Załącznik nr 1a

Parametry sprzętu

**Część I**

**Dostawa serwerów i macierzy wraz z migracją aktualnego środowiska wirtualizacji**

1. **Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach w ilościach:
	1. Serwer – 3 sztuki
	2. Macierz dyskowa – 1 sztuka
2. konfiguracja, instalacja serwerów (3 sztuki) oraz macierzy (1 sztuka) oraz migracja zwirtualizowanego środowiska Zamawiającego na nowo dostarczone serwery i macierz
3. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;
4. przeprowadzenie testów po procesie migracji
5. **Wymagania szczegółowe Zamawiającego**

**Zestawienie minimalnych wymaganych parametrów technicznych serwerów (3 sztuki):**

|  |  |  |
| --- | --- | --- |
| **Nazwa elementu lub cechy** | **Parametry** | **Wykonawca zobowiązany jest wskazać szczegółowe parametry techniczne jakie oferuje, nie dopuszcza się wskazania zakresu, opis musi potwierdzić spełnienie wszystkich wymagań określonych w kolumnie „parametry”** |
|  |  | **Nazwa producenta i model serwera: …………………..** |
| **Obudowa** | - do instalacji w szafie Rack 19", wysokość nie więcej niż 1U, z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych; |  |
| **Procesor** | - Zainstalowane 2 procesory w architekturze x86, maksymalnie 8-rdzeniowe, o TDP nie większym niż 105W. Wynik wydajności procesora instalowanego w oferowanym serwerze nie może być niższy niż 34573 dla wielu wątków, w konfiguracji dwuprocesorowej, opublikowanym przez PassMark CPU Mark.Stan na dzień 17**.11.2022** | **Nazwa producenta i model procesora: …………………..** |
| **Płyta główna** | - Płyta główna dedykowana do pracy w serwerach, wyprodukowana przez producenta serwera lub być przez niego certyfikowana;- Z możliwością zainstalowania do dwóch procesorów wykonujących 64-bitowe instrukcje;- Wyposażona w moduł TPM 2.0;- Minimum 32 sloty DIMM na pamięć DDR4; |  |
| **Pamięć operacyjna** | - Zainstalowane minimum 192GB pamięci RAM o częstotliwości minimum 3200MHz w modułach o pojemności 16GB każdy; - Możliwość rozbudowy/rekonfiguracji serwera do 8TB pamięci RAM DDR4; |  |
| **Zabezpieczenie pamięci** | - Wsparcie dla: memory mirroring, ECC, SDDC lub Advanced ECC; |  |
| **Procesor Graficzny** | - Zintegrowana karta graficzna z minimum 16MB pamięci, osiągająca rozdzielczość 1920x1200 przy 60 Hz;- 1 port VGA na tylnym panelu serwera oraz jeden port VGA na panelu przednim; |  |
| **Zatoki dyskowe i dyski** | - Serwer wyposażony w 8 zatok dyskowych hot-plug 2.5” umożlwiających instalację dysków SSD/HDD interfejsem SAS/SATA;- Serwer wyposażony w min. 2 dyski SATA SSD o pojemności min. 240GB każdy. Dyski klasy serwerowej dedykowane do pracy w oferowanym serwerze i o parametrze DWPD min. 1;- Możliwość rozbudowy serwera o 2 dyski M.2 SSD NVMe o pojemności min. 960GB. Rozwiązanie dedykowane jako nośnik boot, musi umożliwiać konfigurację sprzętowego mirroringu (RAID 1). |  |
| **Kontroler dyskowy** | - Serwer wyposażony w sprzętowy kontroler RAID obsługujący dyski SAS 3.0 i pozwalający na konfigurację RAID 0,1,10,5;- Serwer umożliwiający rozbudowę/rekonfigurację o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 2 GB pamięci cache z podtrzymywaniem bateryjnym- Kontroler obsługujący funkcjonalność SSD Cache na poziomie sprzętowym tj. możliwość wykorzystania dysku SSD do przyśpieszenia operacji odczytu dla grupy RAID na dyskach HDD. |  |
| **Zasilacz** | - Minimum dwa redundantne zasilacze o mocy min. 750W z certyfikatem 80Plus w wersji minimum Platinum. |  |
| **Interfejsy sieciowe** | - Jeden port RJ-45 o przepustowości 1GbE dedykowany dla karty zarządzającej. - 2 porty 10GbE BASE-T oraz - dwa porty 1GbE BASE-T nie zajmujące slotów PCIe serwera; - Karta LAN posiadająca 2 porty 10GbE SFP28 10GbE/25GbE wyposażona we wkładki światłowodowe wielomodowe 10Gbits |  |
| **Sloty PCIe** | - Serwer posiadający min. 3 sloty PCIe generacji 4.0 w tym wszystkie sloty działające z prędkością x16; |  |
| **Dodatkowe porty** | - z przodu obudowy: 1x USB 3.0 - z tyłu obudowy: 2x USB 3.0, 1x VGA- wewnętrzne: 1 x USB 3.0 |  |
| **Chłodzenie** | - Wentylatory wspierające wymianę Hot-Swap, zamontowane nadmiarowo minimum N+1 |  |
| **Zarządzanie** | * Serwer musi posiadać moduł zarządzający wyposażony w minimum jeden port 10/100/1000 Base-T Ethernet, pozwalający na zdalny dostęp i zarządzanie serwerem przy użyciu graficznego interfejsu Web.
* - Moduł musi umożliwiać:
* monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe
* dostęp do karty zarządzającej poprzez dedykowany port RJ45 z tyłu serwera lub dostęp do karty możliwy:
	+ z poziomu przeglądarki webowej (GUI)
	+ z poziomu linii komend (SSH lub IPMI)
* wbudowane narzędzia diagnostyczne
* zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego
* obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie
* wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników
* przesyłanie alertów poprzez e-mail oraz SNMP
* obsługa zdalnego serwera logowania (remote syslog)
* wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB
* funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy)
* monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji
* konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)
* zdalna aktualizacja oprogramowania (firmware)
* możliwość równoczesnej obsługi przez min. 2 administratorów
* wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
 |  |
| **Funkcje zabezpieczeń** | - Czujnik otwarcia obudowy;- Ramka zabezpieczająca przed nieautoryzowanym dostępem do dysków serwera; |  |
| **Urządzenia hot swap** | - Dyski twarde, zasilacze, wentylatory. |  |
| **Wspierane systemy operacyjne** | - Microsoft Windows Server 2019, 2022, Red Hat Enterprise Linux 8, VMware vSphere (ESXi) 8.0 ; |  |
| **Gwarancja** | - min 36 miesięcy wsparcia producenta w trybie pełnego serwisu on-site NBD. Przy czym NBD określa czas reakcji w miejscu instalacji sprzętu;- Usługa wsparcia technicznego musi być świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń; |  |
| **Inne** | - Serwer musi być wyprodukowany zgodnie z normą ISO-9001 oraz ISO-14001;- 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;- Możliwość rozbudowy serwerów zgodnie z ww. wyżej specyfikacją musi być możliwa przy użyciu certyfikowanych komponentów oraz zachowaniu pełnego wsparcia i gwarancji producenta serwera;- Serwer -musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce;- wszystkie interfejsy muszą być wyposażone w odpowiednie okablowanie: - zasilające; - sygnałowe umożliwiające połączenie z przełącznikami oraz poniższą macierzą; |  |

**Zestawienie minimalnych wymaganych parametrów technicznych macierzy dyskowej (1 sztuka)**

|  |  |  |
| --- | --- | --- |
| **Nazwa elementu lub cechy** | **Parametry** | **Wykonawca zobowiązany jest wskazać szczegółowe parametry techniczne jakie oferuje, nie dopuszcza się wskazania zakresu, opis musi potwierdzić spełnienie wszystkich wymagań określonych w kolumnie „parametry”** |
|  |  | **Nazwa producenta i model macierzy:****……………………………………..** |
| Parametry podstawowe  | - System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19'' i zajmować nie więcej niż 2U przestrzeni;- System musi wspierać dyski: SAS od 1200GB do minimum 1800GB; SATA/NL-SAS od 4TB do minimum 18TB; SSD od 800GB do minimum 15,3TB;- Dostarczany system wyposażony w min. 6 dysków 1.92TB SAS SSD;- urządzenie musi być wyposażone w odpowiednie okablowanie: - zasilające; - sygnałowe, umożliwiające połączenie z powyższymi serwerami oraz przełącznikami; |  |
| Kontroler  | - Dwa kontrolery wyposażone w przynajmniej 8GB cache każdy pracujące w trybie dual active (active/active);- W przypadku awarii zasilania dane niezapisane na dyski, przechowywane w pamięci muszą być zabezpieczone za pomocą podtrzymania bateryjnego przez 72 godziny lub jako zrzut na pamięć flash; |  |
| Interfejsy  | Oferowana macierz musi posiadać minimum:- 8 portów 10GbE/25GbE SFP+ iSCSI. Wszystkie porty wyposażone we wkładki wielomodowe LC/LC pozwalające na pracę z pełną przepustowością tj. wkładki SFP 10GbE/25GbE multimode;- 2 porty RJ-45 BASE-T 1GbE dedykowane do zarządzania urządzeniem (po 1 porcie na kontroler). |  |
| RAID  | - Wsparcie dla RAID: 0, 1, 5, 6, 10- Dodatkowo macierz musi posiadać mechanizm tworzenia wirtualnej przestrzeni na minimum 96 dyskach macierzy wraz z wyliczaniem parzystości oraz podwójnej parzystości w celu zabezpieczenia danych. Mechanizm ten musi być przygotowany do optymalizacji procesów odtwarzania dysków pojemnościowych. |  |
| Inne wymagania  | - Macierz musi posiadać wsparcie dla wielościeżkowości dla systemów: Microsoft® Windows Server®, Red Hat Enterprise Linux®, Novell SUSE Linux Enterprise Server, VMware® ESX®- Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen.- Macierz musi posiadać funkcjonalność klonowania danych- Macierz musi umożliwiać dynamiczną zmianę rozmiaru wolumenów logicznych bez przerywania pracy macierzy i bez przerywania dostępu do danych znajdujących się na danym wolumenie.- Macierz musi posiadać funkcjonalność partycjonowania macierzy na odseparowane od siebie logicznie systemy, na których rezydują osobne dyski logiczne dla heterogenicznych systemów. Licencja na macierzy musi pozwalać na wykonanie do 128 partycji. - Macierz musi posiadać funkcjonalność automatycznego balansowania obciążenia kontrolerów macierzy przez przełączanie w trybie online volumenów logicznych pomiędzy nimi w zależności od wygenerowanego na nich ruchu. Musi istnieć możliwość wyłączenia tej funkcjonalności z poziomu interfejsu użytkownika. - Macierz musi pozwalać na dynamiczną migrację pomiędzy poziomami RAID.- Z poziomu graficznego interfejsu do zarządzania musi istnieć możliwość sprawdzenia stanu zużycia dysków SSD.- Macierz musi posiadać możliwość integracji z Active Directory w zakresie definicji i mapowania grup i użytkowników pod kątem autentykacji. - Macierz musi posiadać oprogramowanie do aplikacji pozwalające na integrację z: Vmware vCenter – provisioning i monitoring macierzy z widoku vCenter |  |
| Gwarancja i serwis  | - min. 36 miesięcy wsparcia producenta w trybie pełnego serwisu on-site NBD. Przy czym NBD określa czas reakcji w miejscu instalacji sprzętu;- W przypadku awarii, dyski twarde pozostają u Zamawiającego;- Usługa wsparcia technicznego musi być świadczona przez producenta lub autoryzowany serwis producenta oferowanych urządzeń;- System musi być fabrycznie nowy i pochodzić z oficjalnego kanału dystrybucyjnego w Polsce;- Elementy, z których zbudowany jest system muszą być produktami producenta systemu lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta, o wymaganym w specyfikacji poziomie SLA; |  |

1. **Wymagane prace wdrożeniowe**
2. **Dostarczenie sprzętu wraz z konfiguracją i migracją zasobów wirtualnych na nowe urządzenia**
	1. Zinwentaryzowanie i walidacja aktualnego środowiska serwerowego objętego migracją (3 serwery fizyczne z wirtualizatorem VMWare posiadanym przez Zamawiającego oraz macierz dyskowa)
	2. Podłączenie serwerów (3 sztuki) oraz macierzy (1 sztuka) do infrastruktury elektrycznej i sieciowej Zamawiającego
	3. Wstępna konfiguracja serwerów i macierzy polegająca na nadaniu dostępów, adresacji oraz aktualizacji oprogramowania sprzętowego do najnowszej zalecanej przez producenta wersji
	4. Przygotowanie środowiska wirtualizacji VMWare na nowo dostarczonych serwerach. Zamawiający zobowiązuje się do dostarczenia licencji dla aktualnie wykorzystywanego w infrastrukturze wirtualizatora.
	5. Wykonawca zobowiązuje się do zaktualizowania obecnie posiadanej wersji systemu VMWare do wersji 8.0
	6. Przekazanie dostępów administracyjnych Zamawiającemu.
	7. Wykonanie procesu migracji aktualnych zasobów wirtualnych na dostarczone serwery oraz macierz
	8. Testy po uruchomieniu środowiska wirtualnego, polegające na sprawdzeniu poprawności uruchamiania się środowiska systemowego oraz poprawności pracy systemów
	9. Przygotowanie dokumentacji powdrożeniowej, zawierającej opis wdrożonej konfiguracji wirtualizacji zasobów
	10. Wykonawca do uruchomienia środowiska wykorzysta aktualnie stosowane licencje Microsoft Windows Server
	11. Wykonawca po poprawnym wdrożeniu nowych urządzeń do sieci produkcyjnej, zobowiązany jest to przywrócenia ustawień fabrycznych na obecnie wykorzystywanych urządzeniach (serwer - 3 sztuki oraz macierz dyskowa – 1 sztuka) oraz przekazaniu ich do Zamawiającego.
	12. Wykonawca zobowiązany jest do dodania nowo utworzono klastra do posiadanego przez Zamawiającego systemu kopii zapasowych.

**Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym**

**Zamawiający zaleca zapisanie dokumentu w formacie PDF.**

Załącznik 1b

**Część II**

**Modernizacja infrastruktury sieciowej**

1. **Przedmiot zamówienia:**

Przedmiotem zamówienia jest:

1. dostawa fabrycznie nowego Sprzętu, nie używanego w innych środowiskach ani projektach, w ilościach:
	1. Przełącznik sieciowy Typ 1 – 2 sztuki
	2. Przełącznik sieciowy Typ 2 – 4 sztuk
	3. Przełącznik sieciowy Typ 3 – 3 sztuk
	4. moduł konwertera interfejsu SFP – łącznie 48 sztuk
2. konfiguracja urządzeń oraz fizyczna instalacja w infrastrukturze IT Zamawiającego;
3. wymiana obecnie użytkowanych urządzeń na nowo dostarczone – odtworzenie obecnej konfiguracji na nowych urządzeniach
4. udzielenie przez Wykonawcę gwarancji i zapewnienie w jej ramach serwisu gwarancyjnego oraz wsparcia technicznego na dostarczony Sprzęt;
5. dostarczenie przez Wykonawcę dokumentacji dostarczonego Sprzętu;
6. **Termin realizacji zamówienia**

Termin realizacji zamówienia wynosi 140 dni od dnia podpisania umowy.

1. **Wymagania szczegółowe Zamawiającego:**

**Przełącznik Typ 1 (core)**

Wymagania podstawowe

1. Przełącznik musi posiadać minimum:
	1. 24 porty 1Gb/10Gb SFP+
	2. 1 port 10Gb/40Gb QSFP+
	3. 2 porty 10Gb/25Gb/40Gb/50Gb/100Gb QSFP28, które zostaną wykorzystane do stworzenia stosu za pomocą kabli DAC o przepustowości 400Gb (musi istnieć możliwości wykorzystania ich, jako standardowe porty uplink o przepustowości 100Gb)
2. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management, port konsoli szeregowej oraz port USB
3. Wysokość urządzenia nie większa niż 1U
4. Możliwość łączenia do 8 urządzeń w stos zarządzany z pojedynczego adresu IP, połączenie pomiędzy urządzeniami musi być możliwe z wykorzystaniem portów 100Gb
5. Nieblokująca architektura o wydajności przełączania min. 880 Gbps
6. Szybkość przełączania min. 700 milionów pakietów na sekundę
7. Przełącznik musi być wyposażony w dwa zasilacze, które umożliwiają uzyskanie redundancji zasilania z możliwością wymiany w czasie działania przełącznika. Zasilacze muszą zapewniać przepływ powietrza tył-przód
8. Modularny system chłodzenia z przepływem powietrza tył-przód
9. Tablica MAC adresów min. 272K
10. Pamięć operacyjna: min. 4 GB RAM DDR3
11. Pamięć SSD: min. 32 GB
12. Bufor pakietów: min 12 MB
13. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
14. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
15. Obsługa Quality of Service – co najmniej:
	1. IEEE 802.1p
	2. DiffServ RFC2474 oraz RFC2598, RFC2597 i RFC2475
	3. 8 kolejek priorytetów na każdym porcie wyjściowym
16. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora
17. Możliwość monitorowania zajętości CPU
18. Obsługa wirtualnych routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach

**Wymagania szczegółowe:**

1. Obsługa routingu IPv4:
	1. Pojemność tabeli routingu min. 256K wpisów
	2. Routing statyczny
	3. Obsługa routingu dynamicznego IPv4:
		1. RIP v1/v2
		2. OSPFv2
		3. BGP4 oraz MBGP (BGP4+)
		4. IS-IS
	4. Policy Based Routing dla IPv4
2. Obsługa Routingu IPv6:
	1. Pojemność tabeli routingu min. 128K wpisów
	2. Routing statyczny
	3. Obsługa routingu dynamicznego dla IPv6:
		1. RIPng
		2. OSPFv3
		3. BGP4 oraz MBGP (BGP4+)
		4. IS-IS
	4. Obsługa 6to4 (RFC 3056)
	5. Policy Based Routing dla IPv6
3. Obsługa multicastów:
	1. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
	2. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping, PIM snooping
	3. Możliwość konfiguracji statycznych tras dla routingu multicastów
	4. Możliwość skonfigurowania przynajmniej 4K grup multicast
	5. Obsługa PIM-SM, PIM-DM oraz PIM-SSM
	6. Wsparcie dla Anycast RP dla PIM (RFC 4610)
4. Bezpieczeństwo:
	1. Obsługa Network Login
		1. IEEE 802.1x
		2. Web-based Network Login
		3. MAC based Network Login
	2. Obsługa wielu klientów (min. 12) Network Login na jednym porcie (Multiple supplicants)
	3. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
	4. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
	5. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma
	6. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
		1. definicji sieci VLAN,
		2. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
		3. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
		4. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
	7. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
	8. Bezpieczeństwo MAC adresów
		1. ograniczenie liczby MAC adresów na porcie
		2. zatrzaśnięcie MAC adresu na porcie
		3. możliwość wpisania statycznych MAC adresów na port/vlan
		4. możliwość wyłączenia MAC learning
	9. Zabezpieczenie przełącznika przed atakami DoS
		1. Networks Ingress Filtering RFC 2267
		2. SYN Attack Protection
		3. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
	10. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)
	11. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
	12. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
5. Bezpieczeństwo sieciowe:
	1. Obsługa redundancji routingu VRRP - RFC 2338
	2. Obsługa STP, RSTP, MSTP, PVST+
	3. Obsługa EAPS (RFC 3619) oraz G.8032
	4. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – możliwość konfiguracji co najmniej 128 grup po 32 porty w każdej z nich
	5. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.
6. Zarządzanie:
	1. Zarządzanie przez SNMP v1/v2/v3
	2. Obsługa SYSLOG z możliwością definiowania wielu serwerów
	3. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
7. Inne
	1. Wsparcie dla protokołów przeznaczonych do przesyłania w czasie rzeczywistym sygnałów audio, wideo oraz innych przez sieć Ethernet (np. RAVENNA, AVB lub równoważne) – jeśli wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w chwili dostawy;
	2. Możliwość uruchomienia MPLS, VPLS oraz L3VPN – jeśli wymagają dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w chwili dostawy;
	3. Możliwość uruchomienia funkcjonalności MACsec (802.1AE) - jeśli wymaga dodatkowej licencji lub modułów Zamawiający nie wymaga ich dostarczenia w chwili dostawy;
	4. Wsparcie dla API (RestConf lub NetConf)
	5. Możliwość konfiguracji VXLAN Tunneling End Point (VTEP) oraz Ethernet VPN (EVPN)
	6. Wsparcie dla DCB co najmniej:
		1. Priority Flow Control (IEEE 802.1Qbb)
		2. Data Center Bridging eXchange (DCBX) (IEEE P802.1Qaz/D2.3)
	7. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
	8. Możliwość uruchamiania skryptów
		1. Ręcznie
		2. O określonym czasie lub co wskazany okres czasu
		3. Na podstawie wpisów w logu systemowym
8. Zgodność z europejskimi normami EMC:
	1. EN 55032:2015 Class A
	2. EN 55024:2010
	3. EN 61000-3-2: 2014 (Harmonics)
	4. EN 61000-3-3: 2013 (Flicker)
	5. EN 300 386 v1.6.1 (EMC Telecommunications)
	6. 2014/30/EU EMC Directive

**Wymagane akcesoria:**

Każdy przełącznik musi być wyposażony w kabel zasilający oraz kabel typu DAC (Direct-Attach Copper) 100 Gigabit Ethernet QFSP28-QFSP28 długości min. 1 m umożliwiający połączenie przełączników w stos. Zamawiający wymaga, aby kable typu DAC 100 Gigabit Ethernet QSFP28-QFSP28 pochodziły od Producenta przełączników.

**Przełącznik Typ 2 i 3 (access)**

**Wymagania minimalne dotyczące wszystkich modeli przełączników dostępowych (Typ 2 i Typ 3):**

1. Wysokość urządzenia 1U
2. Każdy z przełączników musi być wyposażony w kabel zasilający i elementy do montażu w szafie typu RACK
3. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az na wszystkich portach 10/100/1000BASE-T
4. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management.
5. Przełącznik musi posiadać wbudowany zasilacz 230V AC, oraz musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza.
6. Możliwość łączenia do 8 przełączników w stos. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych
7. Tablica MAC adresów min. 16k
8. Pamięć operacyjna: min. 1GB pamięci DRAM
9. Pamięć flash: min. 4GB pamięci Flash oraz bufora pakietów min. 1,5MB
10. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094
11. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów)
12. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
13. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
14. Możliwość monitorowania zajętości CPU
15. Pojemność tabeli routingu min. 480 wpisów dla IPv4 oraz 240 wpisów dla IPv6
16. Routing statyczny
17. Obsługa routingu dynamicznego RIP dla IPv4 i IPv6
18. Możliwość rozszerzenia funkcjonalności przełącznika w przyszłości o wsparcie dla protokołu OSPF dla IPv4 i IPv6 – np. poprzez zakup dodatkowej licencji oprogramowania
19. Policy Based Routing dla IPv4 i IPv6
20. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
21. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping
22. Obsługa Network Login
	1. IEEE 802.1x
	2. Web-based Network Login
	3. MAC based Network Login
23. Obsługa wielu klientów (min. 8) Network Login na jednym porcie (Multiple supplicants)
24. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z systemu NAC
25. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
26. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma
27. Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie:
	1. definicji sieci VLAN,
	2. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
	3. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
	4. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
28. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
29. Bezpieczeństwo MAC adresów
	1. ograniczenie liczby MAC adresów na porcie
	2. zatrzaśnięcie MAC adresu na porcie
	3. możliwość wpisania statycznych MAC adresów na port/vlan
	4. możliwość wyłączenia MAC learning
30. Zabezpieczenie przełącznika przed atakami DoS
	1. Networks Ingress Filtering RFC 2267
	2. SYN Attack Protection
	3. zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
31. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika)
32. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
33. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
34. Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania
35. Obsługa STP, RSTP, MSTP, PVST+
36. Obsługa EAPS (RFC 3619) oraz G.8032
37. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów
38. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.
39. Zarządzanie przez SNMP v1/v2/v3
40. Obsługa SYSLOG z możliwością definiowania wielu serwerów
41. Sprzętowa obsługa sFlow
42. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
43. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
44. Możliwość uruchamiania skryptów
	1. ręcznie
	2. o określonym czasie lub co wskazany okres czasu
	3. na podstawie wpisów w logu systemowym

**Wymagania szczegółowe dla urządzeń Typu 2 (24-portowy):**

1. Przełącznik posiadający 24 portów 1G 100/1000BASE-T
2. Przełącznik posiadający 8 portów 1G SFP
3. Przełącznik mający możliwość rozbudowy (licencyjnie kosztem ilości wbudowanych portów SFP, lub za pomocą dodatkowego modułu) o 4 porty 10G SFP+.
4. Nieblokującą architekturę o wydajności przełączania min. 128 Gb/s
5. Szybkość przełączania min. 95 Milionów pakietów na sekundę

**Wymagania szczegółowe dla urządzeń Typu 3 (48- portowy):**

1. Przełącznik posiadający 48 portów 1G 100/1000BASE-T
2. Przełącznik posiadający 8 portów 1G SFP
3. Przełącznik mający możliwość rozbudowy (licencyjnie kosztem ilości wbudowanych portów SFP, lub za pomocą dodatkowego modułu) o 4 porty 10G SFP+.
4. Nieblokującą architekturę o wydajności przełączania min. 176 Gb/s
5. Szybkość przełączania min. 130 Milionów pakietów na sekundę

**Wymagania dotyczące wkładek do switchy**

Należy dostarczyć:

1. moduł konwertera interfejsu (Copper SFP) spełniający poniższe kryteria (44 sztuki):
	1. Musi być zgodny ze standardem 10/100/1000BASE-T
	2. Musi zapewniać transmisję na odległość 100 metrów dla kabla Cat 5 UTP
	3. Musi posiadać złącze miedziane typu RJ-45
	4. Musi pracować w zakresie temperatur od -40oC do 85oC
2. moduł SFP 1 Gbit, spełniających poniższe kryteria (4 sztuki):
	1. Musi być zgodny ze standardem SFP
	2. Musi zapewniać możliwość transmisji na odległość 100m dla światłowodów jednomodowych
	3. Musi zapewniać złącze optyczne LC
	4. Musi pracować w zakresie temperatur od -40oC do 85oC

Wszystkie wskazane wkładki muszą być kompatybilne z rozwiązaniami przedstawionymi w ofercie.

1. **Wymagania ogólne dla wszystkich typów przełączników sieciowych oraz wykonywanych prac:**
2. Dostarczone urządzenia muszą pochodzić z autoryzowanego kanału sprzedaży producentów na rynek polski – do oferty należy dołączyć odpowiednie oświadczenie producenta sprzętu
3. Dostarczone urządzenia muszą być objęte gwarancją opartą o świadczenia gwarancyjne producenta sprzętu, niezależnie od statusu partnerskiego Wykonawcy przez okres co najmniej 12 miesięcy
4. Aktualizacja oprogramowania układowego (firmware) do najnowszej stabilnej wersji, zalecanej przez producenta.
5. Konfiguracja przełączników w logiczny klaster (stack) dla przełącznika Typu 1 oraz wyposażenie przełącznika Typu 1 w dedykowane moduły konwertera interfejsów
6. Implementacja podsieci VLAN umożliwiających bezproblemową komunikację z pozostałymi segmentami sieci LAN Zamawiającego, stanowiąca odwzorowanie konfiguracji aktualnie wykorzystywanych przełączników: Extreme Networks X430, Extreme Networks x440, HPE 2910AL oraz Enterasys B5G124
7. Parametryzacja portów połączeniowych z pozostałymi przełącznikami w sieci Zamawiającego
8. Parametryzacja portów połączeniowych z pozostałymi przełącznikami wskazanymi w postępowaniu Zamawiającego (zapewnienie redundancji, łączności VLAN)
9. Parametryzacja protokołu drzewa rozpinającego współpracującego z pozostałymi przełącznikami,
10. Adresacja przełącznika w wydzielonej podsieci
11. Konfiguracja szyfrowanego dostępu zdalnego za pomocą protokołu SSH
12. Parametryzacja protokołu SNMP na potrzeby zewnętrznych systemów monitorowania sieci
13. Parametryzacja protokołu LLDP na potrzeby administrowania siecią LAN
14. Dostarczający jest zobowiązany do podłączenia urządzeń sieciowych w infrastrukturze Zamawiającego do wskazanych miejsc połączeń sieciowych i elektrycznych
15. Dostarczający jest zobowiązany do aktualizacji oprogramowania sprzętowego dostarczonych urządzeń do najnowsze dostępnej i zalecanej przez producenta wersji
16. Dostarczający musi utworzyć dostępy administracyjne do urządzeń oraz przekazać je Zamawiającemu
17. Montaż przełączników w szafach typu rack w miejscach wskazanych przez Zamawiającego
18. Implementacja połączeń fizycznych umożliwiających bezproblemowe działanie w sieci LAN dostarczonych przełączników wraz z konfiguracją
19. Implementacja połączeń fizycznych między przełącznikami a urządzeniami serwerowymi wraz z wykonaniem testów komunikacji między urządzeniami
20. Wykonanie testów komunikacyjnych mających na celu ocenę poprawności implementacji konfiguracji
21. Wykonanie testów poszczególnych protokołów mających na celu ocenę poprawności ich konfiguracji
22. Dostarczenie protokołów po wykonanych testach potwierdzających poprawność dostarczonej konfiguracji
23. Dokumentacja dostarczonego rozwiązania wraz zaimplementowaną konfiguracją
24. **Gwarancja**

Wymagana gwarancja - co najmniej 12 miesięcy oraz kontrakt serwisowy na okres co najmniej 12 miesięcy umożliwiający:

1. bezpłatne aktualizacje Firmware (minor i major release)
2. wymianę uszkodzonego komponentu z dostawą następnego dnia roboczego od uznania awarii
3. wsparcie techniczne producenta przez linię telefoniczną, e-mail oraz zdalną sesję w cyklu 24x7
4. dostęp do bazy wiedzy producenta

Załącznik 1c

**Część III**

**Rozszerzenie aktualnie posiadanego środowiska pracy w chmurze wraz z wdrożeniem oraz szkoleniem użytkowników**

1. **Przedmiot zamówienia**
2. Przedmiotem zamówienia jest rozszerzenie usługi pracy w chmurze.
3. Dostawa 100 licencji w subskrypcji rocznej usługi przetwarzania danych w chmurze, dedykowanej celom biurowym wraz z dołączeniem ich do posiadanego przez Zamawiającego tenanta w usłudze Microsoft, jako rozszerzenie funkcjonalności wykorzystywanego środowiska MS365. Dostarczone licencje muszą być widoczne i zarządzalne z poziomu tenanta MS365
4. Utworzenie kont użytkowniczych bazując na informacjach przekazanych przez Zamawiającego, przypisanie im dostarczonych licencji, uruchomienie skrzynek pocztowych dostępnych w ramach licencji oraz archiwizacja aktualnie użytkowanej przez pracowników Zamawiającego poczty elektronicznej
5. Przeprowadzenie szkolenia powdrożeniowego dla użytkowników z obsługi rozwiązania.
6. Obecnie zamawiający posiada aktywny tenant usługi chmurowej Microsoft 365 wraz z aktywnymi licencjami
7. **Termin realizacji zamówienia**

Termin realizacji zamówienia wynosi 60 dni od dnia podpisania umowy.

1. **Szczegółowe wymagania odnośnie dostawy licencji**
2. Ilekroć jest mowa o modelu licencyjnym należy przez to rozumieć pakiet biurowy w rozwiązaniu chmurowym.
3. Chmurowy pakiet biurowy, musi spełniać następujące wymagania:
4. Wymagania odnośnie interfejsu użytkownika:
	1. Pełna polska wersja językowa interfejsu użytkownika.
	2. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
5. Wymagane składowe chmurowego pakietu biurowego zwane usługami:
	1. Poczta e-mail i kalendarze - pojemność skrzynki 50GB, maksymalny rozmiar wiadomości 150MB,
	2. Przechowywanie i udostępnianie plików - każda licencja posiada przestrzeń w rozmiarze 1TB, dostępnej w postaci rozwiązania chmurowego w infrastrukturze Producenta
	3. Konferencje Online – do 300 osób,
	4. Wiadomości błyskawiczne i komunikator,
	5. Firmowa sieć społecznościowa,
	6. Witryny zespołów,
	7. Subskrypcja ma umożliwiać dostęp do internetowych wersji aplikacji pakietu chmurowego:
		1. klient poczty,
		2. edytor tekstu,
		3. arkusz kalkulacyjny,
		4. edytor prezentacji,
		5. notes.
		6. Aplikacje muszą być dostępne z poziomu przeglądarki internetowej.
	8. Usługa pocztowa,
	9. Zarządzanie pracą,
	10. Tworzenie biuletynów i prezentacji multimedialnych
	11. Interfejs API dla usług wchodzących w skład oferowanego pakietu
6. Pakiet musi być kompatybilny z formatami dokumentów obsługiwanych i tworzonych u Zamawiającego za pomocą posiadanego oprogramowania pakietów biurowych – MS Office 2013-2019, MS 365.
7. Zamawiający wymaga dostępu do najnowszych wersji modelu subskrypcji przez cały okres jej ważności, tj. przez 12 miesięcy od dnia ich dostarczenia.
8. Dostarczone subskrypcje muszą być aktywne przez okres 12 miesięcy od daty przekazania ich Zamawiającemu, określonej umową (nie później niż 14 dni od jej podpisania).
9. Wymagana jest możliwość korzystania z pomocy w dowolnym momencie, dzięki całodobowej telefonicznej i internetowej pomocy technicznej od firmy dostawcy usługi.
10. Wykonawca musi zapewnić, że dostarczone subskrypcje są wolne od wad, dobrej jakości oraz ich parametry i cechy są zgodne z założeniami niniejszego dokumentu
11. Subskrypcje pakietu biurowego muszą zostać przypisane do aktualnie posiadanego przez Zamawiającego konta licencyjnego Microsoft 365 – centrum administracyjne na koncie Zamawiającego, nie później niż 14 dni pod podpisaniu umowy.
12. **Wymagane prace wdrożeniowe**
13. Walidacja oraz dostosowanie konfiguracji aktualnie posiadanej usługi zgodnie z najlepszymi praktykami, zapewniającymi prawidłową funkcjonalność rozwiązania celem zastąpienia aktualnej usługi pocztowej
14. Implementacja licencji w rozwiązaniu;
15. Zaimportowanie użytkowników na podstawie listy przekazanej przez Zamawiającego;
16. Przypisanie licencji dla poszczególnych użytkowników;
17. Zapewnienie synchronizacji poświadczeń użytkowników z lokalną usługą katalogową Active Directory posiadaną przez Zamawiającego;
18. Zmiana wpisów MX kierujących z obecnego systemu pocztowego, celem przełączenia usługi pocztowej na dostarczone rozwiązanie;
19. Zarchiwizowanie aktualnych skrzynek do lokalnych plików w formacie .pst u 100 użytkowników;
20. Przygotowanie instrukcji zawierającej dane konfiguracyjne dla programów posiadanych przez Zamawiającego: Microsoft Outlook od wersji 2013 i nowszych oraz Mozilla Thunderbird;
21. Wykonanie dokumentacji z przeprowadzonych prac;
22. Prace wdrożeniowe muszą odbyć się po ustaleniu z Zamawiającym harmonogramu wdrożenia, który musi być przedstawiony Zamawiającemu do 4 tygodni od czasu podpisania umowy.
23. **Wymagania odnośnie szkolenia**
24. Szkolenie musi być realizowane w języku polskim.
25. Szkolenia realizowane będą jako szkolenia zamknięte.
26. Szkolenia muszą odbyć się w siedzibie Zamawiającego.
27. Zamawiający zapewni na potrzeby szkolenia projektor i dostęp do Internet.
28. Szkolący musi zapewnić laptopy do przeprowadzenia szkolenia dla każdego uczestnika szkolenia.
29. Szkolenie musi odbywać się w grupach. Zamawiający deklaruje wskazanie 5 grup szkoleniowych po 20 osób w grupie.
30. Realizujący szkolenie ma obowiązek sprawdzania obecności w trakcie każdego ze szkoleń na podstawie list uczestników przekazanych przez Zamawiającego
31. Szkolenie dla każdej z grup musi mieć związek z wdrożonym rozwiązaniem i dotyczyć: klienta poczty, edytora tekstu, arkusza kalkulacyjnego, edytora prezentacji, klienta poczty w wersji przeglądarkowej, komunikatora, witryn zespołów, dysku w chmurze.
32. Szkolenia mają przybliżać interfejs usług oraz ich obsługę: klient pocztowy w wersji przeglądarkowej, ustawianie autoresponderów, konfiguracji stopki, reguł i przekierowań, udostępniania plików oraz dobrych praktyk przy udostępnianiu i hasłowania adresów URL do dokumentów znajdujących się w usłudze dysku chmurowego, korzystania z komunikatora z uwzględnieniem konfiguracji audio/video, tworzenia spotkań, udostępniania linków spotkań, obsługi czatów, zespołów, grup, udostępniania konwersacji i plików za pośrednictwem komunikatora oraz netykiety, obsługi rozwiązań pakietu internetowego z uwzględnieniem edytora tekstu i arkusza kalkulacyjnego w kontekście pracy zespołowej na pliku, możliwości organizacji pracy na witrynach zespołów – szkolenie poglądowe.
33. Wykonawca ma zapewnić możliwość późniejszego odtworzenia spotkania (nagranie szkolenia), z zastrzeżeniem nierozpowszechniania nagrania poza obszar organizacji Zamawiającego
34. Wykonawca jest zobowiązany przeprowadzić szkolenie w oparciu o zaakceptowane przez Zamawiającego materiały dydaktyczne.
35. Wykonawca zobowiązany jest w porozumieniu z Zamawiającym ustalić dokładną datę przeprowadzenia szkoleń.
36. Zamawiający ustali na zasadzie negocjacji z Wykonawcą, w terminie maksymalnie 15 dni roboczych od daty podpisania umowy ramowy harmonogram szkoleń.
37. Wykonawca zobowiązany jest do wystawienia zaświadczenia o odbytym szkoleniu dla każdego uczestnika.

**Załącznik nr 1d**

**Część IV**

**Rozbudowa istniejącego środowiska zarządzania siecią wraz z wdrożeniem rozwiązania NAC**

1. **Przedmiot zamówienia**

Przedmiotem zamówienia jest:

1. Dostarczenie oraz wdrożenie systemów kontroli dostępu do sieci NAC
2. Przeprowadzenie szkolenia z wdrożonego rozwiązania dla administratorów systemu
3. **Termin realizacji zamówienia**

Zamawiający wymaga, aby realizacja niniejszego zadania u Zamawiającego, nastąpiła w terminie do 90 dni od dnia podpisania umowy.

1. **Wymagania odnośnie oprogramowania**
2. Z uwagi na aktualnie wykorzystywane rozwiązanie NetSight Suite (ExtremeManagementCenter), Zamawiający wymaga, aby oprogramowanie było uzupełnieniem bądź rozszerzeniem funkcjonalnym aktualnego środowiska, celem zapewnienia jednolitości środowiska i kompatybilności.
3. Zamawiający dopuszcza, aby rozwiązanie NAC zostało wdrożone jako rozwiązanie równoległe bądź zastępujące aktualnie posiadane.
4. Oprogramowanie zarządzające musi działać w architekturze klient-serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci.
	1. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux lub jako aplikacja dedykowana dla systemu wirtualizacyjnego VMWare
	2. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS
5. Aplikacja musi pozwalać na zarządzanie siecią przewodową i bezprzewodową z jednej konsoli
6. Aplikacja zarządzająca musi zarządzać wszystkimi oferowanymi urządzeniami
7. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
8. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
9. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
10. Aplikacja zarządzająca musi pozwalać na zarządzanie urządzeniami w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
11. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
12. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
13. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów
14. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
15. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla wskazanych urządzeń sieciowych.
16. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email’a, wysłanie trapu SNMP, wpisu do Syslog’a lub uruchomienie skryptu.
17. Aplikacja musi posiadać wbudowany Syslog serwer.
18. Aplikacja musi zapewniać możliwość konfiguracji oraz obsługi Alarmów generowanych na podstawie wpisów w logach systemowych lub logach uzyskiwanych z wykorzystaniem Syslog lub na podstawie SNMP Traps
19. Alarmy muszą zapewniać możliwość ograniczenia ich zakresu np. z dokładnością do zawartości zdarzeń rejestrowanych w logach, urządzeń lub grup urządzeń sieciowych.
20. Alarmy muszą mieć możliwość sygnalizowania problemów z danym urządzeniem poprzez sygnalizację np. czerwonym kolorem, wyświetlenia wszystkich alarmów jak również alarmów dla wskazanego urządzenia.
21. Alarmy muszą mieć możliwość konfiguracji automatycznej reakcji i wyzwolenia zdarzeń takich jak:
22. Wysłanie e-mail do wskazanej grupy adresowej
23. Wysłanie informacji SYSLOG do wskazanego serwera
24. Wysłanie TRAP SNMP do wskazanego adresu IP
25. Uruchomienie skryptu w systemie operacyjnym Linux
26. Uruchomienie skryptu skonfigurowanego w systemie zarządzającym
27. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
28. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
29. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
30. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
	1. połączeń pomiędzy poszczególnymi urządzeniami z monitorowaniem ich stanu
	2. konfiguracji sieci VLAN
31. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet/ssh oraz http/https
32. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
	1. adres IP urządzenia
	2. adresu MAC urządzenia
	3. nazwy urządzenia
	4. wersji oprogramowania
	5. wersji bootrom
	6. lokalizacji urządzenia
	7. danych kontaktowych administratora
	8. numeru seryjnego
	9. numeru inwentaryzacyjnego – własna numeracja
33. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
	1. możliwość automatycznej periodycznej realizacji backup’u konfiguracji urządzeń o wskazanym czasie
	2. możliwość realizacji backup’u konfiguracji z różną częstotliwością dla różnych grup urządzeń sieciowych
	3. możliwość odtworzenia wskazanej konfiguracji urządzenia
	4. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych w ramach tego samego urządzenia, ale z różnych dat lub pomiędzy różnymi urządzeniami i wskazanymi datami
	5. możliwość obsługi backup’u urządzeń sieciowych różnych producentów
34. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie
35. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
36. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
37. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd, CCTV, Access Point itp.
38. Aplikacja musi zapewniać możliwość konfiguracji skonfigurowanych polityk dostępu z uwzględnieniem:
	1. przyłączenia do sieci VLAN
	2. przyłączenia do serwisu w ramach „Fabric” z wykorzystaniem IEEE 802.1Qcj,
	3. konfiguracji Quality of Service
	4. konfiguracji filtracji ruchu z wykorzystaniem ACL – min. L3-L4
	5. możliwości wyłączenia uwierzytelniania wielu użytkowników na porcie – np. w przypadku polityki Access Point, gdzie uwierzytelnienie użytkowników jest przeniesione z portu przełącznika do punktu dostępowego lub kontrolera sieci bezprzewodowej.
39. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
	1. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać, gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
	2. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
	3. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
	4. generowanie raportów
40. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
	1. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
	2. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac, IEEE 802.11ax
	3. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:
		* adres IP kontrolera
		* liczba obsługiwanych klientów
		* szczytowe wartości zajmowanego pasma
		* wersja oprogramowania
	4. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
		* adres IP punktu dostępowego
		* MAC adres punktu dostępowego
		* wersja oprogramowania
		* typ punktu dostępowego
		* kanały pracy poszczególnych interfejsów radiowych
		* szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
	5. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
		* adres IP klienta
		* MAC adres klienta
		* nazwa użytkownika
		* nazwa punktu dostępowego, do którego dołączony jest użytkownik
		* BSSID, do którego dołączony jest użytkownik
		* SSID, do którego dołączony jest użytkownik
	6. Musi być zapewniona możliwość wczytania map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
		* zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
		* zaznaczenie kanałów pracy urządzeń z wizualizacją pokrycia obszaru danym kanałem
		* lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych
41. Aplikacja zarządzająca musi być zintegrowana z systemem zarządzania tożsamością (systemem kontroli dostępu) z zapewnieniem widzialności następujących informacji:
	1. adresu MAC
	2. adresu IP
	3. nazwy komputera
	4. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
	5. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
	6. adres IP urządzenia, do którego dołączony jest klient.
	7. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
	8. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.
	9. nazwa przydzielonej polityki bezpieczeństwa.
42. System zarządzania tożsamością zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
43. System zarządzania tożsamością klientów musi zapewniać możliwość ponownej autoryzacji użytkownika na żądanie (CoA – Change of Authorization) – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
44. System zarządzania tożsamością musi zapewniać możliwość wyboru i wysłania odpowiedniej polityki bezpieczeństwa do urządzenia uwierzytelniającego (np. przełącznik, punkt dostępowy itp.) na podstawie:
	1. Typu uwierzytelnienia – np. IEEE 802.1x PEAP, IEEE 802.1x TLS, IEEE 802.1x TTLS, MAC Authentication, logowanie do urządzenia za pomocą Telnet lub SSH, logowanie użytkownika poprzez Captive Portal itp.
	2. Przynależności do odpowiedniej grupy użytkowników – np. grupy użytkowników z systemu LDAP lub grupy użytkowników skonfigurowanych np. na podstawie nazwy użytkownika.
	3. Realizacji przyłączania do sieci z urządzenia o wskazanym adresie MAC lub prefix MAC
	4. Realizacji przyłączenia do sieci ze wskazanej „lokalizacji” – możliwość wyboru, czy dotyczy to sieci przewodowej, czy bezprzewodowej, adresu IP urządzenia, które zapewnia uwierzytelnianie, numeru portu lub ich zakres, SSID w przypadku sieci bezprzewodowej itp.
	5. Realizacji przyłączenia do sieci we wskazanych zakresach czasowych w poszczególnych dniach tygodnia
45. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List, grupa drukarek itp.
46. Przydział urządzenia do grupy urządzeń powinien być możliwy poprzez dodanie MAC adresu urządzenia do grupy oraz przez wskazanie uwierzytelnionego urządzenia na liście i przeniesienia go do wskazanej grupy – w celu uniknięcia konieczności przepisywania MAC adresów urządzeń.
47. System zarządzania tożsamością zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
48. System zarządzania tożsamością musi zapewniać możliwość modyfikacji stron służących do rejestracji gości – możliwość zmiany kolorów, wczytania własnego logo firmy, zmiany plików definicji strony CSS
49. System zarządzania tożsamością w ramach rejestracji gości musi zapewniać możliwość gromadzenia dodatkowych informacji wymaganych do wypełnienia przez użytkownika np. PESEL, nr. Dokumentu tożsamości, adres email, numer telefonu, adres email osoby zapraszającej itp.
50. System zarządzania tożsamością musi zapewniać możliwość akceptacji dostępu do sieci przez gościa poprzez wysłanie żądania oraz akceptacji przez osobę zapraszającą gościa do firmy.
51. System portalu www służący do rejestracji gości musi zapewniać obsługę gości w języku min. polskim, angielskim i niemieckim z możliwością wyboru tych języków na stronie przez rejestrującego się gościa.
52. System zarządzania tożsamością zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
	1. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
	2. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
	3. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
	4. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
	5. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
53. System zarządzania tożsamością musi być zintegrowany z systemem zarządzającym i jego funkcjami zapewniającymi automatyzację z wykorzystaniem mechanizmów skryptów Python – przykładowo musi zapewniać możliwość uruchomienia skryptu w języku Python po uwierzytelnieniu i autoryzacji systemu końcowego w ramach IEEE 802.1x i/lub MAC authentication
54. System zarządzania tożsamością zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 1 000 urządzeń klienckich (adresów MAC) przez okres minimum 2 lat.
55. System zarządzania musi posiadać przy współpracy z dostarczonymi urządzeniami pozwalając na analizę ruchu w sieci do warstwy 7 – dotyczy przełączników oraz sieci bezprzewodowej
56. Analiza ruchu w sieci do warstwy 7 musi zapewniać możliwość prezentacji z jakich aplikacji korzystają użytkownicy i urządzenia pracujące w sieci LAN i WLAN. Prezentacja musi zapewniać informacji ilościowe ruchu poszczególnych aplikacji.
57. Analiza ruchu musi zapewniać możliwość pomiarów czasów odpowiedzi sieci i czasów odpowiedzi aplikacji – czasy te mają pozwalać na szybką identyfikację ewentualnej przyczyny wolnej pracy klienta, wskazując, czy problem leży po stronie sieci, czy może po stronie konkretnej aplikacji.
58. System Analityki musi zapewniać bieżące monitorowanie krytycznych aplikacji sieciowych takich jak: DHCP, DNS, LDAP, RADIUS, Kerberos
59. System Analityki musi również zapewniać możliwość monitorowania własnych wybranych aplikacji.
60. Monitorowanie aplikacji musi zapewniać możliwość generowania alarmów w przypadku przekroczenia założonych lub automatycznie dobieranych progów czasów odpowiedzi aplikacji.
61. System Analityki musi mieć możliwość wyszukiwania informacji za pomocą wyszukiwarki informacji zapisanych w Systemie Analityki – np. wyświetl najwolniej działające aplikacji we wskazanej lokalizacji, wyświetl aplikacje zajmujące najwięcej pasma, wyświetl powyższe aplikacje dla wskazanego użytkownika itp.
62. System Analityki musi zapewniać możliwość tworzenia raportów.
63. System Analityki musi zapewniać możliwość regularnego tworzenia i wysyłania raportu do wskazanego adresu e-mail.
64. System zarządzania musi posiadać możliwość tworzenia skryptów CLI i Python, które pozwolą na uproszczenie zarządzania siecią poprzez wykonywanie tych samych operacji na wielu urządzeniach lub zapewnią automatyzację poprzez ich uruchomienie na podstawie różnorodnych zdarzeń występujących w Aplikacji Zarządzającej, Systemie Analityki, Systemie zarządzania tożsamością.
65. System zarządzania musi posiadać możliwość uruchomienia skryptów CLI lub pojedynczych komend na wskazanej grupie urządzeń (urządzenia mogą być ręcznie wybierane przez administratora)
66. System zarządzania musi posiadać możliwość uruchomienia skryptu na podstawie zdefiniowanego Alarmu. Alarm musi zapewniać przekazanie wszystkich parametrów z nich związanych w postaci zmiennych dostępnych w skrypcie.
67. System zarządzania musi posiadać możliwość uruchomienia skryptu o określonym czasie lub periodycznie (np. codziennie, co tydzień, co miesiąc) w określonym przedziale czas
68. System zarządzania musi posiadać możliwość uruchomienia skryptu związanego z systemem zarządzania tożsamością – np. pojawienie się nowej niezarejestrowanej w systemie drukarki
69. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów:
	1. Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami firewall takimi jak: Palo Alto, Fortinet, Checkpoint
	2. Musi istnieć możliwość integracji systemu kontroli tożsamości z systemami IPS/IDS i/lub SIEM, które pozwolą na wykrycie zagrożenia i automatyczne przeniesienie urządzenia stanowiącego zagrożenie do wydzielonej sieci kwarantanny
	3. Musi istnieć możliwość integracji systemu kontroli dostępu z systemami MDM – Microsoft Intune, AirWatch MDM
70. System zarządzania musi być objęty 24 miesięcznym wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.
71. **Wymagane prace wdrożeniowe**
72. Wypracowanie z Zamawiającym harmonogramu wdrożenia rozwiązania
73. Instalacja rozwiązania na wskazanym przez Zamawiającego zasobie wirtualnym
74. W oparciu o dobre praktyki Zamawiający wymaga od Wykonawcy przedstawienia zalecanych polityk bezpieczeństwa i konfiguracji wskazanego rozwiązania
75. Wykonawca jest zobowiązany do zidentyfikowania urządzeń końcowych pracujących w sieci Zamawiającego i objęcia ich systemem NAC w ramach dostarczonej licencji
76. Uruchomienie NAC w trybie monitoringu
77. Objęcie systemem NAC aktualnie stosowanych przez Zamawiającego przełączników sieciowych marki Extreme Networks oraz urządzenia UTM marki Fortinet Fortigate
78. Wymagane jest przeprowadzenie testów powdrożeniowych w zakresie wdrożonych polityk i stabilności pracy systemu
79. Wykonawca zobligowany jest do utworzenia i dostarczenia dokumentacji powdrożeniowej Zamawiającemu z wykonanych prac
80. Wymagane jest przeprowadzenie szkolenia zdalnego lub w siedzibie Zamawiającego w liczbie minimum 8h z wdrożonego rozwiązania z zakresu: obsługi interfejsu, administracji, weryfikacji logów zdarzeń oraz tworzenia polityk (szkolenie dla 2 administratorów)
81. Zamawiający przed wykonaniem szkolenia przez Wykonawcę musi zaakceptować ramowy plan szkolenia przedstawiony na minimum 14 dni przed planowanym terminem przeprowadzenia szkolenia
82. W przypadku szkolenia w siedzibie Zamawiającego, Zamawiający zapewnieni odpowiednie warunki do przeprowadzenia szkolenia – dedykowane pomieszczenie i projektor.
83. Wykonawca zobowiązany jest do wystawienia zaświadczenia o odbytym szkoleniu dla każdego uczestnika.