** RJ45 (RS-232)

**Port USB:** minimum 1 port co najmniej w standardzie 2.0

**Szybkość przełączania:** minimum 128Gb/s

**Przepustowość:** minimum 95Mp/s (dla pakietów 64Kb)

**Bufor pakietów:** minimum 1,5MB

**Ramki Jumbo:** minimum 10k

**Tablica adresów MAC:** minimum 16k

**Adresy MAC – Multicast:** minimum 1k

**Tablica ACL:** minimum 384

**Tablica VLAN:** minimum 4094

**Taktowanie procesora:** minimum 800MHz

**Pamięć Flash:** minimum 32MB

**Pamięć RAM:** minimum 256MB

**Temperatura pracy:** zakres minimum 0°C - 50°C

**Wilgotność względna:** zakres minimum 10% - 90% (bez kondensacji)

**Zasilanie:** zabudowany zasilacz 230V AC

**Pobór mocy:** maksymalnie 21W

**Zabezpieczenie przeciwprzepięciowe:** minimum 6kV

**Wymiary:** maksymalna: szerokość 440 mm, wysokość 45mm , głębokość 210mm

**Certyfikaty bezpieczeństwa**: CE, RoHS

**Algorytm:** Store and Forward

**VLAN:** Voice VLAN, Port based VLAN, MAC based VLAN, Protocol based VLAN, Private VLAN, VLAN Translation, N:1 VLAN Translation, GVRP, IEEE 802.1Q, Normal QinQ, Flexible QinQ

**DHCP:** IPv4/IPv6 DHCP Client,IPv4/IPv6 DHCP Relay, Option 82, IPv4/IPv6 DHCP Snooping,IPv4/IPv6 DHCP Server

**Spanning tree:** IEEE802.1D (STP), IEEE802.1W (RSTP), IEEE802.1S (MSTP), Multi-Process MSTP, Root Guard, BPDU guard, BPDU forwarding

**Protekcja ringowa:** ITU-T G.8032 – recovery time < 50ms, Fast Link, Loopback Detection

**Agregacja łączy:** IEEE 802.3ad (LACP), 64 groups per device / 8 ports per group, load balance

**Bezpieczeństwo:** Storm Control based on packets, Port Security, MAC Limit based on VLAN and Port, Anti-ARP-Spoofing , Anti-ARP-Scan, ARP Binding, Gratuitous ARP, ARP Limit, Anti ARP/NDP Cheat, Anti ARP Scan, ND Snooping, DAI, IEEE 802.1x, Authentication, Authorization, Accounting, Radius IPv4/IPv6, TACACS+, MAB, Port and MAC based authentication, Accounting based on time length and traffic, Guest VLAN and auto VLAN,

**Multicast:** IGMP v1/v2/v3 snooping and L2 Query, IGMP Fast leave, MVR, MLD v1/v2 Snooping, IPv4/IPv6 DCSCM, IGMP authentication

**QoS:** 8 queques per port, Bandwidth Control, Flow Control: HOL, IEEE802.3x, Flow Redirect, Classification based on ACL, COS, TOS, DiffServ, DSCP, port number; Traffic Policing, PRI Mark/Remark, IEEE 802.1p, Queuing Method: Strict Priority, Weighted Deficit Round Robin, Strict priority in Weighted Deficit Round Robin; DNS Client, DNS Relay

**Lista kontroli dostępu:** IP Src/Dst ACL, MAC Src/Dst ACL, MAC-IP ACL, User-Defined ACL, Time Range ACL, port number TCP/UDP ACL, VLAN ACL, REDIRECT and Statistics based on ACL, Precedence, Vlan Tag/Untag, Rules can be configured to port and VLAN

**Diagnostyka:** sFlow, Traffic Analysis, RSPAN, VCT, Ping, Trace Route, Dying GASP

**Zarządzanie:** TFTP/FTP, CLI, Telnet, Console, Web/SSL (IPv4/IPv6), SSH (IPv4/IPv6), SNMP v1/v2c/v3, SNMP Trap, Public & Private MIB interface, RMON 1,2,3,9, Syslog (IPv4/IPv6), SNTP/NTP (IPv4/IPv6), Dual IMG, Multiple Configuration Files, Port Mirror, IEEE 802.3ah/802.1ag OAM, ULDP (like UDLD), LLDP/LLDP MED., VSF (4 devices in one stack) – hardware stacking

**Oprogramowanie oraz wsparcie techniczne:** oprogramowanie przełącznika (firmware) dostępne bez ograniczeń czasowych, przez cały okres cyklu życia urządzenia, poprzez Internet, wsparcie techniczne dystrybutora bez konieczności wykupu dodatkowych usług

**Gwarancja: minimum 24 miesiące** lub dłużej zgodnie ze złożoną ofertą gwarancji producenta.

## 2.3 Serwer – 1 szt.

**Obudowa:** typu rack o wysokości max. 1U pozwalająca na montaż 8 dysków twardych 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack

**Procesor:** Zainstalowane dwa procesory min 12-rdzeniowe, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku 30500 w teście Dual CPU Average CPU Mark dostępnym na stronie https://www.cpubenchmark.net/ (Załączyć do oferty wydruk ze strony potwierdzający osiągany wynik - stan nie wcześniej niż dzień ogłoszenia postępowania)**.**

**Płyta główna:** Płyta główna z możliwością zainstalowania dwóch procesorów. Płyta główna zaprojektowana przez producenta i oznaczona jego znakiem firmowym.

**Chipset:** Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych

**Pamięć operacyjna:** min. 128GB DDR4 3200MT/s, na płycie znajduje się min. 24 sloty przeznaczone do instalacji pamięci w tym minimum 20 slotów wolnych. Płyta obsługuje do 3TB Pamięci RAM.

**Wsparcie dla następujących technologii zabezpieczenia pamięci:** Memory Rank Sparing, Memory Mirror, Lockstep

**Gniazda PCI:** Min. 2 sloty PCIe x16 generacji 3

**Interfejsy sieciowe:** Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT (porty nie mogą być osiągnięte poprzez karty w wymaganych slotach PCIe). Dodatkowa karta sieciowa wyposażona w min. 2 interfejsy 10Gb Ethernet w standardzie SFP+. Ponadto 2 wkładki SFP+ wielomodowe ( + niezbędne okablowanie do połączenia) kompatybilne z serwerem i przełącznikami oferowanymi w zamówieniu.

**Kontroler RAID:** Sprzętowy kontroler dyskowy, posiadający min. 8GB nieulotnej pamięci cache z podtrzymaniem, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących.

**Dyski twarde:** możliwość instalacji dysków SAS, SATA, SSD;

Zainstalowane dyski: 2 dyski twarde o pojemności min. 300GB SAS 10K (Hot-Plug), 2 dyski twarde o pojemności min. 900GB HDD SAS 10k (Hot-Plug), dwa dyski twarde o pojemności min. 1.2TB HDD SAS 10k (Hot-Plug);

**Video:** Zintegrowana karta graficzna umożliwiająca wyświetlanie rozdzielczości min. 1280x1024;

**Zasilanie:** Zainstalowane dwa zasilacze max. 700W (każdy) Hot-Plug. Dostarczone kable zasilające min. 2 m.

**Wbudowane porty:** min. 3xUSB, w tym min. 2 porty USB min. 3.0; min. 2 porty VGA z czego 1 na panelu przednim; min. jeden port typu serial; min. 1 port RJ45 pod zarządzanie.

**Karty sieciowe:** Wbudowane dwa porty 1Gb Ethernet, dodatkowy moduł 2x10Gb SFP+ nie zajmujący slotów PCie wraz z 2 wkładkami 10GbE SFP+ do komunikacji z przełącznikami (wymagane 2 kpl).

**Bezpieczeństwo:** Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą; Moduł TPM 2.0.

**Zdalne zarządzanie:** Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:

- zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
- zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
- szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika;
- możliwość podmontowania zdalnych wirtualnych napędów;
- wirtualną konsolę z dostępem do myszy, klawiatury;
- wsparcie dla IPv6;
- wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH;
- możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
- możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
- integracja z Active Directory;
- możliwość obsługi przez dwóch administratorów jednocześnie;
- wsparcie dla dynamic DNS;
- wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;
- możliwość podłączenia lokalnego poprzez złącze RS-232;
- możliwość zarządzania bezpośredniego poprzez złącze USB umieszczone na froncie obudowy;
- dziennik logów dla danych SMART oraz przekierowań konsoli serial;
- automatyzacja w odnawianiu certyfikatów SSL.

**Oprogramowanie do zarządzania:**

- Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych
- integracja z Active Directory
- Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta
- Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish
- Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram

- Szczegółowy opis wykrytych systemów oraz ich komponentów
- Możliwość eksportu raportu do CSV, HTML, XLS, PDF
- Możliwość tworzenia własnych raportów w oparciu o wszystkie informacje zawarte w inwentarzu.
- Grupowanie urządzeń w oparciu o kryteria użytkownika
- Tworzenie automatycznie grup urządzeń w oparciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji
- Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach
- Szybki podgląd stanu środowiska
- Podsumowanie stanu dla każdego urządzenia
- Szczegółowy status urządzenia/elementu/komponentu
- Generowanie alertów przy zmianie stanu urządzenia.
- Filtry raportów umożliwiające podgląd najważniejszych zdarzeń
- Integracja z service desk producenta dostarczonej platformy sprzętowej
- Możliwość przejęcia zdalnego pulpitu
- Możliwość podmontowania wirtualnego napędu
- Kreator umożliwiający dostosowanie akcji dla wybranych alertów
- Możliwość importu plików MIB
- Przesyłanie alertów „as-is” do innych konsol firm trzecich
- Możliwość definiowania ról administratorów
- Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów
- Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)
- Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta
- Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów
- Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących alertów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera.
- Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstawie weryfikacji środowiska w celu wykrycia rozbieżności.

- Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w oparciu o profile
- Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami.
- Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta.
- Zdalne uruchamianie diagnostyki serwera.
- Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarządzającym.
- Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.

**Gwarancja: minimum 24 miesiące** lub dłużej zgodnie ze złożoną ofertą gwarancji producenta z czasem reakcji w następnym dniu roboczym, gwarancja realizowana w miejscu użytkowania sprzętu, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.

Zamawiający wymaga, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

Firma serwisująca musi posiadać certyfikat ISO 9001 lub równoważny na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

Serwis urządzeń realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Zamawiający wymaga dołączenia na etapie dostawy oświadczenia Producenta potwierdzającego powyższe warunki gwarancji oraz, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

**Certyfikaty i dokumenty:** Zamawiający wymaga dołączenia do oferty poniższych dokumentów:

- Certyfikat ISO 9001 lub równoważny producenta o wyprodukowaniu sprzętu zgodnie z tą normą;
- Certyfikat ISO 14001 lub równoważny dla producenta serwera;
- Certyfikat ISO 9001 na świadczenie usług serwisowych oraz posiadanie autoryzacji producenta urządzeń dla firmy serwisującej;
- Oświadczenia Producenta lub Wykonawcy potwierdzające, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta oraz, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

**System operacyjny serwera**: licencja bez ograniczeń czasowych (Polska wersja językowa) obejmująca licencję z możliwością obsługi wszystkich rdzeni oferowanych w serwerze oraz zastosowania 4 maszyn wirtualnych.

Współpraca z procesorami o architekturze x86-64., Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. Na dostarczonym systemie operacyjnym. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów

logicznych (wirtualnych). Pojemność obsługiwanej pamięci RAM w ramach jednej instancji systemu operacyjnego - co najmniej 4TB. Obsługa dostępu wielościeżkowego do zasobów LAN poprzez kontrolery Gigabit Ethernet, w trybie równoważenia obciążenia łącza (load balancing) i redundancji łącza (failover) – natywnie lub z wykorzystaniem sterowników producenta sprzętu. Praca w roli klienta domeny Microsoft Active Directory. Zawarta możliwość uruchomienia roli serwera DHCP, w tym funkcji klastrowania serwera DHCP (możliwość uruchomienia dwóch serwerów DHCP operujących jednocześnie na tej samej puli oferowanych adresów IP).Zawarta możliwość uruchomienia roli serwera DNS. Zawarta możliwość uruchomienia roli klienta i serwera czasu (NTP).Zawarta możliwość uruchomienia roli serwera plików z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory. Zawarta możliwość uruchomienia roli serwera wydruku z uwierzytelnieniem i autoryzacją dostępu w domenie Microsoft Active Directory .Zawarta możliwość uruchomienia roli serwera stron WWW. W ramach dostarczonej licencji zawarte prawo do użytkowania i dostęp do oprogramowania oferowanego przez producenta systemu operacyjnego umożliwiającego wirtualizowanie zasobów sprzętowych serwera. W ramach dostarczonej licencji zawarte prawo do instalacji i użytkowania systemu operacyjnego na co najmniej dwóch maszynach wirtualnych. W ramach dostarczonej licencji zawarte prawo do pobierania poprawek systemu operacyjnego. Wszystkie wymienione parametry, role, funkcje, itp. systemu operacyjnego objęte są dostarczoną licencją (licencjami) i zawarte w dostarczonej wersji oprogramowania (nie wymagają ponoszenia przez Zamawiającego dodatkowych kosztów).

**Licencje dostępowe** 30 szt. dla urządzenia umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności serwera typu Device Cal z wdrożoną rolą Active Directory.

**Oprogramowanie do Kopii Zapasowych**.

Wymagania ogólne.

a) Oprogramowanie musi być produktem przeznaczonym do obsługi środowisk DataCenter. Oferowany produkt musi znajdować się w kwadracie liderów Gartner Magic Quadrant for Data Center Backup and Recovery Solutions oraz na ogólnie dostępnej liście referencyjnej Gartner: https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions i spełniać minimalne wymaganie: - minimalna liczba referencji 150, - minimalna ocena z referencji 4,5,

b) Oprogramowanie musi współpracować z infrastrukturą VMware w wersji 6.5 oraz 6.7 oraz Microsoft Hyper-V 2012 R2 i 2019. Wszystkie funkcjonalności w specyfikacji muszą być dostępne na wszystkich wspieranych platformach wirtualizacyjnych, chyba, że wyszczególniono inaczej.

c) Oprogramowanie musi współpracować z hostami zarządzanymi przez VMware vCenter oraz pojedynczymi hostami.

d) Oprogramowanie musi współpracować z hostami zarządzanymi przez System Center Virtual Machine Manger, klastrami hostów oraz pojedynczymi hostami.

e) Oprogramowanie musi zapewniać tworzenie kopii zapasowych wszystkich systemów operacyjnych maszyn wirtualnych wspieranych przez vSphere i Hyper-V.

f) Oprogramowanie musi zapewniać tworzenie kopii zapasowych z sieciowych urządzeń plikowych NAS opartych o SMB, CIFS i/lub NFS oraz bezpośrednio z serwerów plikowych opartych o Windows i Linux.

Możliwości:

a) Oprogramowanie musi być niezależne sprzętowo i umożliwiać wykorzystanie dowolnej platformy serwerowej i dyskowej.

b) Oprogramowanie musi tworzyć "samowystarczalne" archiwa do odzyskania których nie wymagana jest osobna baza danych z metadanymi deduplikowanych bloków.

c) Oprogramowanie musi pozwalać na tworzenie kopii zapasowych w trybach: Pełny, pełny syntetyczny, przyrostowy i odwrotnie przyrostowy (tzw. reverse-inremental).

d) Oprogramowanie musi mieć mechanizmy deduplikacji i kompresji w celu zmniejszenia wielkości archiwów. Włączenie tych mechanizmów nie może skutkować utratą jakichkolwiek funkcjonalności wymienionych w tej specyfikacji.

e) Oprogramowanie nie może przechowywać danych o deduplikacji w centralnej bazie. Utrata bazy danych używanej przez oprogramowanie nie może prowadzić do utraty możliwości odtworzenia backupu. Metadane deduplikacji muszą być przechowywane w plikach backupu.

f) Oprogramowanie nie może instalować żadnych stałych agentów wymagających wdrożenia czy upgradowania wewnątrz maszyny wirtualnej dla jakichkolwiek funkcjonalności backupu lub odtwarzania.

g) Oprogramowanie musi mieć możliwość uruchamiania dowolnych skryptów przed i po zadaniu backupowym lub przed i po wykonaniu zadania snapshota.

h) Oprogramowanie musi mieć wbudowane mechanizmy backupu konfiguracji w celu prostego odtworzenia systemu po całkowitej reinstalacji.

i) Oprogramowanie musi mieć wbudowane mechanizmy szyfrowania zarówno plików z backupami jak i transmisji sieciowej.

j) Oprogramowanie musi wspierać backup maszyn wirtualnych używających współdzielonych dysków VHDX na Hyper-V (shared VHDX).

Wymagania RPO:

a) Oprogramowanie musi wykorzystywać mechanizmy Change Block Tracking na wszystkich wspieranych platformach wirtualizacyjnych. Mechanizmy muszą być certyfikowane przez dostawcę platformy wirtualizacyjnej.

b) Oprogramowanie musi wspierać kopiowanie plików na taśmy.

c) Oprogramowanie musi mieć możliwość tworzenia retencji GFS (Grandfather-Father-Son).

d) Oprogramowanie musi wspierać BlockClone API w przypadku użycia Windows Server 2016 lub 2019 z systemem pliku ReFS jako repozytorium backupu. Podobna funkcjonalność musi być zapewniona dla repozytoriów opartych o linuxowy system plików XFS.

e) Oprogramowanie musi mieć możliwość replikacji włączonych wirtualnych maszyn bezpośrednio z infrastruktury Hyper-V oraz VMware vSphere, pomiędzy hostami ESXi, włączając asynchroniczną replikacją ciągłą. Dodatkowo oprogramowanie musi mieć możliwość użycia plików kopii zapasowych jako źródła replikacji.

f) Oprogramowanie musi umożliwiać przechowywanie punktów przywracania dla replik.

g) Oprogramowanie musi umożliwiać wykorzystanie istniejących w infrastrukturze wirtualnych maszyn jako źródła do dalszej replikacji (replica seeding).

h) Oprogramowanie musi posiadać takie same funkcjonalności replikacji dla Hyper-V.

i) Oprogramowanie musi wykorzystywać wszystkie oferowane przez hypervisor tryby transportu (sieć, hot-add, LAN Free-SAN).

j) Oprogramowanie musi dawać możliwość tworzenia backupów ad- hoc z konsoli jak i z klienta webowego vSphere.

Wymagania RTO:

a) Oprogramowanie powinno umożliwiać jednoczesne uruchomienie wielu maszyn wirtualnych bezpośrednio ze zdeduplikowanego i skompresowanego pliku backupu, z dowolnego punktu przywracania, bez potrzeby kopiowania jej na storage produkcyjny. Funkcjonalność musi być oferowana dla środowisk VMware oraz Hyper-V niezależnie od rodzaju storage'u użytego do przechowywania kopii zapasowych.

b) Oprogramowanie musi pozwalać na migrację on-line tak uruchomionych maszyn na storage produkcyjny. Migracja powinna odbywać się mechanizmami wbudowanymi w hypervisor. Jeżeli licencja na hypervisor nie posiada takich funkcjonalności - oprogramowanie musi realizować taką migrację swoimi mechanizmami.

c) Oprogramowanie musi pozwalać na zaprezentowanie pojedynczego dysku bezpośrednio z kopii zapasowej do wybranej działającej maszyny wirtualnej vSpehre.

d) Oprogramowanie musi umożliwiać pełne odtworzenie wirtualnej maszyny, plików konfiguracji i dysków.

e) Oprogramowanie musi umożliwić odtworzenie plików na maszynę operatora, lub na serwer produkcyjny bez potrzeby użycia agenta instalowanego wewnątrz wirtualnej maszyny. Funkcjonalność ta nie powinna być ograniczona wielkością i liczbą przywracanych plików.

f) Oprogramowanie musi mieć możliwość odtworzenia plików bezpośrednio do maszyny wirtualnej poprzez sieć, przy pomocy PowerShell Direct dla platformy Hyper-V.

g) Oprogramowanie musi wspierać odtwarzanie plików z następujących systemów: Linux, BSD, Mac OS, Novell, Solaris, AIX,

h) Oprogramowanie musi umożliwiać szybkie granularne odtwarzanie obiektów aplikacji bez użycia jakiegokolwiek agenta zainstalowanego wewnątrz maszyny wirtualnej.

i) Oprogramowanie musi wspierać granularne odtwarzanie obiektów Active Directory takich jak konta komputerów, konta użytkowników oraz pozwalać na odtworzenie haseł.

Ograniczenie ryzyka:

a) Oprogramowanie musi umożliwiać integrację z oprogramowaniem antywirusowym w celu wykonania skanu zawartości pliku backupowego przed odtworzeniem jakichkolwiek danych. Integracja musi być zapewniona minimalnie dla Windows Defender, oraz ESET.

Pozostałe wymagania:

a) Liczba VM: 7.

b) Liczba serwerów fizycznych: 3.

c) Karta sieciowa PCIe 10Gb 2-Port SFP+ kompatybilna z serwerem Lenovo 7x08.

## 2.4 Serwer NAS - 1 szt.

1. Obudowa: max. 2U wraz z szynami umożliwiającymi montaż serwera w szafie rack**,**
2. Procesor, o minimalnej wydajność pojedynczego **CPU min. 4000** punktów w PassMark, www.cpubenchmark.net (Pomiar średni - Average CPU Mark) - stan nie wcześniej niż dzień ogłoszenia postępowania. Załączyć wydruk do Oferty.
3. Pamięć systemowa: min. 8 GB DDR4 ECC
4. pamięć flash min. 4 GB,
5. wnęka dysków – min. 12 x 3,5” SATA,
6. port LAN – min. 2 x 10 GbE SFP+,
7. port LAN – min. 2 x min. 1 GbE RJ45,
8. port USB – min. 4 x USB w tym min. 2 x 3.2,
9. zasilacz nadmiarowy/wymieniany podczas pracy; 2 x max. 300 W,
10. Funkcje hot swap RAID 0/1/5/6. Przywracanie RAID. Migracja Poziomów RAID.
11. Bezpieczny zdalny backup sieci komputerowej poprzez SSH / rsync.
12. Kopia na dyski zewnętrzne i inne urządzenia.
13. Zgodność z VMware / Hyper-V.
14. Możliwość tworzenia połączeń sieciowych: fail-over, load balancing, agregacji.
15. Współdzielenie zasobów np. drukarki USB dla systemów Windows i MacOS.
16. Zainstalowane:

- min. 2 dyski o pojemności min. 240GB SSD NVMe M.2,

- min. 4 dyski o pojemności min. 4 TB SATA 6 Gb/s 7200 RPM, bufor 256 MB, czas pracy MTBF 1 200 000. Dyski twarde zgodne ze stroną kompatybilności producenta.

17. Inne wymagania:
    - Buforowanie SSD,
    - Nadmiarowa alokacja SSD
    - Migawka/kopia zapasowa jednostek iSCSI LUN,
    - Kontroler domeny i serwer NTP,
    - Wolumin z elastycznym alokowaniem,
    - Jednostki iSCSI LUN oparte na blokach,
    - Odzyskiwanie miejsca,
    - Funkcja typu Storage Plug & Connect (iSCSI i CIFS),
    - Obsługa ACL na poziomie folderów współdzielonych,
    - Kopie Migawkowe,
    - Replikacja zdalna w czasie rzeczywistym,
    - Replikacja zdalna (rsync),
    - Oprogramowanie do tworzenia kopii zapasowych,
    - Obsługa etykiet woluminu na dyskach zewnętrznych,
    - Uwierzytelnianie AD,
    - Serwer i klient LDAP,
    - Powiadomienia (e-mail),
    - Kosz sieciowy,
    - SNMP,
    - Logowanie administratora przez Telnet i SSH,
    - **Gwarancja minimum 24 miesiące** lub dłużej zgodnie ze złożoną ofertą gwarancji producenta on-site,
    - W przypadku wystąpienia awarii dysku twardego w urządzeniu objętym gwarancją, uszkodzony dysk twardy pozostaje u Zamawiającego.

Dodatkowo należy dostarczyć kartę sieciową 2 portową 10GE SFP+ oraz moduł do zamontowania z dwoma dyskami 240GB SSD NVMe M.2 kompatybilnymi z serwerem NAS.

## 2.5 UTM – 2 szt.

**1. Wymagania Ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

**2. Funkcje modułu Firewall**

1. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
2. Możliwość uruchomienia w formie klastra wysokiej dostępności (HA) - co najmniej Active-Passive.
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.

22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego
29. agenta na stacjach roboczych użytkowników.
30. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
31. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
32. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
33. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
34. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
35. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
36. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
37. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
38. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
39. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
40. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.

41. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

**3. Dostarczony system bezpieczeństwa musi zapewniać:**

1. Ochronę z wykorzystaniem mechanizmów IPS.
2. Ochronę antywirusową.
3. Ochronę przed nieznanymi zagrożeniami.
4. Ochronę przed phishingiem.
5. Ochronę przed niechcianą pocztą.
6. Kontrolę wykorzystywanych aplikacji.
7. Możliwość filtrowania URL.

**4. Parametry fizyczne systemu Firewall:**

1. Element systemu pełniący funkcję Firewall musi dysponować:
   - Min. 8 portami 1Gb RJ45 w tym 2 porty obsługujące standard PoE+ (802.3at).
   - Możliwość rozbudowy urządzenia o dodatkowy port 10Gb SFP+.
   - Wbudowany dysk SSD o pojemności min. 128GB.
   - Minimum 4 GB pamięci RAM.
   - Minimum 2 porty USB 3.0.
   - Minimum jeden port typu Console.
   - Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza.

**5. Parametry wydajnościowe systemu:**

- Przepustowość Firewall minimum: 4.7 Gbps.
- Przepustowość IPSec VPN nie mniejsza niż: 1.4 Gbps.
- Przepustowość skanowania antywirusowego nie mniejsza niż: 1.1 Gbps.
- Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 909 Mbps.
- Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 631 Mbps.
- Obsługa nie mniej niż: 60 tuneli IPSec site-to-site.
- Obsługa nie mniej niż: 60 tuneli client-to-site.
- Obsługa nie mniej niż: 500.000 jednoczesnych połączeń.
- Obsługa nie mniej niż: 25.000 nowych połączeń na sekundę.
- W ramach Firewall system musi obsługiwać minimum: 75 sieci VLAN.


6. **W ramach ochrony przed atakami system musi zapewniać:**
   1. Automatyczną aktualizację bazy sygnatur IPS. Powinna ona zawierać co najmniej 4500 definicji sygnatur.
   2. Automatyczne blokowanie znanych źródeł ataków.
   3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
   4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
   5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.
   6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.
7. **W ramach kontroli antywirusowej system musi zapewniać:**
   1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.
   2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
   3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
   4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.
   5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
   6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
   7. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
   8. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
   9. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.
8. **W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać:**
   1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:
      - W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).
      - Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.

- Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.
- Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.
- Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.
- Możliwość analizy plików o rozmiarze co najmniej 10MB.
- Brak ograniczeń co do ilości analizowanych plików

**9. W ramach ochrony przed phishingiem system musi zapewniać:**

1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:
   - Możliwość blokowania dostępu do spreparowanych stron.
   - Ochronę przed phishingiem nie zależnie od typu połączenia, protokołu, portu.
   - Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.
   - Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.
   - Kontrolę zapytań DNS.

**10. W ramach kontroli antyspamowej system musi zapewniać:**

1. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
2. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
3. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
4. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.
5. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

**11. W ramach filtrowania zawartości URL system musi zapewniać:**

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url powinna zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Odpytywanie bazy on-line w czasie rzeczywistym.
4. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.

5. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
6. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
7. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
8. Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.
9. Możliwość filtrowania treści w oparciu o typy MIME.
10. Możliwość blokowania plików cookies dla określonych domen.
11. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
12. Analizę treści dla protokołu https.
13. Wyłączenie inspekcji https dla wybranych kategorii stron www.

**12. W ramach kontroli aplikacyjnej system musi zapewniać:**

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1000, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.

**13. Wymagane funkcje VPN systemu:**

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.

10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
13. Dla połączeń Client-to-Site możliwość zastosowania dwuskładnikowego uwierzytelnienia w oparciu o tokeny sprzętowe lub programowe.
14. Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.
15. Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.
16. Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML.

**14. Zarządzanie**

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.
2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

**15. Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:**

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online

4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania powinny zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.
17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
19. Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
23. Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.

**16. Licencje i wsparcie techniczne**

1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Powinny one obejmować:

2. Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem – na okres 1 roku.

**17. Gwarancja oraz wsparcie**

Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**18. Dokumenty i certyfikaty**

W ramach postepowania, wraz z e sprzętem i licencjami należy dostarczyć:

- Oświadczenie producenta lub oświadczenie autoryzowanego przedstawiciela producenta potwierdzające zgodność wszystkich parametrów oferowanego urządzenia wskazanych w Opisie przedmiotu zamówienia.

Wraz z ofertą należy złożyć poniższe dokumenty:

- Deklaracja zgodności CE oferowanego urządzenia.

## 2.6 Szkolenie UTM - 1 kpl.

### 2.6.1 Szkolenia stacjonarne dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania (typ I) – 1szt.

Szkolenie z obsługi zakupionego urządzenia UTM dla jednego informatyka Urzędu Gminy Lubań.

Zakres szkolenia musi obejmować minimum:

- Administracja. Konfiguracja i zarządzanie Firebox (NTP i SNMP; Podstawy zasad zapory...);
- Wykrywanie zagrożeń (Default Handling Packet; blokowanie adresów IP i portów; rodzaje ochrony przed zagrożeniami);
- Logowanie i monitorowanie - Dimension (Cloud; Raporty Dimension; Fireware Web UI);
- Ustawienia sieciowe (DNS, aliasy, sieci VLAN, Multi-Wan, SD-WAN, Quality of Service (QoS)NAT'owanie;
    - Formy NAT'a dostępne w Firebox'ie;
    - Dynamic NAT – co to jest i jak skonfigurować;
    - Użyj Static NAT do ochrony Twoich publicznych serwerów;
    - NAT 1-do-1;
- Reguły Zapory Sieciowej (Policy Manager; konfiguracja; ustawianie);
- Usługi bezpieczeństwa - Fireware Web UI;

- Reguły Zapory Sieciowej w trybie Proxy (DNS; serwer DNS; serwer Proxy; APT Blocker; VoIP; proxy SMTP, IMAP i POP3; WebBlocker oraz proxy HTTP i HTTPS; Zasady HTTPS-proxy 187; E-mail Proxy i blokowanie spamu; Ustawienia URL filteringu; Instalacja i konfigurowanie modułów);
- Autoryzacja użytkowników (uwierzytelnianie; typy; grupy; niestandardowy certyfikat web server)
- Mobilny VPN (VPN z IKEv2; VPN z SSL; VPN z L2TP; VPN z IPSec)
- Branch Office VPN - Łączenie lokalizacji tunelem VPN (Nowość)
    - Wprowadzenie do BOVPN
    - Jak działa BranchOffice VPN?
    - Topologia VPN
    - Typy BOVPN
    - Różnice między typami BOVPN
    - Algorytmy i protokoły IPSec VPN
    - Zasady ruchu VPN
    - Jak skonfigurować ręcznie BOVPN między dwoma Firebox'ami
    - BOVPN i NAT
    - BOVPN i dynamiczne publiczne adresy IP
    - BOVPN przez TLS
    - Topologie BOVPN
    - Rozwiązywanie problemów z tunelami BOVPN.

**Szkolenie** należy zrealizować w postaci dostaw vouchera z opcją do wykorzystania przez kolejne 9 miesięcy od momentu ich dostarczenia.

Szkolenia muszą być prowadzone w Autoryzowanym Centrum Szkoleniowym, min. 4 dni szkoleniowe po 8 godzin łącznie min. 32 godziny.

Wykonawca zapewni dostęp do autoryzowanych materiałów szkoleniowych.

Wykonawca zapewni Certyfikat ukończenia szkolenia.

### 2.6.2 Szkolenia stacjonarne dla pracowników urzędu w zakresie obsługi zakupionego sprzętu i oprogramowania (typ II) – 1szt.

Szkolenia dla jednego Informatyka z Urzędu Gminy Lubań.

**Szkolenie 1**

Program Administrowanie AD o zakresie nie mniejszym niż MS-10969 Active Directory Services with Windows Server.

- Wdrażanie i administracja AD DS w systemie Windows Server 2019.

- Bezpieczne wdrożenie AD DS.

- Wdrażanie i konfiguracja lokacji AD DS oraz zarządzanie replikacją.

- Wdrażanie i zarządzanie zasadami grupy.

-Zarządzanie ustawieniami użytkowników za pomocą zasad grupy.

- Proces implementacji hierarchii urzędu certyfikacji za pomocą usług AD CS i sposobami zarządzania urzędami certyfikacji.

- Wdrażanie i zarządzanie certyfikatami.

- Wdrażanie i zarządzanie AD RMS.

- Wdrażanie i zarządzanie usługami AD FS.

- Zabezpieczanie i zapewnianie dostępu do danych za pomocą technologii takich jak dynamiczna kontrola dostępu, foldery robocze i dołączanie do miejsca pracy.

- Proces monitorowania, rozwiązywania problemów i zapewnienie ciągłości działania usług AD DS.

- Proces implementacji usługi Windows Azure Active Directory.

-Wdrażanie i zarządzanie usługami Active Directory Lightweight Directory Services (AD LDS).

**Szkolenie** należy zrealizować w postaci dostaw vouchera z opcją do wykorzystania przez kolejne 9 miesięcy od momentu ich dostarczenia.

Szkolenia muszą być prowadzone przez autoryzowanego trenera Microsoft (MCT).

Wykonawca zapewni dostęp do autoryzowanych materiałów szkoleniowych w platformie SkillPipe.

Wykonawca zapewni Certyfikat ukończenia szkolenia.

**Szkolenie 2**

Program:

- Administracja. Konfiguracja i zarządzanie

- Wykrywanie zagrożeń

- Logowanie i monitorowanie

- Ustawienia sieciowe

- NAT'owanie

- Reguły Zapory Sieciowej

- Usługi bezpieczeństwa - Fireware Web UI

- Reguły Zapory Sieciowej w trybie Proxy

- E-mail Proxy i blokowanie spamu

- Ustawienia URL filteringu

- Autoryzacja użytkowników

- Mobilny VPN

- Branch Office VPN - Łączenie lokalizacji tunelem VPN

**Szkolenie** należy zrealizować w postaci dostaw vouchera z opcją do wykorzystania przez kolejne 9 miesięcy od momentu ich dostarczenia.

Szkolenia muszą być prowadzone przez autoryzowanego trenera UTM.

Wykonawca zapewni Certyfikat ukończenia szkolenia.

## 2.7 Wdrożenie i konfiguracja sprzętu oraz sieci wraz z uruchomieniem domeny AD

1. Szczegółowy opis montażu elementów wyposażenia serwerowni.
2. Konfiguracja sprzętu musi być wykonywana w godzinach i dniach wolnych od pracy Zamawiającego, w godzinach od 16:00 do 6:00 rano dnia kolejnego lub w weekendy. W terminach uzgodnionych z Zamawiającym.
3. Macierz dyskowa musi być zainstalowana (dyski zamontowane) i skonfigurowana do pracy wg ustaleń z zamawiającym, wykonawca przeprowadzi szkolenie z obsługi macierzy.
4. Serwery oraz NAS muszą być zainstalowane i skonfigurowane, gotowe do pracy wg ustaleń z zamawiającym. W odniesieniu do NASa Wykonawca przeszkoli w zakresie obsługi i administracji serwera NAS administratora sieci. Serwer NAS ma umożliwiać między innymi archiwizację przyrostową i pełną serwerów zainstalowanych w budynku urzędu.
5. Kable światłowodowe w serwerowni w przypadku potrzeby powinny zostać przedłużone i zespawane.
6. Serwery muszą zostać zainstalowane w szafie RACK
7. Skonfigurowanie połączeń fizycznych, logicznych, podłączenie i skonfigurowanie urządzenia pozwalające na rozpoczęcie pracy.
8. Serwer musi mieć zainstalowany zaproponowany system oraz załączone oprogramowanie i być skonfigurowane do pracy. Serwer NAS zapasowy będzie wykorzystywany do celów backupu oraz do zabezpieczenia przed ransomware, co należy skonfigurować.
9. System należy zainstalować i skonfigurować na systemie macierzowym zgodnie z zaleceniami zamawiającego oparty na platformie wirtualizacji Hyper-V Server. Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.
10. W urządzeniach Aktywnych Wykonawca nada IP służące do zarządzania, zamienić standardowe Hasła na wskazane przez Zamawiającego, konfiguracyjnie odseparować sieci produkcyjną od sieci zarządzalnej.

11. Wykonawca:

    a. Zapewni połączenia pomiędzy urządzeniami typu: przełączniki agregacyjne i dostępowe, 1 serwer, 1 serwer NAS, UTM wykorzystując wkładki światłowodowe 10GE z patchcordami światłowodowymi kompatybilnymi zaoferowanymi wkładkami lub DAC zapewniając maksymalną prędkość i przepustowość. UTM połączy 1GE RJ45 w trybie

    b. Dokona zainstalowania i skonfigurowania DC wraz z kontrolerem zapasowym DC

    c. Utworzy i skonfiguruje role: WSUS, DHCP, SERWER PLIKÓW, NTP,

    d. Przeprowadzi audyt istniejących polityk oraz wdroży rekomendowane polisy bezpieczeństwa,

    e. Utworzy 3 przykładowe polityki GPO.

    f. Uruchomi dodatkowe usługi – zgodnie z potrzebami Zamawiającego.

    g. Przeprowadzi instruktaż dla Administratora.

    h. Zainstaluje wszystkie zamówione programy, zaktualizuje do najnowszej wersji.