Spis treści

## 1. *Zakres projektu – zamówienia*

Przedmiot zamówienia obejmuje dostawę sprzętu komputerowego, sprzętu do konferencji multimedialnych, licencji na oprogramowanie, w zakresie:

a) Zakup i dostawa sprzętu serwerowego,
b) Zakup i dostawa sprzętu sieciowego,
c) Zakup i dostawa sprzętu obsługi konferencji multimedialnych,
d) Zakup i dostawa sprzętu do archiwizacji dokumentacji medycznej,
e) Zakup i dostawa oprogramowania,

Przedmiot zamówienia należy zrealizować:

a) Zgodnie z wytycznymi Zamawiającego,
b) Z uwzględnieniem terminu realizacji prac, o którym mowa w Rozdziale 3 „Terminy realizacji prac",
c) Z uwzględnieniem warunków gwarancji, o których mowa w Rozdziale 4 „Warunki gwarancji";

Przedmiot zamówienia będzie podlegał procedurom odbioru zgodnie z zapisami Rozdziału 5 „Warunki weryfikacji i odbioru Przedmiotu zamówienia".

## 2. Platforma sprzętowa

### *2.1 Serwer Aplikacyjny – 1 sztuka*

| Element konfiguracji | Wymagania minimalne |
|---|---|
| Obudowa | Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez odłączania urządzenia). Serwer wyposażony w zdejmowany panel przedni umożliwiający montaż zamka chroniącego przed nieuprawionym dostępem do dysków wraz z czujnikiem otwarcia obudowy współpracującym z BIOS. |
| Procesor | Dwa procesory 8-rdzeniowe klasy x86 - 64 bity, osiągające w testach SPECrate2017_fp_base wynik nie gorszy niż 92 punkty w konfiguracji dwuprocesorowej oferowanego modelu serwera. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org<br><br>Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, o mocy maksymalnej 205W i maksymalnym taktowaniu procesora 3.6GHz |
| Liczba możliwych procesorów | Minimum 2 |
| Pamięć operacyjna | Minimum 64 GB RDIMM DDR4 (w kościach po 16GB). Możliwość rozbudowy do minimum 3TB. Minimum 24 sloty na pamięć. |

| | |
|---|---|
| | Zabezpieczenia pamięci: Advanced ECC oraz Online Spare.<br><br>Serwer z obsługą pamięci typu NVDIMM |
| Sloty rozszerzeń | Minimum 3 sloty PCI-Express Generacji 3 w tym minimum dwa sloty x16 (prędkość slotu – bus width) pełnej wysokości oraz minimum jeden slot x8 (prędkość slotu – bus width). |
| Dysk twardy | Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5" i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5" montowane z przodu obudowy oraz możliwość zainstalowania 1 dysku SFF SAS/SATA/SSD, 2,5" z tyłu serwera.<br><br>W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 11 zatok dyskowych SFF gotowych do instalacji dysków SAS/SATA/SSD 2,5" typu Hot Swap.<br><br>Zainstalowane dwa dyski min. 600GB SAS HDD 10k każdy<br><br>Serwer umożliwiający instalacje modułu pamięć flash zapewniających pojemność min. 32GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera. |
| Kontroler | Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.<br><br>Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym.<br><br>Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie. |
| Interfejsy sieciowe | Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń".<br><br>Minimum 2 porty SFP+ 10Gb osiągnięte przez zastosowanie karty nie zajmującej gniazd PCIe opisanych w sekcji „Sloty rozszerzeń" wraz z odpowiednimi wkładkami/modułami producenta serwera.<br><br>Możliwość wymiany na 2 porty obsługujące prędkości 10/40 Gb/s (możliwość konfiguracji pracy z prędkościami 10 i 40Gb/s), przez zastosowanie karty nie zajmującej gniazd PCIe opisanych w sekcji „Sloty rozszerzeń". |
| Karta graficzna | Zintegrowana karta graficzna |
| Porty | 5 x USB 3.0 (w tym 2 porty wewnętrzne)<br><br>1x VGA<br><br>Wewnętrzny slot na kartę micro SD.<br><br>Możliwość rozbudowy o:<br><br>- dodatkowy port typu DisplayPort dostępny z przodu serwera |

| | |
|---|---|
| | - port szeregowy typu DB9/DE-9 (9 pinowy), wyprowadzony bezpośrednio z płyty głównej na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Dla realizacji funkcjonalności nie dopuszcza się stosowania kart PCI-Express |
| Zasilacz | Minimum 2 szt., typ Hot-plug, redundantne, typu Platinium minimum 500W każdy. |
| Chłodzenie | Zestaw wentylatorów redundantnych typu hot-plug<br>Możliwość skonfigurowania serwera do pracy w temperaturze otoczenia równej 45 st. C, tak, żeby zapewnić zgodność ze standardem ASHRAE Class A4 |
| Napęd wewnętrzny | Możliwość instalacji wewnętrznego napędu DVD-ROM lub DVD-RW |
| Diagnostyka | Możliwość instalacji elektronicznego panelu diagnostycznego dostępnego z przodu serwera, pozwalającego uzyskać informacje o stanie: procesora, pamięci, wentylatorów, kary sieciowej, zasilaczy, kartach rozszerzeń, temperaturze. |
| Karta/moduł zarządzający | Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:<br>• monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe<br>• wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP<br>• dostęp do karty zarządzającej poprzez:<br>- dedykowany port RJ45 z tyłu serwera<br>- przez współdzielony port zintegrowanej karty sieciowej serwera<br>dostęp do karty możliwy<br>- z poziomu przeglądarki webowej (GUI)<br>- z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP)<br>- z poziomu skryptu (XML/Perl)<br>- poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface)<br>• wbudowane narzędzia diagnostyczne<br>• zdalna konfiguracji serwera (BIOS) i instalacji systemu operacyjnego<br>• obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie<br>• wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie |

| | |
|---|---|
| | użytkowników<br>• przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough)<br>• obsługa zdalnego serwera logowania<br>• wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i wirtualnych folderów<br>• mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie<br>• funkcja zdalnej konsoli szeregowej przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności<br>• monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji<br>• konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping)<br>• zdalna aktualizacja oprogramowania (firmware)<br>• zarządzanie grupami serwerów, w tym:<br>- tworzenie i konfiguracja grup serwerów<br>- sterowanie zasilaniem (wł/wył)<br>- ograniczenie poboru mocy dla grupy (power caping)<br>- aktualizacja oprogramowania (firmware)<br>- wspólne wirtualne media dla grupy<br>• autentykacja dwuskładnikowa (Kerberos)<br>• wsparcie dla Microsoft Active Directory<br>• obsługa TLS i SSH<br>• enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli<br>• możliwość równoczesnej obsługi przez min. 6 administratorów<br>• wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API<br>• wsparcie dla Integrated Remote Console for Windows clients<br>• możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) |
| Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych | Microsoft Windows Server 2016, 2019<br>Red Hat Enterprise Linux (RHEL) 6.9 oraz 7.3<br>SUSE Linux Enterprise Server (SLES) 11 SP4 oraz 12 SP2<br>ClearOS<br>CentOS |

| | |
|---|---|
| | VMware ESXi 6.0 U3<br><br>VMware ESXi 6.5 oraz U1 |
| Gwarancja/wsparcie techniczne | Minimum 3 lata, w miejscu instalacji z możliwością zgłaszania usterek w trybie 24x7 z czasem reakcji w następnym dniu roboczym (uszkodzony dysk pozostaje u zamawiającego) realizowany przez polski oddział serwisu producenta. Możliwość rozszerzenia usługi gwarancyjnej producenta z gwarantowanym czasem naprawy w ciągu 6 godzin od momentu odebrania zgłoszenia przez serwis |
| Inne | Serwer oraz jego komponenty muszą pochodzić od tego samego producenta, być fabrycznie nowe i wyprodukowane nie wcześniej niż 3 miesiące przed terminem dostawy. Dostarczany sprzęt powinien być zakupiony bezpośrednio u producenta albo w oficjalnym kanale dystrybucyjnym na rynku polskim, razem z odpowiednim pakietem usług gwarancyjnych wymaganych przez Zamawiającego.<br><br>Przeznaczeniem oferowanego sprzętu musi być rynek polski. Zamawiający zastrzega możliwość weryfikacji legalności kanału dostawy u producenta.<br><br>Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.<br><br>Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001.<br><br>Deklaracja zgodności CE. |
| Instalacja i konfiguracja | Wraz z dostawą sprzętu, Wykonawca zapewni instalacje i konfigurację urządzenia w środowisku Zamawiającego |

### *2.2 Macierz – 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Obudowa | Obudowa wolnostojąca, wysokości max. 2U, przystosowana do montażu w szafie rack 19', wraz z szynami montażowymi |
| Procesor | Min. dwurdzeniowy procesor o taktowaniu zegara 2,9 GHz |
| Pamięć RAM | Pamięć RAM 8GB, możliwość rozbudowy do 64GB DDR4 |
| Wnęki na dyski | 12 dysków 3,5"<br>Obsługa dysków hot-plug: 3.5" SATA HDD, 2.5" SATA HDD, 2.5" SATA SSD |
| Dyski | Przestrzeń 24TB zbudowana w oparciu o 6 dysków po 4TB HDD SATA każdy |
| Interfejsy sieciowe | Macierz musi posiadać min. 4 porty Gigabit Ethernet RJ-45 oraz min. 2 porty 10GbE SFP+<br><br>Możliwość instalacji kart z min. 2 interfejsami 10GbE Base-T oraz min. 2 portami Thunderbolt 3 |

| | |
|---|---|
| Poziomy RAID | Pojedynczy dysk, RAID 0, RAID 1 (Disk Mirroring), RAID 5, RAID 5 + hot spare, RAID 6, RAID 10, RAID 50, RAID 60 |
| Złącza | Min. 2 złącza PCIe w tym min. 2 złącza Gen3<br>Min. 4 porty USB 3.0<br>Min. 1 port USB 2.0<br>Min. 1 port HDMI<br>Min. 1 port konsoli |
| Obsługiwane systemy plików | ZFS, EXT2 (Virtual Volume), EXT3 (Virtual Volume), EXT4 (Virtual Volume), FAT (Virtual Volume), NTFS (Virtual Volume) |
| Obsługiwane protokoły | FTP, CIFS, AFP, NFS |
| Usługi | iSCSI Target, Serwer LDAP, DDNS, Serwer plików, Serwer FTP |
| Zarządzanie dyskami | SSD Cache, Auto Tiering, Thin provisioning, Deduplikacja, SSD Trim, Migawki do 4096, SSD Trim, SED (Self Encrytping Disks) |
| Zasilanie | Redundantne zasilacze o mocy min. 250W każdy |
| Wsparcie dla systemów operacyjnych | VMWare 6.7, Microsoft Hyper-V, Citrix 7.0<br>Windows<br>Mac OS X<br>Linux (min. 2.6)<br>UNIX |
| Gwarancja i serwis | Min. 36 miesięcy z możliwością zgłaszania usterek w trybie NBD. |
| Dodatkowe elementy | Kabel - 10GbE SFP+/SFP+ DAC o długości min. 2 m – 2 szt. |
| Instalacja i konfiguracja | Wraz z dostawą sprzętu, Wykonawca zapewni instalacje i konfigurację urządzenia w środowisku Zamawiającego |

### *2.3 Przełącznik – 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Obudowa | Obudowa wolnostojąca, wysokości 1U, przystosowana do montażu w szafie rack 19'.<br>Wbudowane wentylatory<br>Wewnętrzne zasilanie 230V AC o mocy 950W zapewniające budżet mocy PoE na poziomie nie niższym niż 740W. Pobór mocy (bez PoE) nie może być większy niż 80W.<br>Praca w środowisku z temperaturą otoczenia od 0°C do 45°C i wilgotnością od 15% do 95%. |
| Ogólne wymagania funkcjonalne | 1. Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+)<br>2. Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy<br>3. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych<br>4. Dedykowany port konsoli USB |

| | |
|---|---|
| | 5. Port USB 2.0 (niezależny od portu konsoli USB)<br>6. Minimum 8GB pamięci operacyjnej<br>7. Minimum 15GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).<br>8. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)<br>9. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)<br>10. Wydajność: minimum 130 Mp/s<br>11. Bufor pakietów: minimum 7.5 MB<br>12. Wielkość tablicy routingu: minimum 2000 wpisów IPv4, 1000 wpisów IPv6<br>13. Wielkość tablicy ARP co najmniej 8000 wpisów, wielkość tablicy ND co najmniej 8000 wpisów<br>14. Tablica adresów MAC o wielkości minimum 16000 pozycji<br>15. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)<br>16. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 1000 grup), MLD (co najmniej 1000 grup)<br>20. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)<br>21. Wbudowany serwer DHCP<br>22. Obsługa blokowania nieautoryzowanych serwerów DHCP |
| Stackowanie | 1. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Dostępne metody łączenia przełączników muszą umożliwiać realizację stosów na odległość co najmniej 300m.<br>2. Realizacja łączy agregowanych w ramach różnych przełączników będących w stosie |
| Funkcjonalność warstwy L2 | 1. Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN<br>2. Obsługa standardu 802.1v<br>3. Obsługa protokołu MVRP<br>4. Wsparcie dla VXLAN<br>5. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)<br>6. Obsługa Jumbo Frames<br>7. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)<br>8. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego |
| Funkcjonalność warstwy L3 | 1. Obsługa protokołów rutingu: ruting statyczny, OSPF, OSPFv3<br>2. Address Resolution Protocol (ARP) |
| Funkcje QoS | 1. Mechanizmy związane z zapewnieniem jakości usług w sieci: priorytetyzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting |

| | |
|---|---|
| Funkcje bezpieczeństwa | 1. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne<br>2. Obsługa Secure FTP lub SCP<br>3. Obsługa uwierzytelniania użytkowników zgodna z 802.1x<br>4. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS<br>5. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera<br>6. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie<br>7. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+<br>8. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+<br>9. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)<br>10. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Co najmniej 5000 wpisów typu ingress i 2000 wpisów typu egress dla IPv4 i MAC |
| Funkcje zarządzania | 1. Obsługa sFlow lub Netflow<br>2. Obsługa skryptów w języku Python<br>3. Obsługa REST API<br>4. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.<br>5. Obsługa RMON (minimum grupy 1,2,3 i 9)<br>6. Obsługa SNTPv4 lub NTP<br>7. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)<br>8. Wbudowana sonda IP SLA |
| Pozostałe | 1. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania<br>2. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.<br>3. Przełącznik oraz jego komponenty muszą pochodzić od tego samego producenta, być fabrycznie nowe i wyprodukowane nie wcześniej niż 3 miesiące przed terminem dostawy. Dostarczany sprzęt powinien być zakupiony bezpośrednio u producenta albo w oficjalnym kanale dystrybucyjnym na rynku polskim, razem z odpowiednim pakietem usług gwarancyjnych wymaganych przez Zamawiającego.<br><br>Przeznaczeniem oferowanego sprzętu musi być rynek polski. Zamawiający zastrzega możliwość weryfikacji legalności kanału dostawy u producenta.<br><br>Urządzenia i ich komponenty muszą być oznakowane przez producentów w taki |

| | |
|---|---|
| | sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. |
| Gwarancja | 1. Minimum 3 letni serwis producenta obejmujący wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający reakcję w miejscu instalacji maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania urządzenia oraz wsparcia technicznego. Dostępność usługi w trybie 8x5 w godzinach od 8:00 do 17:00. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego. |
| Dodatkowe elementy | 1. Wkładki 10GbE SFP+ 10GBaseSR – 4 sztuki. Wkładki SFP+ muszą być w pełni kompatybilne z przełącznikami opisanymi w tym dokumencie. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników.<br><br>2. Wraz z urządzeniem Wykonawca dostarczy niezbędną do zamawianego sprzętu ilość licencji uprawniającą do korzystania z dedykowanego przez producenta urządzenia oprogramowania do zarządzania środowiskiem sieciowym oraz monitorowania stanu i wydajności wszystkich podłączonych urządzeń w sieci LAN i WLAN. Licencje muszą być bezterminowe. |
| Instalacja i konfiguracja | Wraz z dostawą sprzętu, Wykonawca zapewni instalacje i konfigurację urządzenia w środowisku Zamawiającego. |

### *2.4 UTM – 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Wymagania ogólne | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. 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.<br><br>System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.<br><br>W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 9 administratorów do poszczególnych instancji systemu.<br><br>System musi wspierać IPv4 oraz IPv6 w zakresie: |

| | |
|---|---|
| | • Firewall.<br>• Ochrony w warstwie aplikacji.<br>Protokołów routingu dynamicznego. |
| Redundancja, monitoring, wykrywanie awarii | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.<br>2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.<br>Monitoring stanu realizowanych połączeń VPN. |
| Interfejsy | 1. System realizujący funkcję Firewall musi dysponować minimum:<br>• 10 portami Gigabit Ethernet RJ-45.<br>2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.<br>W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. |
| Dysk | System musi być wyposażony w wbudowany dysk wewnętrzny SSD o pojemności min. 120GB |
| Zasilanie | System musi być wyposażony w zasilanie AC |
| Parametry wydajnościowe: | 1. W zakresie Firewall'a obsługa nie mniej niż 700 000 jednoczesnych połączeń oraz 35 000 nowych połączeń na sekundę.<br>2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.<br>3. Przepustowość Stateful Firewall: nie mniej niż 6 Gbps dla pakietów 64 B.<br>4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.<br>5. Wydajność szyfrowania VPN IPSec dla pakietów 512B, przy zastosowaniu algorytmu o mocy nie mniejszej niż AES256 – SHA256: nie mniej niż 6,5 Gbps.<br>6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,4 Gbps.<br>7. Wydajność skanowania ruchu typu Enterprise Traffic Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 700 Mbps.<br>Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (dla ruchu http – minimum 600 Mbps. |
| Funkcje systemu bezpieczeństwa | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:<br>1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.<br>2. Kontrola Aplikacji.<br>3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.<br>4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.<br>5. Ochrona przed atakami - Intrusion Prevention System.<br>6. Kontrola stron WWW. |

| | |
|---|---|
| | 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.<br>8. Zarządzanie pasmem (QoS, Traffic shaping).<br>9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).<br>10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.<br>Analiza ruchu szyfrowanego protokołem SSL |
| Polityki, Firewall | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.<br>2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:<br>• Translację jeden do jeden oraz jeden do wielu.<br>• Dedykowany ALG (Application Level Gateway) dla protokołu SIP.<br>W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| Połączenia VPN | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:<br>• Wsparcie dla IKE v1 oraz v2.<br>• Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).<br>• Obsługa protokołu Diffie-Hellman group 19 i 20.<br>• Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.<br>• Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.<br>• Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.<br>• Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.<br>• Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.<br>• Mechanizm „Split tunneling" dla połączeń Client-to-Site.<br>2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:<br>• Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.<br>Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta. |
| Routing i obsługa łączy WAN | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:<br>• Routingu statycznego.<br>• Policy Based Routingu.<br>• Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.<br>System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |

| | |
|---|---|
| Zarządzanie pasmem | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.<br>2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.<br>System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| Kontrola Antywirusowa | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).<br>2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.<br>3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.<br>System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). |
| Ochrona przed atakami | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.<br>2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.<br>4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.<br>5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.<br>Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| Kontrola aplikacji | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.<br>2. Baza Kontroli Aplikacji powinna zawierać minimum 2100 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.<br>3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.<br>4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.<br>Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| Kontrola WWW | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.<br>2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.<br>3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.<br>4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia |

| | |
|---|---|
| | wyjątków – białe/czarne listy dla adresów URL.<br>5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.<br>Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
| Uwierzytelnianie użytkowników w ramach sesji | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:<br>• Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.<br>• Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.<br>• Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.<br>2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.<br>Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| Zarządzanie | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.<br>2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.<br>3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego.<br>4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.<br>5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.<br>System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| Logowanie | 1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.<br>2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.<br>3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.<br>Musi istnieć możliwość logowania do serwera SYSLOG. |
| Certyfikaty | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny |

| | |
|---|---|
| | posiadać następujące certyfikacje:<br>• ICSA lub EAL4 dla funkcji Firewall.<br>• ICSA lub NSS Labs dla funkcji IPS.<br>• ICSA dla funkcji IPSec VPN.<br>ICSA dla funkcji SSL VPN. |
| Serwisy i licencje | W ramach zamówienia powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:<br>Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy. |
| Gwarancja i wsparcie | Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 36 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. |
| Usługi | Wraz z dostawą urządzeń wykonawca zapewni usługę instalacji i konfiguracji urządzenia zgodnie z wymogami zamawiającego, ponadto zapewni dla co najmniej jednej osoby min. 2 dniowy, wykonany przez autoryzowane certyfikowane centrum szkoleniowe producenta, instruktaż z zakresu m.in.: logowania i monitoringu, konfiguracji polityk firewalla, translacji adresów sieciowych, lokalnego uwierzytelniania użytkowników, konfiguracji ssl vpn, ipsec vpn, skanowania antywirusowego, filtracji stron www, kontroli aplikacji, zakończony wydaniem certyfikatu producenta urządzenia. |

### *2.5 UPS – 1 sztuka*

| **Nazwa komponentu** | **Wymagane minimalne parametry techniczne komputerów** |
|---|---|
| Typ obudowy | Rack do montażu w szafie 19” maksymalnie 2U |
| Moc pozorna | 3000VA |
| Moc rzeczywista | 2700W |
| Architektura UPS | Line interactive lub on-line |
| Maksymalny czas przełączania na baterię | 4 ms |
| Liczba i rodzaj gniazd wyjściowych | 8x IEC320 C13; 1x IEC320 C19 |
| Typ gniazda wejściowego | 1x IEC320 C20 |
| Porty | 1x USB |

| | |
|---|---|
| Czas podtrzymania dla obciążenia 100% | Min.3 min. |
| Czas podtrzymania dla obciążania 50% | Min. 8 min. |
| Gwarancja | 36 miesięcy w trybie Next Business Day |

### *2.6 Kontroler Sieci Bezprzewodowej– 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Ogólne | 1. Kontroler musi w pełni obsługiwać punkty dostępowe opisane w tym dokumencie<br>2. Kontroler musi zarządzać siecią bezprzewodową złożoną z 10 punktów dostępowych z możliwością rozbudowy do co najmniej 32 punktów dostępowych<br>3. Musi posiadać funkcje pełnostanowej zapory sieciowej (stateful firewall)<br>4. Musi posiadać funkcje VPN Gateway<br>5. Kontroler musi zapewniać możliwość integracji z innymi kontrolerami różnej wielkości (liczba obsługiwanych punktów dostępowych), pracując w systemie hierarchicznym.<br>6. Kontroler musi mieć funkcję pracy w klastrze HA<br>7. Komunikacja pomiędzy kontrolerami musi wykorzystywać protokoły sieciowe niewymagające instalacji dodatkowych urządzeń sieciowych.<br>8. Kontroler musi zapewniać centralne zarządzanie wszystkimi punktami dostępowymi w sieci, łącznie z tworzeniem i zarządzaniem obrazami konfiguracyjnymi oraz aktualizacją oprogramowania<br>9. Kontroler musi zapewniać centralne zarządzenia licencjami, tzn. w architekturze sieci, w której występuję więcej niż jedne kontroler, jeden z kontrolerów musi pełnić funkcję tzw. serwera z licencjami, który automatycznie będzie przydzielał licencję pozostałym kontrolerom. |
| Parametry sieciowe | 1. Możliwość wdrożenia w warstwie 2 i 3 ISO/OSI,<br>2. Wsparcie dla sieci VLAN w tym również trunk 802.1q<br>3. Wbudowany serwer DHCP<br>4. Obsługa SNMPv2, SNMPv3<br>5. Ruting dynamiczny OSPF |
| Funkcje obsługi | 1. Metody szyfrowania i kontroli połączeń: WEP, dynamic WEP, TKIP WPA, WPA2, WPA3, AES-CCMP, EAP, PEAP, TLS, TTLS, LEAP, EAP-FAST, DES, 3DES, AES-CBC<br>2. Obsługę szyfrowania AES-CCM, TKIP i WEP centralnie na kontrolerze<br>3. Obsługę SSL i TLS, RC4 128-bit oraz RSA 1024 i 2048 bit<br>4. Autoryzację dostępu użytkowników:<br>- Typy uwierzytelnienia: IEEE 802.1X (EAP, LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal", 802.1X i MAC<br>- Możliwość wykorzystania nazwy użytkownika, adresu IP, adresu MAC i klucza szyfrowanego do uwierzytelnienia<br>- Wsparcie dla autoryzacji: Microsoft NAP, CISCO NAC, Juniper NAC, Aruba |

| | |
|---|---|
| | NAC<br>- Możliwość utworzenia nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal"<br>- Możliwość wykorzystania mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)<br>- Terminowanie sesji użytkowników sieci bezprzewodowej musi odbywać się na kontrolerze, nie na punkcie dostępowym<br>- Uwierzytelnienie oraz autoryzacja muszą być możliwe przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających. Kontroler musi wspierać co najmniej następujące serwery AAA: Radius, LDAP, SSL Secure LDAP, TACACs+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius.<br>5. Kontroler musi gwarantować automatyczne przełączenie z zewnętrznego serwera AAA na lokalną bazę danych w przypadku awarii serwerów uwierzytelniających.<br>6. Musi istnieć mechanizm definiowania ról użytkowników oraz bazując na nich egzekwowania polityki dostępu<br>7. Kontroler musi zapewniać obsługę XML API do uwierzytelnienia |
| Obsługa transmisji danych | 1. Integracja jednoczesnej transmisji danych i głosu<br>2. Obsługa QoS Voice Flow Classification, SIP, Spectralink SVP, Cisco SCCP, Vocera ALGs, kolejkowanie w powietrzu, obsługa 802.11e-WMM, U-APSD, T-SPEC, SIP authentication tracking, Diff-serv marking, 802.1p<br>3. Musi obsługiwać szybkie przełączanie się klientów pomiędzy punktami dostępowymi (tzw. fast roaming)<br>4. Ograniczanie pasma dla użytkownika oraz dla roli użytkownika<br>5. Ograniczenie pasma dla poszczególnych aplikacji<br>6. Ograniczenie pasma dla poszczególnych kategorii stron internetowych bądź też poziomu zaufania<br>7. Ograniczenie pasma dla poszczególnych SSID |
| Zarządzanie pasmem radiowym | 1. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe<br>2. Stałe monitorowanie pasma oraz usług<br>3. Przełączenie AP w tryb pracy monitorowania sieci bezprzewodowej w przypadku wystąpienie interferencji między kanałowymi<br>4. Rozkład ruchu pomiędzy różnymi punkami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma<br>5. Wykrywanie urządzeń obsługujących MU-MIMO i podłączenie ich do punktów dostępowych obsługujących tą technologię (pracujących w standardzie 802.11ac 2Wave)<br>6. Przełączania użytkowników zdolnych pracować w paśmie 5Ghz do pracy w tymże paśmie<br>7. Zapewnienie sprawiedliwego dostępu do medium w środowisku, w który znajdują się klienci pracujący zgodnie ze standardami (802.11ac, 11n, 11g, 11a, 11b)<br>8. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału<br>9. Wsparcie dla 802.11h, 802.11k, 802.11r, 802.11v, 802.11w<br>10. Integracja z systemami RFID - wymagane jest wbudowane stosowne API |

| | |
|---|---|
| Zapora sieciowa | 1. Inspekcja pakietów z uwzględnieniem reguł bazujących na: użytkownikach, rolach, protokołach i portach, adresacji IP, lokalizacji, czasie dnia<br>2. Mirroring sesji<br>3. Szczegółowe logi (per packet) do późniejszej analizy<br>4. ALG (Application Layer gateway) co najmniej dla protokołów FTP, TFTP, SIP, SCCP, SVP, NOE, RTSP, Vocera, PPTP<br>5. Translacja źródłowa, docelowa adresów IP<br>6. Identyfikacja i blokowanie ataków DoS<br>7. Obsługa protokołu GRE<br>8. Deep packet inspection (DPI)<br>9. Możliwość rozpoznawania oraz tworzenia reguł opartych na aplikacjach których używają klienci wifi |
| Serwer VPN | 1. Site-to-site oraz client-site VPN<br>2. Terminacja ruchu L2TP/IPSEC VPN, XAUTH/IPSEC, PPTP<br>3. Obsługa tokenów<br>4. Wsparcie dla serwerów Radius i LDAP w celu uwierzytelnienia sesji VPN przy użyciu: PAP CHAP, MS-CHAP, MS-CHAP2<br>5. Wsparcie dla algorytmów kryptograficznych: DES, 3DES, AES przy wykorzystaniu dedykowanych układów scalonych kontrolera<br>6. Wsparcie dla dedykowanego klienta VPN (jeżeli konieczne są licencje, nie muszą być zawarte w ofercie) |
| System WIDS/ WIPS | Kontroler musi posiadać funkcję systemu WIDS/ WIPS (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie).<br>Moduł WIPS musi posiadać co najmniej następujące funkcje:<br>1. Detekcja i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP). Automatyczna klasyfikacja obcych urządzeń i możliwość ich blokowania poprzez wysyłanie odpowiednio spreparowanych pakietów.<br>2. Identyfikacja i możliwość blokowania sieci Adhoc<br>3. Identyfikacja anomalii sieciowych, jak wireless bridge czy Windows client bridging<br>4. Ochrona przed atakami sieciowymi na sieć bezprzewodową, m.in. DoS, Management Frame Flood, fake AP, Airjack, ASLEAP, null probe response detection, Netstumbler<br>5. Identyfikacja błędów konfiguracji klientów WLAN<br>6. Identyfikacja podszywania się pod autoryzowane punkty dostępowe |
| Parametry ilościowe/wydajnościowe | 1. Ilość obsługiwanych punktów dostępowych nie mniej niż 32<br>2. Ilość jednocześnie obsługiwanych adresów MAC nie mniej niż 2000<br>3. Ilość aktywnych sesji zapory sieciowej nie mniej niż 32000, przepustowość zapory sieciowej nie mniej niż 4Gbps<br>4. Ilość obsługiwanych BSSID nie mniej niż 1000<br>5. Ilość jednoczesnych tuneli IPSEC nie mniej niż 1000<br>6. Przepustowość ruchu szyfrowanego nie mniejsza niż 2 Gbps dla algorytmu 3DES, 3Gbps dla algorytmu AES-CCM<br>7. Minimum 16 portów 10/100/1000Base-T (w tym minimum 12 portów PoE/PoE+ (budżet mocy minimum 150W)<br>8. Minimum 2 porty 1000BaseX ze stykiem definiowanym przez SFP (dopuszcza się porty typu Combo, współdzielone z portami 10/100/1000BaseT)<br>9. 1 interfejs konsoli (mini USB/RJ-45) |

| | |
|---|---|
| | 10. 1 port USB 2.0<br>11. Zużycie energii nie większe niż 60W (bez PoE |
| Normy | 1. FCC Part 15 Class B<br>2. EN 55022 Class B<br>3. EN 55024<br>4. IEC/EN 60950<br>5. CE Marking<br>6. cTUVus Marked<br>7. CB Scheme Certified |
| Pozostałe funkcjonalności | 1. Kontroler musi umożliwiać integrację ze środowiskiem Microsoft Lync poprzez SDN API.<br>2. Kontroler musi umożliwiać stworzenie strony dla gości tzw. Captive Portal<br>3. Kontroler musi umożliwiać stworzenie dedykowanej strony (interfejsu) do tworzenia kont dostępu do sieci dla gości – strona przeznaczona dla osób nie pracujących w dziale IT (np. dla pracownika recepcji bądź portierni)<br>4. Kontroler musi posiadać funkcję analizatora widma. Włączenie analizatora widma musi być możliwe w zamawianych dwuradiowych punktach dostępowych w trybie pracy wyłącznie jako analizator oraz w trybie hybrydowym, gdzie punkt zarówno analizuje widmo jak i obsługuje ruch użytkowników (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie).<br>5. Kontroler musi mieć możliwość wprowadzenia klasyfikacji treści przeglądanych przez użytkowników stron www (np. przemoc, hazard itp.) oraz określenia ich reputacji. (dopuszcza się możliwość rozbudowy poprzez licencję, która nie jest wymagana na tym etapie, dostęp do bazy treści może być oferowany w formie subskrypcji, o ile dostępna jest ona na co najmniej 10 lat bez konieczności jej odnawiania)<br>6. Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli.<br>7. Kontroler musi zapewniać wsparcie dla protokołów Bonjour, UPnP i DLNA |
| Inne | 1.Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), o ile nie wyspecyfikowano inaczej, nie dopuszcza się licencji czasowych i subskrypcji.<br>2. Wkładki 1GbE SFP 1000BaseSX – 2 sztuki. Wkładki SFP muszą być w pełni kompatybilne z przełącznikami i kontrolerami opisanymi w tym dokumencie. W szczególności muszą być wskazane jako dedykowane w oficjalnych kartach katalogowych przełączników oraz muszą być serwisowane przez serwis producentów przełączników.<br>3. Wraz z urządzeniem Wykonawca dostarczy niezbędną do zamawianego sprzętu ilość licencji uprawniającą do korzystania z dedykowanego przez producenta urządzenia oprogramowania do zarządzania środowiskiem sieciowym oraz monitorowania stanu i wydajności wszystkich podłączonych urządzeń w sieci LAN i WLAN. Licencje muszą być bezterminowe. |
| Gwarancja | 1. Minimum 3 letni serwis producenta obejmujący wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniający reakcję w miejscu instalacji maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania urządzenia oraz wsparcia technicznego. Dostępność usługi w trybie 8x5 w |

| | |
|---|---|
| | godzinach od 8:00 do 17:00. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Aktualizacje oprogramowania i poprawki muszą być dostępne (bezpośrednio od producenta) przez cały czas użytkowania przełącznika, również po wygaśnięciu kontraktu serwisowego. |
| Instalacja i konfiguracja | Wraz z dostawą sprzętu, Wykonawca zapewni instalacje i konfigurację urządzenia w środowisku Zamawiającego. Usługa obejmować ma swym zakresem konfigurację sieci WLAN z wykorzystaniem dostarczanych urządzeń (przełącznik, kontroler, punkty dostępowe, oprogramowanie). |

### *2.7 Punkty Dostępowe– 10 sztuk*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Ogólne | 1. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2/ax oraz 2.4GHz b/g/n<br>2. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej, w szczególności z kontrolerem opisanym w tym dokumencie.<br>3. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj bez nadzoru centralnego kontrolera:<br>- Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https<br>- Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki<br>- Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.<br>4. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:<br>- System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako kontroler główny, a pozostałych punktów dostępowych w klastrze jako kontrolery podrzędne<br>- W przypadku awarii punktu dostępowego pełniącego rolę kontrolera głównego, kolejny punkt dostępowy pracujący w trybie kontrolera podrzędnego i musi przejąć jego rolę w sposób automatyczny, przełączanie takie występuje aż do momentu awarii ostatniego punkt dostępowego pracującego w kastrze<br>- Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe<br>- Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję<br>- Tworzenie klastra do co najmniej 130 urządzeń<br>5. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP<br>6. W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa |

| | |
|---|---|
| | 7. W system musi być wbudowany serwer DHCP<br>8. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów<br>9. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:<br>- EAP-TLS<br>- PEAP-MSCHAPv2<br>- PEAP-GTC<br>- TTLS-MSCHAPv2<br>10. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP<br>11. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID per radio, oraz co najmniej 1000 urządzeń klienckich per radio<br>12. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN<br>13. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:<br>- Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania<br>- Zewnętrzny portal WWW<br>14. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT<br>15. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne<br>16. Minimalizacja interferencji związanych z sieciami 3G/4G LTE<br>17. Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej oraz jako dostęp do konsoli urządzenia<br>18. Obsługa roamingu klientów w warstwie 2<br>19. Obsługa monitoringu przez SNMP<br>22. Obsługa logowania na zewnętrznym serwerze SYSLOG<br>23. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci |
| Zarządzanie pasmem radiowym | 1. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:<br>- Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe<br>- Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu<br>- Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma<br>- Wykrywanie interferencji oraz miejsc bez pokrycia sygnału<br>- Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz<br>- Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac wave 2 oraz starszych (802.11b/g) |

| | |
|---|---|
| | - Wsparcie dla 802.11d oraz 802.11h<br>- Możliwość stworzenia profili czasowych w których dane SSID ma być rozgłaszane |
| Interfejs zarządzania | 1. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:<br>- Widok diagnostyczny prezentujący problemy z sygnałem/prędkością<br>- Wykorzystanie pasma<br>- Ilość klientów korzystających z systemu/interferujących<br>- Ilość ramek wejściowych/wyjściowych dla każdego radia<br>- Ilość odrzuconych/błędnych ramek/s dla każdego radia<br>- Szum tła dla każdego radia<br>- Wyświetlanie logów systemowych |
| Anteny | 1. Punkt dostępowy musi wbudowane anteny dookólne do pracy w trybie 4x4: MU-MIMO. Uzyska anten nie powinien być mniejszy niż<br>- 3,5 dBi dla 2,4 GHz<br>- 5,4 dBi dla 5 Ghz |
| Obsługa standardów | 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2, 802.11ax |
| Specyfika standardów | - 802.11b: DSSS<br>- 802.11a/g/n/ac: OFDM<br>- 802.11ax: OFDMA z 37 RU przy kanale 80 MHz |
| Specyfika modulacji | - 802.11b: BPSK, QPSK, CCK<br>- 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM<br>- 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM , 1024-QAM<br>- 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM , 1024-QAM |
| Specyfikacja szerokości kanałów pracy | - 802.11n high-throughput (HT) wspiera MT20/40<br>- 802.11ac very high-throughput (VHT) wspiera VHT20/40/80/160<br>- 802.11ax high efficiency (HE) wspiera HE20/40/80/160 |
| Obsługiwane częstotliwości | - 5.150 ~ 5.250 GHz (low band)<br>- 5.250 ~ 5.350 GHz (mid band)<br>- 5.470 ~ 5.725 GHz (Europa)<br>- 5.725 ~ 5.850 GHz (high band) |
| Wspierane prędkości przesyłania danych (Mbps) | - 802.11b: 1,2,5.5,11<br>- 802.11a/g 6,9,12,18,24,36,48,54<br>- 802.11n: od 6.5 do 600 (MCS0 do MCS31, HT20 do HT40) do 800 z 256-QAM<br>- 802.11ac: od 6.5 do 1733 (MCS0 do MCS9, NSS= 1 do 4, VHT20 do VHT160) 2166 z 1024-QAM<br>- 802.11ax (2,4 GHz) od 3.6 2402 (MCS0 do MCS11, NSS=1 do 4, HE20 do HE40)<br>- 802.11ax (5GHz) 3.5 do 2402 (MCS0 do MCS11, NSS = 1 do 4, HE20 do HE160) |
| Moc transmisji | Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm<br>1. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz<br>2. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac<br>3. Wsparcie dla: |

| | |
|---|---|
| | - MRC (Maximal ratio combining)<br>- CDD/CSD (Cyclic delay/shift diversity)<br>- STBC (Space-time block coding)<br>- LDPC (Low-density parity check)<br>- Technologia TxBF<br>- TWT (Target Wait Time) |
| Parametry ilościowe/wydajnościowe | 1. 2 interfejsy 100/1000/2500/5000 Base-T<br>- z funkcją PoE 802.3at/bt<br>- zgodny ze standardem 802.3az Energy Effcient Ethernet EEE<br>2. 1 interfejs konsoli szeregowej (micro USB)<br>3. Zasilanie PoE zgodne z 802.3af/802.3.at<br>- maksymalny pobór mocy 26.4 W PoE<br>- możliwość za pomocą obydwu portów Ethernet z możliwością agregacji mocy (zasilanie na obydwu portach 802.3at jest równoznaczne z zasianiem 802.bt na jednym)<br>4. przycisk przywracający konfigurację fabryczną<br>5. Kontrolka LED do określania statusu systemu i interfejsów radiowych<br>6. slot zabezpieczający Keningston<br>7. Zigbee (802.15.4)<br>8. Bluetooth 5.0 Low Energy (BLE5.0)<br>9. USB 2.0 (host) (Type A)<br>10. Port zasilania DC 48Vdc |
| Parametry pracy | 1.Temperatura otoczenia: 0°C- +50°C<br>2. Wilgotność 5% - 93% nie skondensowana<br>3.Znak CE<br>4.EN 300 019 |
| Certyfikaty | 1.Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac wave 2/ ax |
| Pozostałe | 1.Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni<br>2. Wraz z urządzeniem Wykonawca dostarczy niezbędną do zamawianego sprzętu ilość licencji uprawniającą do korzystania z dedykowanego przez producenta urządzenia oprogramowania do zarządzania środowiskiem sieciowym oraz monitorowania stanu i wydajności wszystkich podłączonych urządzeń w sieci LAN i WLAN. Licencje muszą być bezterminowe. |
| Gwarancja | 1.Minimum 3 letnia gwarancja producenta obejmująca wszystkie elementy urządzenia zapewniająca dostawę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. |
| Instalacja i konfiguracja | Wraz z dostawą sprzętu, Wykonawca zapewni instalacje i konfigurację urządzenia w środowisku Zamawiającego. Usługa obejmować ma swym zakresem, fizyczny montaż punktów dostępowych, konfigurację sieci WLAN z |

| | |
|---|---|
| | wykorzystaniem dostarczanych urządzeń (przełącznik, kontroler, punkty dostępowe, oprogramowanie). |

### *2.8 Rzutnik– 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Technologia wyświetlania | DLP |
| Rozdzielczość natywna | 1920 x 1080 (FHD) |
| Rozdzielczość maksymalna | 1920 x 1200 (WUXGA) |
| Format obrazu | 4:3<br>16:9<br>16:10 |
| Jasność | 4500 lm |
| Kontrast | 10 000:1 |
| Wielkość rzutowanego obrazu | 60" - 180" |
| Żywotność lampy | 2 500 h (tryb normalny)<br>3 500 h (tryb ekonomiczny) |
| Moc lampy | 310 W |
| Złącza | Wejście audio - 1 szt.<br>Wyjście audio - 1 szt.<br>Wejście mikrofonowe - 1 szt.<br>Wejście audio L/R (RCA) - 1 szt.<br>Composite video (RCA) - 1 szt.<br>HDMI - 1 szt.<br>HDMI/MHL - 1 szt.<br>VGA in (D-sub) - 1 szt.<br>VGA out (D-sub) - 1 szt.<br>S-Video - 1 szt.<br>RJ-45 (LAN) - 1 szt. |

| | |
|---|---|
| | USB 2.0 (zasilanie) - 1 szt.<br>Mini USB - 1 szt.<br>RS-232 - 1 szt.<br>AC in (wejście zasilania) - 1 szt. |
| 3D Ready | Tak |
| Łączność bezprzewodowa | Nie |
| Moc rzeczywista | 2700W |
| Gwarancja | Minimum 36 miesiące |

### *2.9 Uchwyt Sufitowy Rzutnika – 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Typ | Sufitowy |
| Kolor | Biały |
| Maksymalne obciążenie | 15 kg |
| Obrót | 90° |
| Pochylenie | +/-15° |
| Wysokość | 450 - 760 mm |
| Szerokość | 50 - 200 mm |
| Głębokość | 50 - 200 mm |
| Gwarancja | Minimum 36 miesiące |

### *2.10 Zestaw do wideokonferencji – 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| **Kamera** | |
| Rozdzielczość kamery | FULL HD 1080p /60fps |
| Zoom | 12 x zoom optyczny |
| Kąt widzenia | 72,5 ° |
| Focus | Auto |
| Wymagania | Półka do montażu kamery na ścianie |

| | |
|---|---|
| dodatkowe | |
| **Zestaw Głośnomówiący** | |
| Technologia dźwięku | Full HD (A2DP), full duplex, automatyczna eliminacja echa i tłumienie hałasu |
| Mikrofon | Dookolny 360 °, zbieranie głosu od 12 osób, |
| Częstotliwość | 100 – 24000 Hz |
| Wyświetlacz | Kolorowy<br>Dotykowy<br>Rozdzielczość 240 x 320 pixeli |
| **HUB** | |
| Wyposażenie | Kabel 5m USB (typ A/ typ B) do podłączenia kamery z HUBem<br>Kabel 3m USB (typ A/ typ B) do podłączenia HUBa z komputerem<br>Zasilacz<br>Kabel do zasilacza<br>Pilot |
| Interfejsy | 1 x USB 3.0<br>1 x USB 2.0<br>1 x HDMI |
| Gwarancja | 36 miesięcy |

### *2.11 Skaner – 1 sztuka*

| **Element konfiguracji** | **Wymagania minimalne** |
|---|---|
| Rodzaj urządzenia | Skaner dokumentów - desktop |
| Typ interfejsu | USB 2.0 |
| Rozmiar maksymalny nośnika | 304.8 x 4064 mm |
| Typ wejścia | Kolor |
| Skala szarości (zewnętrzna) | 8 bitów (256 odcieni szarości) |
| Głębia koloru | Kolor 48-bitowy |
| Głębia koloru | 24-bit (16,7 miliona kolorów) |

| | |
|---|---|
| (zewnętrzna) | |
| Rozdzielczość optyczna | 600 dpi x 600 dpi |
| Rozdzielczość interpolowana | 1200 dpi x 1200 dpi |
| Automatyczny dupleks | Tak |
| Typ Czujnika Skanowania | Dual CCD |
| Rodzaj źródła światła / lampa | Dual LED |
| Szybkość maksymalna skanowania dokumentu czarno-białego / w kolorze | 50 stron/min / 50 stron/min |
| Cykl pracy | 15000 skanów/dzień |
| Szybkość skanowania - szczegóły | 50 stron/min - poziomo biało-czarny - Letter - 300 dpi<br>100 cali/min - dupleks - poziomo biało-czarny - Letter - 300 dpi<br>50 stron/min - poziomo skala szarości - Letter - 300 dpi<br>100 cali/min - dupleks - poziomo skala szarości - Letter - 300 dpi<br>50 stron/min - poziomo kolor - Letter - 300 dpi<br>100 cali/min - dupleks - poziomo kolor - Letter - 300 dpi |
| Cechy skanera | Color Dropout,<br>Ultrasonic Double Feed Detection,<br>Automatic Image Orientation,<br>Automatyczne wykrywanie kolorów,<br>Auto Crop, i Thresholding, Perfect Page,<br>Skanowanie dwustrumieniowe,<br>Ekran dotykowy LCD,<br>Adaptacyjne przetwarzanie progowe,<br>Image merge,<br>Automatyczne ustawienie jaskrawości,<br>Deskew,<br>Blank Page Detection |
| Rodzaj podajnika nośników | Automatyczny |
| Pojemność podajnika | 250 arkusze |
| Dodatkowe wymagania | Zasilacz - Adapter zasilania zewnętrznego |
| Wymagany system operacyjny | Microsoft Windows Vista (32/64 bits) SP2,<br>Ubuntu 10.04,<br>Microsoft Windows 7 (32/64 bits) SP1, |

| | |
|---|---|
| | Microsoft Windows XP (32/64 bits) SP3,<br>Windows 8 (32/64 bits),<br>Windows 10 (64 bits) |

### *2.12 Licencje dostępowe - 12 sztuk*

Licencja dostępowa dla urządzenia umożliwiająca podłączenie i wykorzystywanie wszystkich dostępnych funkcjonalności posiadanego przez Zamawiającego serwera usługi katalogowej (Windows Server Std 2016)
Dostarczone licencje muszą być kompatybilne z obecnie posiadanymi licencjami oraz pozwalać na założenie i obsługę wskazanej liczby kont usługi katalogowej.
Dostarczone przez Wykonawcę licencje muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia Zamawiający nie dopuszcza dostawy licencji typu OEM.
Zamawiający oczekuje dostawy licencji nieograniczonych czasowo.
Licencja musi zapewniać możliwość korzystania z wcześniejszych wersji zamawianego oprogramowania.

### *2.13 Serwerowy system operacyjny - 2 sztuki*

Licencja na oprogramowanie musi zostać dostarczona dla odpowiedniej ilości rdzeni fizycznych dla obydwu procesorów serwerów aplikacyjnych będących w posiadaniu zamawiającego.
Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i minimum dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
Licencja musi uprawniać do instalacji starszych wersji oferowanego serwerowego systemu operacyjnego. Serwerowy system operacyjny (SSO) musi posiadać następujące, wbudowane cechy:
· Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 1 TB pamięci RAM w środowisku fizycznym
· Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
Wbudowane wsparcie instalacji i pracy na wolumenach, które:
· pozwalają na zmianę rozmiaru w czasie pracy systemu,
· umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
· umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, o umożliwiają zdefiniowanie listkontroli dostępu (ACL).
· Mają wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
· umożliwiają uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
· umożliwiają dystrybucję ruchu sieciowego HTTP pomiędzy kilka serwerów.
· Mają wbudowaną zaporę internetową (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
Graficzny interfejs użytkownika.
Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 4 języków poprzez wybór z listy dostępnych lokalizacji w tym język polski.

Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów(oprogramowania) innych producentów wymagających dodatkowych licencji:
· Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
· Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: - Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, - Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, - Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. o Zdalna dystrybucja oprogramowania na stacje robocze.
Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
· Serwis udostępniania stron WWW.
· Wsparcie dla protokołu IP w wersji 6 (IPv6),

### *2.14 Pakiet Biurowy - 12 sztuki*

Pakiet biurowy Microsoft Office 2019 dla Użytkowników Domowych i Małych Firm 64Bit PL BOX zawierający min. Word, Excel, Power Point i program pocztowy z licencją nieograniczoną czasowo wraz z unikatowym kluczem do aktywacji każdego dostarczonego pakietu lub inny równoważny zintegrowany pakiet biurowy. Przy czym, równoważność będzie oceniana w zakresie posiadania przez zaproponowane oprogramowanie, oprócz istotnych zbliżonych cech i parametrów do produktu referencyjnego, które muszą umożliwiać pełną obsługę wszystkich istniejących dokumentów, wytworzonych przy użyciu oprogramowania Microsoft Office: 2003, 2007, 2010, 2013, 2016, 2019 (pliki tekstowe, dokumenty, arkusze kalkulacyjne zawierające makra i formularze, prezentacje itp.) bez utraty jakichkolwiek ich parametrów i cech użytkowych, również następujących szczegółowych funkcjonalności:

- dla edytora tekstu MS Word 2019:
    a. podział okna roboczego na kilka dokumentów,
    b. edytor rysunków,
    c. wykonywanie korespondencji seryjnej bazującej na danych adresowych pochodzących np. z arkusza kalkulacyjnego,
    d. wstawianie tabel i wykresów z arkusza kalkulacyjnego, w tym tabel przestawnych,
    e. otwieranie plików PDF i edytowanie ich zawartości.

- dla arkusza kalkulacyjnego MS Excel 2019:
    a. ustawianie obszaru wydruku,
    b. ręczne rysowanie obramowania,
    c. automatyczne dopasowanie wielkości komórek do zawartości,
    d. obsługa makr,
    e. obsługa co najmniej 2 tys. kolumn,
    f. nagrywanie, tworzenie i edycję makr automatyzujących wykonywane czynności,
    g. tworzenie wykresów linowych (wraz z linią trendu), słupkowych, kołowych,

- dla programu do prezentacji MS Power Point 2019:

a. możliwość ustawiania dowolnego rozmiaru slajdu w centymetrach lub pikselach,

b. prowadzenie prezentacji w trybie prezentera.

## 3. Termin realizacji pracy

Wymagane terminy realizacji Przedmiotu zamówienia:

1. Przedmiot zamówienia należy zrealizować w terminie 21 - 45 dni od daty zawarcia umowy.
2. Dostawę sprzętu i oprogramowania należy zrealizować w godzinach pracy Zamawiającego, od poniedziałku do piątku (z wyjątkiem dni ustawowo wolnych od pracy)

## 4. Warunki gwarancji

1. Okres gwarancji liczony będzie od daty podpisania przez Zamawiającego Protokołu Odbioru Przedmiotu Zamówienia.
2. Gwarancja świadczona będzie w siedzibie Zamawiającego (nie dotyczy sprzętu wymienionego w Rozdziale 2 – Projektor multimedialny, skaner, telewizor, zestaw do konferencji multimedialnych).
3. Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
4. Zamawiający ma prawo do dokonywania rozbudowy sprzętu, zgodnie z dokumentacją techniczną, przez wykwalifikowanych pracowników, bez utraty gwarancji. Wykonawca nie ponosi odpowiedzialności za uszkodzenia mechaniczne powstałe z winy Zamawiającego.
5. Na oprogramowanie, Wykonawca udziela gwarancji na zasadach określonych standardowo przez producenta oprogramowania w odpowiednich kartach gwarancyjnych.

## 5. Warunki odbioru przedmiotu zamówienia

1. Sprzęt komputerowy i oprogramowanie dostarczone przez Wykonawcę i przekazane do odbioru będzie poddawane weryfikacji zgodnie z poniższą procedurą:
    a. Wykonawca zobowiązany jest przed przeprowadzeniem dostawy Przedmiotu zamówienia powiadomić (pisemnie lub drogą mailową) Zamawiającego o planowanej dostawie całości lub części na co najmniej 3 dni robocze przed jej przeprowadzeniem
    b. Wykonawca zobowiązany jest przeprowadzić dostawę Przedmiotu zamówienia w Godzinach pracy Zamawiającego i w miejscu uzgodnionym z Zamawiającym
    c. Wykonawca przygotuje Przedmiot zamówienia w sposób umożliwiający jego weryfikację

d. po dostarczeniu przez Wykonawcę Przedmiotu zamówienia podpisywany jest przez Strony protokół odbioru ilościowego, stwierdzający faktyczną ilość sztuk dostarczonego sprzętu i oprogramowania;
e. Zamawiający w ciągu 5 dni roboczych od podpisania protokołu odbioru ilościowego zweryfikuje czy dostarczony Przedmiot zamówienia jest zgodny z OPZ oraz złożoną ofertą;
f. w przypadku nie zgłoszenia przez upoważnionych przedstawicieli Zamawiającego uwag do odbieranego Przedmiotu zamówienia, podpisywany jest Protokół Odbioru Przedmiotu Zamówienia;
g. w przypadku jakichkolwiek uwag do odbieranego Przedmiotu zamówienia Zamawiający ma prawo odmówić dokonania odbioru. W takim przypadku Wykonawca będzie zobowiązany do dostarczenia niewadliwego Przedmiotu zamówienia w terminie nie dłuższym niż 3 dni robocze (z uwzględnieniem terminu

2. Protokół Odbioru Przedmiotu Zamówienia, zawierać będzie w szczególności: 1)wykaz dostarczonego sprzętu oraz oprogramowania wraz z numerami seryjnymi; 2)datę odbioru ilościowego danego sprzętu i/lub oprogramowania.
3. Realizacja Przedmiotu zamówienia zostanie uznana za zakończoną po zatwierdzeniu Protokołu Odbioru Przedmiotu Zamówienia przez uprawnioną osobę Zamawiającego.