Opis Przedmiotu Zamówienia

na "modernizację i rozbudowę infrastruktury urządzeń aktywnych sieci LAN, SAN oraz infrastruktury macierzowej wraz z systemami bezpieczeństwa w Urzędzie Miasta Płocka"

Przedmiot zamówienia dotyczy modernizacji i rozbudowy części infrastruktury teletechnicznej w Urzędzie Miasta Płocka funkcjonującej w sieci wewnętrznej LAN i SAN. Są to:

- urządzenia aktywne sieci LAN – przełączniki core w wersji redundantnej i przełączniki accesowe, wraz z pełnym okablowaniem,
- urządzenia aktywne sieci SAN – przełączniki, karty Host Bus Adapter fibre channel, macierze dyskowe wraz z pełnym okablowaniem,
- system kontroli dostępu do sieci (NAC),
- system zarządzania urządzeniami sieciowymi.
- wkładki SFP+ do przełączników LAN
- półki dyskowe do serwerów NAS
- przedłużenie wsparcia gwarancyjnego o 3 lata na urządzenia UTM

W zakres modernizacji wchodzi:

- dostawa nowych urządzeń i licencji oprogramowania,
- wymiana wyeksploatowanych aktywnych urządzeń sieciowych na nowe i przeniesienie obecnej konfiguracji / funkcjonalności,
- montaż i wdrożenie nowego klastra macierzy dyskowych wraz z podłączeniem do serwerów i konfiguracją.

Zadanie ma na celu podniesienie standardu funkcjonowania sieci wewnętrznej LAN m.in. po przez podniesienie przepustowości sieci szkieletowej z 1 Gb/s do 10 i 40 Gb/s oraz wymianę wyeksploatowanych i niewspieranych urządzeń aktywnych, a tym samym podniesienie bezpieczeństwa teleinformatycznego Urzędu Miasta Płocka. Rozbudowa farmy serwerów o sieć SAN i macierze zwiększy wydajność, skalowalność systemów wirtualnych oraz ochronę danych

Sprzęt który podlega wymianie:

1. przełącznik modularny 3com 8800 (2 x switch 48p 1 x fiber optic switch 24p) - 2 szt
2. przełącznik 3com 5500 52 portowy - 12 szt
3. przełącznik 3com 5500 28 portowy - 10 szt
4. przełącznik cisco WS-C2960G-48TC-L - 4 szt

Dostawa nowego sprzętu i licencji oprogramowania:

- **Wykonawca winien przedstawić w formularzu oferty oferowany sprzęt i licencje oprogramowania (przedstawić nazwę producenta wraz z kompletnym zestawieniem numerów katalogowych produktów i wszystkich jego dodatkowych składników umożliwiających ich jednoznaczną identyfikację u producenta sprzętu jak i oprogramowania)**
- **Wszystkie opisane wymagane parametry są wymaganiami minimalnymi. Zamawiający akceptuje rozwiązania o parametrach równoważnych lub lepszych, bez utraty funkcjonalności i wydajności (równoważne tj. spełniające wszystkie minimalne wymagania specyfikacji technicznej).**
- **Oferowane produkty muszą spełniać wszystkie parametry określone w niniejszym załączniku oraz być fabrycznie nowe, pochodzić z legalnego źródła**

I. PRZEŁĄCZNIK LAN MODULARNY CORE – 2 szt

Ogólne:

- Oferowane produkty muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski.

Wymagania minimalne:

- Przełącznik o budowie modularnej pozwalającej na instalację minimum 288 portów gigabitowych, 96 portów 10-gigabitowych SFP+, 96 portów miedzianych 1/2,5/5/10-gigabitowych z negocjacją prędkości oraz obsługą standardu PoE+, 24 porty 40-gigabitowych lub ich kombinacji.
- Przełącznik musi posiadać redundantne moduły zarządzające wyposażone w minimum 1GB pamięci stałej (typu Flash) oraz minimum 4GB pamięci operacyjnej (typu RAM) na każdym z modułów.
- Przełącznik wyposażony w:
  - minimum 48 portów 100BaseTX/1000BaseT,
  - minimum 24 porty gigabitowe SFP,
  - minimum 24 porty 1/10-gigabitowymi SFP+. Dla zapewnienia redundancji porty SFP+ muszą być rozdzielone na co najmniej dwa różne moduły,
  - minimum 2 porty 40Gb QSPF+ lub QSFP28,
  - minimum 8 portów miedzianych 1/2,5/5/10-gigabitowe 10GBaseT z negocjacją prędkości oraz obsługą standardu 802.3at (PoE+)
- Redundantne, wewnętrzne, modularne, zasilacze wspierające standard 802.3at (PoE+) zapewniające minimum 500W dla PoE oraz zapewniające redundancję zasilania i budżetu mocy w trybie N+N.
- Wolne sloty umożliwiające dalszą rozbudowę do zadanej minimalnej liczby portów.
- Modularną wentylację (zapewniające redundancję wentylatory umieszczone na dedykowanym module).
- Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych.
- Obsługa ramek typu Jumbo.
- Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 2 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.
- Obsługa sFlow oraz RMON (minimum grupy 1,2,3 i 9).
- Automatyczne wykrywanie przeplotu (AutoMDIX) na portach 100/1000BaseT.
- Obsługa 4094 tagów IEEE 802.1Q oraz 4094 jednoczesnych sieci VLAN.
- Obsługa standardu IEEE 802.1v.
- Wsparcie dla VxLAN.
- Dostęp do urządzenia przez konsolę szeregową (RS-232 i USB), HTTPS, SSHv2 i SNMPv3.
- Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s).
- Obsługa Secure FTP.
- Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP).
- Obsługa Simple Network Time Protocol (SNTP) v4.
- Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping).
- Obsługa protokołów rutingu: ruting statyczny, RIP v1, RIP v2, OSPF, OSPFv3, VRRP, PIM-SM, PIM-DM, BGP.
- Obsługa 802.1ad (Q-in-Q).
- Wielkość tablicy rutingu: minimum 10000 wpisów IPv4 i 5000 wpisów IPv6.
- Wielkość tablicy MAC: minimum 60000 wpisów.
- Prędkość matrycy przełączającej nie mniejsza niż 2000 Gb/s.
- Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED).

- Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED) oraz CDPv2.
- Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting.
- Obsługa uwierzytelniania użytkowników zgodna z 802.1x.
- Obsługa uwierzytelniania użytkowników w oparciu o lokalną bazę adresów MAC.
- Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS.
- Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW.
- Obsługa różnych metod uwierzytelniania (802.1x, MAC, WWW) w tym samym czasie na tym samym porcie.
- Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie.
- Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+.
- Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+.
- Wbudowany serwer DHCP.
- Obsługa funkcji User Datagram Protocol (UDP) helper.
- Obsługa blokowania nieautoryzowanych serwerów DHCP.
- Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection).
- Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP.
- Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link Detection Protocol (DLDP) lub równoważnego.
- Obsługa protokołu OpenFlow w wersji co najmniej 1.0 i 1.3.
- OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
- Musi być możliwe wielotablicowe przetwarzanie zapytań Open Flow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP).
- Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
- Obsługa standardu 802.3az Energy Efficient Ethernet.
- Obsługa standardu 802.1AE MACsec.
- Obsługa ochrony procesora.
- Obudowa maksymalnie 7U umożliwiająca instalację w szafie 19" o głębokości nie większej niż 46 cm.
- Minimalny zakres pracy od 0°C do 45°C

Gwarancja:

- 5 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę 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. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.
- 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.

II. PRZEŁĄCZNIK LAN (typ 1) – 28 szt

Ogólne:

- Oferowane produkty muszą być dostarczone przez autoryzowany kanał sprzedaży

producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski.

Parametry minimalne:

- Minimum 48 portów gigabitowych w standardzie 100/1000BaseT.
- Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
- Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika).
- Wydajność: minimum 112 Mp/s.
- Tablica adresów MAC o wielkości minimum 32000 pozycji.
- Obsługa ramek Jumbo.
- Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów).
- Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów).
- Wielkość sprzętowej tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6.
- Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping.
- Obsługa VxLAN.
- Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol.
- Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN.
- Funkcja Root Guard oraz BPDU protection.
- 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. Przełączniki muszą łączyć się we wspólne stosy z przełącznikami typu 2 opisanymi w punkcie III.
- Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie.
- Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping.
- Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.
- Obsługa standardu 802.1p – min. 8 kolejek na porcie.
- Funkcja mirroringu portów.
- Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED).
- Funkcja autoryzacji użytkowników zgodna z 802.1x.
- Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+.
- RADIUS Accounting.
- Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3.
- OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
- Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP).
- Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow.
- Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
- Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az.

- Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
- Obsługa Syslog.
- Obsługa NTP lub SNTPv4.
- Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku.
- Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej.
- Wsparcie dla funkcji Private VLAN lub równoważnego.
- Obsługa protokołu VTP lub MVRP.
- Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego.
- Minimalny zakres pracy od 0°C do 45°C.
- Wysokość w szafie 19" – 1U, głębokość nie większa niż 30 cm.
- 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.
- Do urządzenia należy dołączyć patchcordy UTP unshielded RJ45 kat.6A (24 szt 2 mb + 24 szt 3 mb)

Gwarancja:

- 5 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.

III. PRZEŁĄCZNIK LAN (typ 2) – 13 szt

Ogólne:

- Oferowane produkty muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski.

Wymagania minimalne:

- Minimum 48 portów gigabitowych w standardzie 100/1000BaseT ze wsparciem dla standardu 802.3at (PoE+).
- Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).
- Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika).
- Wydajność: minimum 112 Mp/s.
- Tablica adresów MAC o wielkości minimum 32000 pozycji.
- Obsługa ramek Jumbo.
- Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów).
- Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów).
- Wielkość sprzętowej tablicy rutingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6.
- Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping.
- Obsługa VxLAN.

- Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol.
- Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN.
- Funkcja Root Guard oraz BPDU protection.
- 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. Przełączniki muszą łączyć się we wspólne stosy z przełącznikami typu 1 opisanymi w punkcie II.
- Automatyczne wykrywanie punktów bezprzewodowych podłączonych do przełącznika (co najmniej punktów opisanych w tym postępowaniu), automatyczne konfigurowanie portów, do których są one podłączone (minimum sieć VLAN, CoS, budżet mocy PoE, priorytet PoE).
- Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie.
- Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping.
- Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI.
- Obsługa standardu 802.1p – min. 8 kolejek na porcie.
- Funkcja mirroringu portów.
- Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED).
- Funkcja autoryzacji użytkowników zgodna z 802.1x.
- Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+.
- RADIUS Accounting.
- Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3.
- OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic.
- Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP).
- Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow.
- Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az.
- Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https.
- Obsługa Syslog.
- Obsługa NTP lub SNTPv4.
- Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku.
- Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej.
- Wsparcie dla funkcji Private VLAN lub równoważnego.
- Obsługa protokołu VTP lub MVRP.
- Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego.
- Minimalny zakres pracy od 0°C do 45°C.
- Wysokość w szafie 19” – 1U, głębokość nie większa niż 50 cm.
- Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W.
- 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.
- Do urządzenia należy dołączyć patchcordy UTP unshielded RJ45 kat.6A (24 szt 2 mb + 24 szt 3 mb)

Gwarancja:

- 5 letnia gwarancja (serwis) producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę 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. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis.

IV. PRZEŁĄCZNIK LAN (typ 3) – 80 szt

Wymagania minimalne:

- Klasa przełącznika: zarządzalny.
- Warstwa przełączania: L3.
- Architektura sieci – 10BASE-T, 100BASE-TX, 1000BASE-T.
- Liczba portów 10/100/1000 Mbps: 8 szt.
- Tryb przekazywania: Store-and-forward.
- Przepustowość: 6 Gbps.
- Prędkość przekazywania: 11.9 Mpps.
- Rozmiar tablicy adresów MAC: 8000.
- Obsługa ramek Jumbo.
- Obsługa sieci VLAN.
- Obsługiwane protokoły i standardy
  - IEEE 802.1d
  - IEEE 802.1q
  - IEEE 802.1s
  - IEEE 802.1w
  - IEEE 802.3
  - IEEE 802.3ab
  - IEEE 802.3ad
  - IEEE 802.3x
  - LLDP-MED
- Zarządzanie, monitorowanie, konfiguracja:
  - HTTP
  - HTTPS
  - RMON
  - SNMP v1
  - SNMP v2c
  - SNMP v3
- Zasilanie: PoE +

Gwarancja:

- Co najmniej ograniczona dożywotnia gwarancja producenta tj. gwarancja przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

V. BEZPRZEWODOWY PUNKT DOSTĘPOWY (AP) – 20 szt

Wymagania minimalne:

- 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 oraz 2.4GHz b/g/n.
- Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej.
- Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera:
  - Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https.
  - Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki.
  - 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.
- Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:
  - System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego.
  - W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny.
  - Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe.
  - Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję.
  - Tworzenie klastra do 130 urządzeń.
- Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.
- Punkt dostępowy musi mieć możliwość pracy jako analizator widma.
- W system operacyjny musi być wbudowana pełnostanowa zapora sieciowa.
- W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.
- Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
  - EAP-TLS,
  - PEAP-MSCHAPv2,
  - PEAP-GTC,
  - TTLS-MSCHAPv2.
- Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP.
- Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID.
- Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
- Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
  - Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania,
  - Zewnętrzny portal WWW.
- Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
- Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne.
- Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
  - Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe,

    - Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu,
    - Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma,
    - Wykrywanie interferencji oraz miejsc bez pokrycia sygnału,
    - Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz,
    - Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac oraz starszych (802.11b/g),
    - Wsparcie dla 802.11d oraz 802.11h,
    - Możliwość stworzenia profili czasowych w których dane ssid ma być rozgłaszane.
- Minimalizacja interferencji związanych z sieciami 3G/4G LTE.
- Punkt dostępowy musi mieć wbudowany moduł Bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej.
- Obsługa roamingu klientów w warstwie 2.
- Obsługa monitoringu przez SNMP.
- Obsługa logowania na zewnętrznym serwerze SYSLOG.
- W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
- Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
    - Widok diagnostyczny prezentujący problemy z sygnałem/prędkością,
    - Wykorzystanie pasma,
    - Ilość klientów korzystających z systemu/interferujących,
    - Ilość ramek wejściowych/wyjściowych dla każdego radia,
    - Ilość odrzuconych/błędnych ramek/s dla każdego radia,
    - Szum tła dla każdego radia,
    - Wyświetlanie logów systemowych.
- Punkt dostępowy musi posiadać 2 dwu zakresowe wbudowane anteny do pracy w trybie 2x2:2 MU-MIMO, o zysku co najmniej 3,3 dBi dla 2,4 Ghz oraz co najmniej 5,8 dBI dla 5 GHz. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2.
- Praca w trybie MIMO 2X2:2.
- specyfikacja radia 802.11a/n/ac wave 2.
    - Obsługiwana technologia OFDM.
    - Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM.
    - Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm.
    - Prędkości transmisji:
        - 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a,
        - MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11n,
        - MCS0-MCS9, NSS = 1-4(6.5 Mbps do 867 Mbps) dla 802.11ac,
    - Obsługa HT – kanały 20/40MHz dla 802.11n.
    - Obsługa VHT – kanały 20/40/80MHz dla 802.11ac.
    - Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz.
    - Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac.
    - Wsparcie dla:
        - MRC (Maximal ratio combining),
        - CDD/CSD (Cyclic delay/shift diversity),
        - STBC (Space-time block coding),
        - LDPC (Low-density parity check),
        - Technologia TxBF.
- specyfikacja radia 802.11b/g/n:
    - Częstotliwość 2,400 ~2,4835,
    - Technologia direct sequence spread spectrum (DSSS), OFDM,
    - Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM,
    - Moc transmisji konfigurowalna przez administratora,
    - Prędkości transmisji:
        - 1,2,5.5,11 Mbps dla 802.11b,
        - 6,9,12,18,24,36,48,54 Mbps dla 802.11g,

- Punkt dostępowy musi posiadać co najmniej
  - 1 interfejs 10/100/1000 Base-T
    - z funkcją PoE,
    - zgodny ze standardem 802.3az Energy Effcient Ethernet.
  - 1 interfejs konsoli RS-232/USB.
  - Moduł Bluetooth Low Energy (BLE) radio .
  - zasilanie 12V AC oraz PoE 48V DC zgodne z 802.3af
    - maksymalny pobór mocy 12W przy zasilaniu PoE,
    - maksymalny pobór mocy 9W przy zasilaniu DC.
  - przycisk przywracający konfigurację fabryczną.
  - slot zabezpieczający Keningston.
- Parametry pracy urządzenia:
  - Temperatura otoczenia: 0-40 °C,
  - Wilgotność 5% - 92%,
  - Znak CE,
  - UL/IEC/EN 60950,
  - EN 60601-1-1, EN60601-1-2,
  - MTBF minimum 90 lat przy temperaturze 25 C.
- Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac wave2.
- Wszystkie dostępne na urządzeniu funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
- Punkt dostępowy musi zostać dostarczony z elementami montażowymi niezbędnymi do montażu na płaskiej powierzchni.

Gwarancja:

- Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancją producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 10 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

VI. SYSTEM KONTROLI DOSTĘPU DO SIECI (NAC)

Wymagania minimalne:

System do kontroli dostępu musi charakteryzować się następującymi cechami:
- Musi być systemem współpracującym z urządzeniami wielu producentów (tzw. multi vendor).
- System musi odsługiwać minimum 1500 urządzeń klienckich (w tym gości). Licencje mają dotyczyć aktualnie podłączonych urządzeń i ma być zwalniania po rozłączeniu urządzenia.
- Praca jako maszyna wirtualna.
- Musi posiadać wbudowany serwer Radius oraz TACACS +
- Musi wspierać RADIUS VSA co najmniej 100 producentów, w tym:
  - Cisco Systems,
  - Fortinet,
  - Microsoft,
  - Alcatel-lucent Enterprise,
  - Aruba Networks,
  - Huawei,
  - Extreme Networks,
  - PaloAlto,
  - Producenta urządzeń sieciowych opisanych w tym postępowaniu

- System musi posiadać możliwość przesyłania atrybutów VSA do kontrolera sieci bezprzewodowej takich jak rola użytkownika oraz VLAN bez potrzeby dokonywania dodatkowej konfiguracji kontrolera.
- System musi posiadać możliwość otrzymywania od kontrolera sieci bezprzewodowej dodatkowych informacji o autoryzacji użytkownika między innymi takich jak SSID, grupa punktów dostępowych, IP punktu dostępowego.
- Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.
- Musi posiadać wbudowaną bazę użytkowników oraz móc integrować się z następującymi bazami danych:
  - Microsoft Active Directory,
  - Radius,
  - Kerberos,
  - Ldap,
  - ODBC,
  - Współpraca z serwerami tokenów.
- Musi obsługiwać metody profilowania:
  - DHCP,
  - TCP,
  - MAC OUI,
  - SNMP,
  - Cisco device sensor.
- Wspierać protokoły:
  - Radius, Radius CoA, TACACS +, web authentication, SAML v2.0,
  - EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS),
  - PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP-PWD),
  - TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP),
  - EAP-TLS,
  - PAP, CHAP, MSCHAPv1 i v2, EAP-MD5,
  - NAC, Microsoft NAP,
  - Windows machine authentication,
  - MAC Auth,
  - Audit (role oparte na porcie oraz skanowanie podatności),
  - OCSP (Online Certificate Status Protocol),
  - SNMP generic MIB, SNMP private MIB,
  - CEF (Common Event Format), LEEF (Log Event Extended Format),
  - TLS 1.2.
- Funkcja integracji z systemem monitorowania sieci w celu ułatwienia diagnozowania problemów z klientami.
- Maszyna wirtualna musi mieć możliwość uruchomienia na platformach:
  - Co najmniej ESX 4.0, ESXi 4.1 do 6.0,
  - Co najmniej Hyper-V 2012 R2 oraz Windows 2012 R2 enterprise.

Posiadać moduł odpowiedzialny za Dostęp Gościnny. Obsługa użytkowników typu Gość w liczbie co najmniej równej minimalnej liczbie obsługiwanych urządzeń klienckich (1500). Jeżeli moduł ten wymaga dodatkowych licencji, muszą być one zawarte.

System obsługi ruchu gościnnego musi spełniać poniższe funkcjonalności:
- Samodzielna rejestracja klientów gościnnych w oparciu o:
  - Adres e-mail,
  - Numer telefonu (wiadomość SMS),
  - Dostęp sponsorowany (gość musi podać adres e-mail pracownika, na który jest wysłana prośba o autoryzację dostępu poprzez kliknięcie w znajdujący się w wiadomości link).
- Logowanie w oparciu o portale społecznościowe.
- Funkcja integracji z systemami trzecimi poprzez API.
- Wsparcie dla tworzenia komercyjnych systemów HOT-SPOT wykorzystujących do

płatności systemy płatności kartą kredytową.
- Wspieranie rozwiązań mobilnych poprzez automatyczne skalowanie portalu gościnnego do rozmiarów urządzeń mobilnych.
- Funkcja personalizacji strony gościnnej

Posiadać moduł odpowiedzialny za obsługę urządzeń typu BYOD. Dopuszcza się rozbudowę poprzez dokupienie odpowiedniej licencji.

- Konfiguracja urządzeń ma odbywać się bez potrzeby angażowania pracowników działo IT.
- System musi wspierać obsługę następujących systemów operacyjnych:
  - MS Windows,
  - Mac OS X,
  - iOS,
  - Android,
  - Ubuntu.
- Umożliwienie klientowi samo rejestracji oraz bezpiecznego skonfigurowania urządzenia do pracy w sieci.
- Automatyczna konfiguracja urządzeń do pracy w sieci przewodowej jak i bezprzewodowej.
- Użycie profilowania do identyfikacji rodzaju urządzenia, producenta oraz modelu.
- Funkcja tworzenia unikalnych certyfikatów dla urządzeń.
- Wbudowane CA na potrzeby generowania certyfikatów konfigurowanych urządzeń.
- Funkcja konfiguracji urządzeń bezprzewodowych w oparciu o jedną lub dwie sieci SSID.

Posiadać moduł odpowiedzialny za kontrolę końcówek klienckich. Licencja pozwalająca na obsługę co najmniej 1500 końcówek klienckich.

System kontroli końcówek klienckich musi mieć następujące funkcjonalności:
- System musi wspierać następujące systemy operacyjne:
  - Microsoft Windows 7 i nowsze (może być uruchomiony jako serwis),
  - Apple Mac OS X 10.7 i nowsze,
  - Red HAT Enterprise Linux 4 i nowsze,
  - CentOS 4 (Community Enterprise Operating System) i nowsze,
  - Fedora Core 5 i nowsze,
  - SUSE linux 10.x i nowsze.
- Funkcja kontroli stanu oprogramowania anty-wirusowego, anty-spyware, firewall.
- Wyświetlanie informacji on-line o statusie monitorowanych końcówek.
- System powinien obsługiwać agenta w formie:
  - Stałej (Presistent Agent),
  - Tymczasowej (Dissolvabe Agent),
  - Agenta NAP.

Do rozwiązania musi być dostępna publicznie, na stronie producenta, dokumentacja techniczna opisująca wdrożenie i użytkowanie systemu. Wszystkie wymagane funkcje muszą być dostępne w chwili składania oferty i udokumentowane (opisane w dokumentacji lub możliwe do sprawdzenia na wersji ewaluacyjnej systemu) (nie dopuszcza się scenariusza, w którym jakieś elementy są zaplanowane do realizacji w przyszłości). Zamawiający zastrzega sobie prawo do weryfikacji spełnienia wymagań.

- Testy
  - Zamawiający wymaga przeprowadzenia testów wybranych funkcji sprzętu i oprogramowania wymaganych w ramach tego postępowania. Testy potwierdzające działania wymaganych funkcji muszą zostać przeprowadzone w siedzibie Zamawiającego w terminie nie dłużysz niż 5 dni roboczych od chwili dostarczenia i wdrożenia sprzętu.

Gwarancja:

- Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

VII. SYSTEM ZARZĄDZANIA URZĄDZENIAMI SIECIOWYMI – MINIMUM 100 LICENCJI DOSTĘPOWYCH

Wymagania minimalne:

- System musi być zbudowany w architekturze klient – serwer.
- System musi być zbudowany modułowo, tak aby możliwe było doinstalowanie modułów dających dodatkową funkcjonalność, minimalnie:
  - Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA,
  - Zarządzanie siecią bezprzewodową WLAN,
  - Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetSream v5 oraz analizy zawartości pakietów SMTP, FTP, http,
  - Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS,
  - Zarządzanie dostępem zdalnym Ipsec/VPN,
  - Wbudowany serwer TACACS,
  - Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników,
  - Funkcja monitorowania wydajności aplikacji.
- System musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru Systemu.
- Licencja na System musi umożliwiać zarządzanie wszystkimi urządzeniami sieciowymi różnych producentów.
- System musi posiadać funkcje umożliwiać automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet.
- System musi posiadać funkcje monitorowania stanu urządzeń po protokole SNMP i wyświetlania informacji co najmniej o:
  - Średnim wykorzystaniu CPU i pamięci RAM,
  - Średnim czasie odpowiedzi urządzenia,
  - Obciążeniu interfejsów (dla ruchu wchodzącego i wychodzącego),
  - Ilość błędnych lub odrzuconych pakietów na interfejsie.
- System musi posiadać funkcje konfiguracji urządzeń po protokole SNMP i SSH.
- System musi posiadać funkcje zarządzania konfiguracją urządzeń, tworzenia backup'ów (ręcznie oraz automatycznie w określonych odstępach czasu) oraz grupowego implementowania konfiguracji na zarządzane urządzenia. System musi zachowywać historię tworzenia backup'ów wraz z informacją czy przebiegł on pomyślnie, a w przypadku, jeżeli nie, powinien także poinformować o przyczynie niepowodzenia.
- System musi pozwalać na tworzenie szablonów konfiguracji co najmniej w oparciu o cały plik konfiguracyjny, fragment konfiguracji, skrypt CLI, skrypt TCL.
- System musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń, w tym możliwość przechowywania kilku wersji oprogramowania dla jednego modelu urządzenia, możliwość importowania obrazu z komputera do Systemu (tzw. Offline), możliwość pobrania obrazu do Systemu bezpośrednio z Internetu (tzw. Online/LiveUpdate).
- System musi pozwalać na globalne zarządzanie VLAN, tzn. na tworzenie, modyfikowanie oraz usuwanie VLAN jednocześnie ze wszystkich lub wybranych przełączników zarządzanych przez System. Musi istnieć także możliwość automatycznego generowania map logicznej topologii sieci obrazującej konkretny VLAN

a zarządzanych urządzeniach.
- System musi posiadać funkcję zarządzania listami kontroli dostępu (ACL), w tym: możliwość importowania ACL z urządzeń i tworzenie na ich podstawie szablonu, tworzenie ACL w systemie zarządzania, możliwość pojedynczej lub grupowej.
- System musi posiadać możliwość wyświetlania zbiorczej tablicy routingu zbudowanej w oparciu o tablice zarządzanych urządzeń.
- System musi posiadać zcentralizowany mechanizm przeglądania zdarzeń w sieci, tzw. Dashboard (skonsolidowany, syslog, trapy snmp, zdarzenia i alarmy).
- System musi generować alarmy na podstawie takich parametrów jak: wykorzystanie CPU, wykorzystanie RAM, temperatura urządzenia, obciążenie interfejsów fizycznych na wejściu i wyjściu, ilość odrzuconych pakietów; Muszą być dostępne co najmniej dwa poziomy alarmu dla pojedynczego parametru oraz muszą być one możliwe do zmiany.
- System musi posiadać funkcje wysyłania alarmów np. e-mailem lub SMS'em wraz z możliwością konfiguracji konkretnego zakresu czasowego i dnia tygodnia, w którym wiadomości będą wysyłane.
- System musi pozwalać na budowanie widoków przez administratora.
- System musi posiadać funkcje generowania raportów (co najmniej w formatach PDF, CSV, Excel, XLSX, Docx) w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta. Generowanie raportów musi się odbywać na życzenie (on demand) i w regularnych odstępach czasowych (scheduled, np. codziennie, raz w tygodniu, raz na kwartał itp.).
- System musi posiadać narzędzia graficznej prezentacji topologii sieciowej wraz z dynamiczną prezentacją zmian stanu urządzeń oraz poziomem występujących na nich alarmów. Musi być też możliwość zmiany ikony reprezentującej urządzenie na topologii sieci wraz z możliwością wykorzystania różnych ikon dla różnych poziomów alarmów na urządzeniu.
- System musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji sprzętu używanego w sieci.
- System musi posiadać funkcje lokalizowania użytkowników przewodowych po adresie IP lub MAC. Wynikiem musi być wskazanie konkretnego portu zarządzanego urządzenia sieciowego, do którego podłączony jest użytkownik.
- System musi posiadać funkcję powiązywania konkretnego interfejsu fizycznego zarządzanego urządzenia z adresem MAC urządzenia końcowego, które będzie miało dostęp do sieci tylko na tym interfejsie. Po wykryciu nieautoryzowanej próby połączenia musi być możliwość wygenerowania alarmu, wyłączenia interfejsu po określonym czasie od zaistnienia zdarzenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund) oraz ponownego włączenia interfejsu po określonym czasie od wyłączenia (wartość konfigurowalna minimum w zakresie 10-1800 sekund).
- System musi posiadać predefiniowaną bazę zakresów adresów MAC dla urządzeń sieciowych oraz biurowych wiodących producentów. Baza musi być zbudowana co najmniej dla takich producentów jak: Cisco, Epson, Toshiba, NEC, Nortel, Canon, Sony, Samsung, 3Com, Siemens, Nokia, Apple, Lexmark, Xerox, Avaya, D-Link, LG, Dell, Alcatel, Netgear, HPE, TP-Link, Ruckus oraz Huawei. Musi istnieć możliwość ręcznego dodania wpisu do tej bazy.
- System musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie.
- System musi posiadać funkcje tworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym, w tym:
    - Wykrywanie ataków między innymi takich jak: Duplicate ARP Address, ICMP Flood, TCP Port Scan, WinNuke, IP Spoofing, ICMP Redirect, Source Route, SYN Flood, UDP Port Scan, UDP Flood, Ping of Death, DHCP Server Detect,
    - Stworzenie topologii obrazującej logiczne połączenia między urządzeniami objętymi jednym lub kilkoma atakami sieciowymi, tzn. pokazuje urządzenie/urządzenia będące źródłem ataku i łączy je z urządzeniem/urządzeniami będącymi celem ataku,
    - Stworzenie topologii obrazującej fizyczne połączenie między urządzeniami objętymi pojedynczym atakiem sieciowym, tzn. pokazuje całą ścieżkę fizyczną między źródłem, a celem ataku.

- System musi posiadać funkcję Telnet/SSH oraz GUI proxy umożliwiającą zarządzanie CLI/Web przez przeglądarkę Internetową.
- System musi posiadać funkcje zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android.
- System musi posiada funkcje dostępu do sytemu zarządzania realizowaną przez przeglądarkę internetową (min. Chrome i Firefox).
- System musi posiadać funkcje zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, e-mail.
- System musi posiadać funkcje tworzenia kont administratorskich z różnymi poziomami uprawnień oraz z możliwością przypisywania administratorów do grup urządzeń. Dodatkowo musi być możliwość stworzenia kont jedynie z uprawnieniami do podglądu – bez możliwości dokonywania zmian w systemie ani na urządzenia.
- System musi posiadać funkcję zarządzania VXLAN – tworzenie listy urządzeń wspierających VXLAN, tworzenie tuneli, tworzenie topologii sieci VXLAN, wyświetlanie informacji o statystykach ruchu w tunelach.
- System musi posiadać funkcje zarządzania siecią wirtualną poprzez integrację z VMware (minimum wersja 6.0) i Microsoft Hyper-V(minimum w wersji 2012). Między innymi musi pozwalać na:
  - Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem VMware ESX z wykorzystaniem protokołu SOAP,
  - Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Virtual Machine Manager z wykorzystaniem Windows PowerShell,
  - Uzyskanie bezpiecznego dostępu zdalnego do zarządzania serwerem Microsoft Hyper-V z wykorzystaniem protokołu WMI,
  - Zarządzanie siecią wirtualną, w tym serwerami VMware vCenter Server oraz Microsoft Virtual Machine Manager, wirtualnymi maszynami oraz wirtualnymi przełącznikami,
  - Przedstawienie wszystkich zasobów, szczegółowych informacji o nich oraz ich wzajemnych relacji w środowisku wirtualnym. Wymaga się, aby był wgląd minimum w:
    - Listę wszystkich fizycznych serwerów VMware ESX oraz Microsoft Hyper-V dostępnych w sieci. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: producent, model, nazwa serwera, adres IP, informacje na temat Managera sieci wirtualnej, ilość pamięci RAM (wraz z poziomem wykorzystania), CPU (wraz z poziomem wykorzystania) oraz informację czy dany serwer wspiera funkcję migracji maszyn wirtualnych,
    - Listę wirtualnych przełączników przyporządkowanych do konkretnych serwerów VMware ESX oraz Microsoft Hyper-V. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa przełącznika, ilość wirtualnych portów,
    - Listę wirtualnych maszyn przyporządkowanych do konkretnych przełączników wirtualnych. Dodatkowo wymaga się, aby dla każdego fizycznego serwera była możliwość wyświetlenia informacji takich jak: nazwa wirtualnej maszyny, adres IP, stan maszyny (Running, Stopped, Suspended).
  - Zmianę stanu (minimum: Start VM, Stop VM, Suspend VM, Reset VM) i parametrów wirtualnej maszyny takich jak: zasoby CPU, ilość pamięci RAM, ilość przestrzeni dyskowej,
  - Dodawanie, klonowanie i usuwanie wirtualnych masz,
  - Kreowanie szablonów służących do tworzenia nowych wirtualnych maszyn, gdzie można zdefiniować parametry początkowe takie jak: nazwę VMware ESX/Microsoft Hyper-V, zasoby CPU, ilość pamięci RAM, przestrzeń dyskową, system operacyjny wirtualnej maszyny,
  - Dodawanie wirtualnych przełączników wraz z możliwością wyboru konkretnych kart sieciowych fizycznego serwera, do których będzie połączony wirtualny przełącznik. Dodatkowo musi istnieć możliwość „load balancingu" pomiędzy kartami sieciowymi co najmniej w oparciu o: IP hash, MAC hash, port fizyczny ruchu przychodzącego.

Musi być także możliwość ustawienia kart sieciowych w trybie Active-Standby.
- System musi posiadać funkcje zarządzania co najmniej dla 1000 predefiniowanych modeli urządzeń. Oprócz tego musi być możliwość wgrania dowolnej bazy MIB dla urządzeń sieciowych nie obsługiwanych domyślnie przez System.
- System musi posiadać funkcję automatycznej aktualizacji przez Internet.
- System musi posiadać funkcje implementacji rozproszonej, wykorzystując różne serwery do instalacji swoich komponentów.
- System musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled).
- System musi pozwalać na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy.
- Wszystkie wymagane licencje muszą działać permanentnie (dożywotnio), nie dopuszcza się licencji czasowych.

Gwarancja:

- Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

VIII. PRZEŁĄCZNIK SAN FC – 4 szt

Ogólne:

- Oferowane produkty muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski.

Wymagania minimalne:

- Przełącznik FC musi być wykonany w technologii FC minimum 32 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 32, 16, 8, 4 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.
- W przypadku obsadzenia portu FC za pomocą wkładki SFP 32Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 32, 16 lub 8 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.
- W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.
- Przełącznik FC musi być wyposażony, w co najmniej 16 aktywnych portów FC obsadzonych wkładkami SFP 16Gb/s z możliwością rozbudowy do 24 portów za pomocą odpowiedniej licencji i dodatkowych wkładek optycznych.
- Wszystkie zaoferowane porty przełącznika FC muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 16Gb/s lub 32Gb/s w zależności od zastosowanych wkładek FC.
- Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji (24 porty) wyposażonej we wkładki 32Gb/s musi wynosić minimum 768 Gb/s end-to-end.
- Oczekiwana wartość opóźnienia przy przesyłaniu ramek FC między dowolnymi portami przełącznika nie może być większa niż 900ns.
- Rodzaj obsługiwanych portów, co najmniej: E, D oraz F.
- Przełącznik FC musi mieć wysokość maksymalnie 1 U (jednostka wysokości szafy

montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.

- Przełącznik FC musi być wyposażony w mechanizm agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu ISL Trunk o przepustowości minimum 256 Gb/s half duplex (dla wkładek 32Gbps) dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postepowania.
- Przełącznik FC musi wspierać mechanizm balansowania ruchu, pomiędzy co najmniej 16 różnymi ścieżkami o tym samym koszcie wewnątrz wielodomenowych sieci fabric, przy czym balansowanie ruchu musi odbywać się w oparciu o 3 parametry nagłówka ramki FC: DID, SID i OXID.
- Przełącznik FC musi zapewniać jednoczesną obsługę mechanizmów ISL Trunk oraz balansowania ruchu w oparciu o DID/SID/OXID. Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postepowania.
- Przełącznik FC musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.
- Przełącznik FC musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:
  - mechanizm tzw. Fabric Binding, który umożliwia zdefiniowanie listy kontroli dostępu regulującej prawa przełączników FC do uczestnictwa w sieci fabric,
  - uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP,
  - uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP,
  - szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2, ◦ definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control),
  - definiowane kont administratorów w środowisku RADIUS, LDAP w MS Active Directory, Open LDAP, TACACS+,
  - szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS,
  - obsługa SNMP v1 oraz v3,
  - IP Filter dla portu administracyjnego przełącznika,
  - wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP,
  - wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP.
- Przełącznik FC musi mieć możliwość konfiguracji przez:
  - polecenia tekstowe w interfejsie znakowym konsoli terminala,
  - przeglądarkę internetową z interfejsem graficznym lub dedykowane oprogramowanie.
- Przełącznik FC musi być wyposażony w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:
  - logowanie zdarzeń poprzez mechanizm „syslog”,
  - ciągłe monitorowanie parametrów pracy przełącznika, portów, wkładek SFP i sieci fabric z automatycznym powiadamianiem administratora, wyłączeniem pracy portu lub przesunięciem przepływów tzw. slow drain na niski priorytet w przypadku przekroczenia zdefiniowanych wartości granicznych. Powiadamianie administrator musi być możliwe za pomocą wysyłania wiadomości e-mail, pułapki SNMP lub komunikatu w logu. Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postepowania.
  - port diagnostyczny tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających komunikację portu przełącznika z wkładką SFP, połączenie optyczne pomiędzy dwoma przełącznikami, testowe obciążenie połączenia pełną przepustowością 16Gbps/32Gbps oraz pomiar opóźnienia i odległości między

przełącznikami z dokładnością co najmniej do 5m dla wkładek SFP 16Gbps lub 32Gbps. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric,
    - Fcping,
    - FC traceroute,
    - kopiowanie danych wymienianych pomiędzy dwoma wybranymi portami na inny wybrany port przełącznika,
    - Przełącznik musi być wyposażony w mechanizm sprzętowego monitorowania przepływów danych dla wskazanych jak i automatycznie wykrywanych par urządzeń komunikujących się przez dany port przełącznika. Dla każdego monitorowanego przepływu muszą być gromadzone statystyki dotyczące, co najmniej liczby wysłanych i odebranych ramek, przepustowości, liczby zapisów i odczytów SCSI, przy czym musi istnieć możliwość zawężenia zakresu monitorowania do następujących typów ramek: SCSI Reserve, SCSI Aborts, SCSI Read, SCSI Write, rejected frames. Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postepowania.
    - Przełącznik musi być wyposażony w mechanizm sprzętowego generatora ruchu umożliwiającego symulowanie komunikacji w wielodomenowych sieciach SAN bez konieczności angażowania fizycznych urządzeń takich jak serwery lub macierze dyskowe. Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postepowania.
    - Przełącznik musi być wyposażony w mechanizm umożliwiający kopiowanie pierwszych 64 bajtów ramek dla wybranych przepływów danych do pamięci lokalnej przełącznika w celu dalszej analizy,
    - Przełącznik musi być wyposażony w mechanizm umożliwiający sprzętowe identyfikowanie ramek FC oznaczonych parametrem VM ID oraz integrację tego mechanizmu z systemami monitorowania przepływów danych w szczególności w zakresie przepustowości oraz liczby zapisów i odczytów na sekundę.
- Po zainstalowaniu dodatkowej licencji przełącznik FC musi zapewnić możliwość przydzielenia, co najmniej 1700 tzw. buffer credits do pojedynczego portu FC przełącznika. Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postępowania.
- Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet.
- Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.
- Przełącznik FC musi realizować kategoryzację ruchu między parami urządzeń (initiator - target) oraz przydzielenie takich par urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi się odbywać za pomocą standardowych narzędzi do konfiguracji zoningu.
- Przełącznik FC musi realizować kategoryzację ruchu na podstawie wartości parametru CS_CTL w nagłówku ramki FC oraz odpowiednie przydzielenie ramki do kategorii o wysokim, średnim lub niskim priorytecie.
- Wsparcie dla N_Port ID Virtualization (NPIV). Obsługa, co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.

Gwarancja:

- Minimum 3 letnia gwarancja (serwis) producenta.

IX. MACIERZ DYSKOWA – 2 szt

Ogólne:

- Oferowane produkty muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski.

Wymagania minimalne:

Techniczne:

- Obudowa - gęstość upakowania:
  - Możliwość zainstalowania w standardowej szafie RACK 19",
  - Wysokość dostarczanej macierzy nie może być większa niż 2U,
  - Urządzenie musi wspierać półki dyskowe 2U obsługujące co najmniej 24 dyski 2,5" lub 12 dysków 3.5”,
  - Urządzenie musi wspierać półki dyskowe wysokiej gęstości obsługujące co najmniej 90 dysków na maksymalnej wysokości 5U.
- Zarządzanie:
  - Urządzenie musi umożliwiać zarządzanie za pomocą interfejsu Ethernet,
  - Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej,
  - Funkcjonalność bezpośredniego monitoringu stanu w jakim w danym momencie znajduje się macierz,
  - Interfejs zarządzający GUI, CLI, oraz zapewnienie możliwości tworzenie skryptów użytkownika.
- Ilość portów:
  - Minimum 4 porty Ethernet 10Gb/s BaseT,
  - Minimum 8 portów Fibre Channel 16Gb/s w pełni obsadzone modułami 16 Gb/s.
- Obsługa dysków:
  - Macierz musi być wyposażona w minimum 24 dyski SSD o pojemności 3.84TB,
  - Macierz musi obsługiwać dyski:
    - SAS 2,5” o pojemności minimum: 2.4 TB i prędkości 10k rpm,
    - NLSAS 2,5” o pojemności minimum : 2 TB i prędkości 7.2k rpm,
    - SAS 3,5” o pojemności minimum: 2.4 TB i prędkości 10k rpm (dopuszczalna jest instalacja dysków 2.5” w obudowach 3.5”),
    - NL SAS 3,5” o pojemności minimum: 14 TB i prędkości 7.2k rpm,
    - SSD 2,5” o pojemności minimum: 30 TB.
  - Macierz musi mieć możliwość rozbudowy do co najmniej 500 dysków 2,5" na parę kontrolerów z zastosowaniem dodatkowych półek bez potrzeby wymiany zainstalowanych komponentów.
  - Musi umożliwiać konfigurację, która w jednym rozwiązaniu łączyć będzie półki rozszerzeń na dyski 2,5" z półkami na dyski 3,5".
  - Macierz musi obsługiwać poziomy RAID 0,1,10 oraz umożliwiać stworzenie rozproszonego / wirtualnego systemu RAID 5 i 6.
  - Macierz musi zapewnić możliwość wymiany uszkodzonych dysków podczas pracy systemu (Hot-Swap).
- Obsługa pamięci Cache:
  - Macierz musi być wyposażona w minimum 64 GB pamięci cache przeznaczonej dla danych (sumarycznie dla obu kontrolerów). Macierz musi posiadać funkcjonalność Cache dla procesu odczytu oraz Mirrored Cache dla procesu zapisu.
  - Macierz musi umożliwiać rozbudowę pamięci cache do 128GB w ramach klastra macierzy zarządzanego z jednego interfejsu GUI, CLI.
- Wsparcie dla systemów operacyjnych (co najmniej):
  - Microsoft Windows Server 2012 R2, 2016, 2019,
  - Vmware vSphere 6.5, 6.7, 7.0,
  - Hyper-V 2012 R2, 2016, 2019,
  - Red Hat Enterprise Linux 7, 8,
  - SUSE Linux Enterprise Server 15,
  - HP-UX 11iv3, IBM i 7.4

Dodatkowe wymagania i funkcjonalności:

- Funkcje niezawodnościowe:
  - Wszystkie krytyczne komponenty urządzenia takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu.
  - Komponenty te muszą być wymienialne w trakcie pracy macierzy.
  - Urządzenie musi cechować brak pojedynczego punktu awarii.
  - Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu Hot-Swap. Wentylatory typu Hot-Swap. Wbudowane co najmniej dwa kontrolery RAID. Urządzenie musi posiadać pamięć typu Flash dla zapisu danych z pamięci cache na wypadek zaniku zasilania oraz system podtrzymania zasilania pozwalający na zapis danych z cache do pamięci typu Flash.
- Funkcjonalności:
  - Musi istnieć funkcjonalność Cache dla procesu odczytu.
  - Musi istnieć funkcjonalność Mirrored Cache dla procesu zapisu.
  - Możliwość wyłączenia cache dla poszczególnych wolumenów.
  - Funkcjonalność dynamicznego zwiększania i zmniejszania rozmiaru wolumenów.
  - Funkcjonalność zarządzania ilością operacji wejścia / wyjścia wykonywanych na danym wolumenie - zarządzanie musi być możliwe zarówno poprzez określenie ilości operacji l/O na sekundę jak również przepustowości określonej w MB/s.
  - Urządzenie musi obsługiwać funkcjonalność ochrony przed skasowaniem lub odmapowaniem od hosta woluminu dyskowego, do którego były przestane operacje wejścia/wyjścia w żądanym przez użytkownika czasie.
  - Macierz musi wspierać dostęp wieloma ścieżkami do zasobów dyskowych poprzez dedykowane sterowniki dostarczane przez producenta macierzy lub poprzez natywne sterowniki MPIO systemów operacyjnych.
- Obsługa wirtualnych dysków logicznych:
  - Minimalna ilość wspieranych wirtualnych dysków logicznych (LUN) dla całej (globalnej) puli dyskowej musi wynosić co najmniej 2000. Funkcjonalność LUN Masking i LUN Mapping.
  - Macierz musi posiadać funkcjonalność tworzenia mirrorowanych LUN pomiędzy różnymi zasobami dyskowymi, dla których awaria jednej kopii lustra musi być niezauważalna dla systemu hosta.
- Funkcjonalność thin provisioning:
  - Urządzenie musi obsługiwać funkcjonalność thin provisioning dla wszystkich wolumenów. Musi istnieć możliwość wyłączenia tej funkcjonalności dla wybranych wolumenów. Jeżeli funkcjonalność wymaga dodatkowych licencji to należy je dostarczyć na całość oferowanych zasobów.
- Kopie migawkowe:
  - Urządzenie musi mieć możliwość wykonywania natychmiastowej kopii danych (point-in- time copy). Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postępowania.
- Migracja wolumenów logicznych:
  - Urządzenie musi mieć możliwość wykonania migracji wolumenów logicznych pomiędzy różnymi typami dysków wewnątrz macierzy bez zatrzymywania aplikacji korzystającej z tych wolumenów. Wymaga się, aby zasoby źródłowe podlegające migracji oraz zasoby, do których są migrowane mogły być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, SATA).
- Replikacja:
  - Macierz musi umożliwiać replikację synchroniczną i asynchroniczną danych na inną identyczną macierzą. Zasoby źródłowe kopii zdalnej oraz docelowe kopii zdalnej mogą być zabezpieczone różnymi poziomami RAID i egzystować na różnych technologicznie dyskach stałych (SAS, SSD, NL-SAS/SATA/midline SAS). Replikacja musi być realizowana zarówno przy użyciu interfejsów Fibre Channel (FC) jak i protokołu IP. Macierz musi wspierać program Vmware Site Recovery Manager. Replikacja nie może być realizowana przez oprogramowanie lub urządzenie zewnętrzne.

    - Jeżeli funkcjonalność wymaga licencji to należy ją dostarczyć.
- Klaster macierzowy:
    - Zaoferowane rozwiązanie musi posiadać implementacje klastra geograficznego.
    - W ramach architektury klastra geograficznego musi być wspierane bezprzerwowe migrowanie maszyn wirtualnych pomiędzy ośrodkami. W przypadku awarii jednego z ośrodków nastąpi bezprzerwowe przełączenie do lokalizacji zapasowej. Powyższa funkcjonalność musi być realizowana niezależnie od systemu operacyjnego na poziomie przełączania ścieżek do urządzenia logicznego. Rozwiązanie nie może być zrealizowane przez oprogramowanie lub urządzenie zewnętrzne.
    - Jeżeli funkcjonalność wymaga licencji to należy ją dostarczyć.
- Wirtualizacja zasobów:
    - Macierz musi mieć możliwość wirtualizacji zasobów znajdujących się na innych niż oferowane macierze dyskowe na potrzeby migracji danych. Migracja musi się odbyć w trybie bezprzerwowym.
- Kompresja i deduplikacja danych:
    - Macierz musi mieć możliwość kompresji i deduplikacji danych.
- Macierz musi mieć funkcjonalność wykonywania pełnej kopii lokalnych wolumenów logicznych z wykorzystaniem jedynie kontrolerów macierzy. Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postępowania.
- Macierz musi mieć możliwość dodawania kolejnych półek dyskowych oraz dysków bez przerywania pracy macierzy, dla dowolnej konfiguracji macierzy.
- Macierz musi mieć możliwość aktualizacji oprogramowania macierzy (firmware) w trybie Online.
- Macierz musi umożliwiać budowanie wolumenów o pojemności nie mniejszej niż 256 TB.
- Macierz musi optymalizować wykorzystanie dysków SSD i HDD poprzez automatyczną identyfikację najbardziej obciążonych fragmentów woluminów w zarządzanych zasobach dyskowych (wewnętrznych jak i zewnętrznych, zwirtualizowanych) oraz ich automatyczną migrację na grupę dyskową składającą się z szybszych nośników. Macierz musi posiadać możliwość wykorzystania mechanizmu optymalizacji umiejscowienia danych pomiędzy przynajmniej 3 rodzajami grup dyskowych składających się z dysków - SSD, SAS oraz NL-SAS/SATA/midline SAS, jak również przy wykorzystaniu dwóch dowolnych z wyżej wymienionych typów. Opisany powyżej proces optymalizacji musi posiadać funkcję włączenia/wyłączenia na poziomie pojedynczego woluminu.
- Jeżeli funkcjonalność wymaga licencji to nie jest ona wymagana na tym etapie postępowania.
- Do macierzy należy dołączyć wszelkie niezbędne okablowanie umożliwiające redundantne podłączenie do obudowy i dwóch serwerów (konfiguracja HA)

Inne:

- Dostarczone urządzenie musi mieć zainstalowane wszystkie najnowsze zestawy poprawek dotyczących dostarczanego sprzętu (najnowsza wersja firmware na dzień dostawy).
- Oferowane produkty (urządzenia, sprzęty) w przedmiotowym postępowaniu o udzielenie zamówienia publicznego muszą spełniać wymagania norm CE, tj. muszą spełniać wymogi niezbędne do oznaczenia produktów znakiem CE.
- Wszystkie oferowane urządzenia muszą być fabrycznie nowe.
- Urządzenia i ich komponenty muszą być oznakowane przez producenta w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta.
- Urządzenie musi współpracować z siecią energetyczną o parametrach w przedziale 200V- 230V, 50 Hz.

Gwarancja:

- Wymagana jest gwarancja świadczona w trybie NBD (Next Business Day) przez 5 dni w tygodniu na wszystkie elementy macierzy (sprzęt oraz oprogramowanie) na okres minimum 3 lat.

- Ze względu na minimum 3 letni okres zamawiający wymaga, aby usługi serwisowe świadczone były wyłącznie przez producenta oferowanego sprzętu lub autoryzowanego partnera serwisowego producenta (wymagane oświadczenie producenta).
- Wymagane jest pozostawienie uszkodzonych nośników danych u klienta.

X. KARTA HOST BUS ADAPTER FIBRE CHANNEL (typ1) – 2 szt

Wymagania minimalne:

- Ogólne:
  - Rodzaj urządzenia: Host bus adapter.
  - Typ obudowy: Karta wkładana do gniazda - niski profil.
  - Karta musi być kompatybilna z serwerem DELL R640 (service tag: JT0NY03, 1V0NY03) który posiada zamawiający.
  - Karta musi być nowa, nie refabrykowana.
- Praca w sieci:
  - Porty: 16Gb Fibre Channel x 2.
  - Technologia podłączania: Przewodowa.
  - Protokół komunikacyjny danych: 16Gb Fibre Channel.
- Rozszerzenie / połączenie
  - Interfejsy: 2 x 16Gb Fibre Channel.
  - Zamawiający dostarczy 2 wkładki 16Gb Fibre Channel.

Gwarancja:

- 12 miesięcy

XI. KARTA HOST BUS ADAPTER FIBRE CHANNEL (typ2) – 2 szt

Wymagania minimalne:

- Ogólne:
  - Rodzaj urządzenia: Host bus adapter.
  - Typ obudowy: Karta wkładana do gniazda - wysoki profil.
  - Karta musi być kompatybilna z serwerem DELL R720 (service tag: 80QQ022, 3VPQ022) który posiada zamawiający.
  - Karta musi być nowa, nie refabrykowana.
- Praca w sieci:
  - Porty: 16Gb Fibre Channel x 2.
  - Technologia podłączania: Przewodowa.
  - Protokół komunikacyjny danych: 16Gb Fibre Channel.
- Rozszerzenie / połączenie
  - Interfejsy: 2 x 16Gb Fibre Channel.
  - Zamawiający dostarczy 2 wkładki 16Gb Fibre Channel.

Gwarancja:

- 12 miesięcy

XII. PÓŁKA ROZSZERZEŃ Z DYSKAMI DO SERWERA NAS – 2 szt

Wymagania minimalne:

- Ogólne:
  - Półka musi być kompatybilna z serwerem NAS - Synology RS3618xs (sn: 18C0QNRN5GSG7, 18C0QNRWDVYJA), które posiada zamawiający,
  - Powinna być wyposażona w 12 szt dysków HDD 3,5" o pojemności 6TB SATA certyfikowanych do serwerów NAS i trybu pracy 24x7,
  - dysk powinien znajdować się na liście zgodności produktów firmy Synology na stronie https://www.synology.com/pl-pl/compatibility
  - Półka powinna być wyposażona w zestaw szyn do montażu w szafie rack 19".
- Parametry techniczne półki:
  - Przechowywanie:
    - Kieszeń/kieszenie na dyski: 12 szt
    - Zgodny typ dysków:
      - 3.5" SATA HDD
      - 2.5" SATA HDD
      - 2.5" SATA SSD
    - Maksymalna pojemność wewnętrzna:
      - 192 TB (16 TB drive x 12) (Pojemność może się różnić w zależności od typu macierzy RAID)
      - Dysk z możliwością wymiany podczas pracy (hot-swap): TAK
    - Zarządzanie macierzami RAID za pomocą wbudowanego systemu: TAK
  - Porty zewnętrzne
    - Infiniband port: 1
  - Zasilanie:
    - Przywracanie zasilania: synchronizowane z serwerem,
    - Zasilacz / Adapter: 500 W,
    - Napięcie wejściowe zasilania prądem zmiennym: 100 V do 240 V AC,
    - Częstotliwość zasilania: 50/60 Hz, Jednofazowy.
  - Inne:
    - Wentylator obudowy: 80 mm x 80 mm x 3 szt
    - Łatwy w wymianie wentylator obudowy: TAK

Gwarancja półka:

- Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

Gwarancja dyski HDD:

- Minimum 3 letnia gwarancja (serwis) producenta

XIII. DWUPORTOWA KARTA ROZSZERZEŃ 10GbE SFP+ DLA SERWERA NAS – 2 szt

Wymagania minimalne:

- Ogólne:
  - Karta musi być kompatybilna z serwerem NAS - Synology RS3618xs (sn: 18C0QNRN5GSG7, 18C0QNRWDVYJA), które posiada zamawiający,
  - Powinna być wyposażona w 2 porty SFP+,
  - Z kartą musi być dostarczona 1 wkładka SFP+ 10GBASE-SR i 1 wkładka 10GBASE-T
  - Wkładki powinny być kompatybilne z kartą i znajdować się na liście zgodności

produktów firmy Synology na stronie https://www.synology.com/pl-pl/compatibility

- Parametry techniczne karty:
  - Interfejs magistrali hosta:
    - PCIe 3.0 zgodny z PCIe 2.0
    - 8-liniowe lub 4-liniowe z automatyczną negocjacją
  - Wysokość mocowania: Niskoprofilowe i o pełnej wysokości
- Sieć:
  - Zgodność ze specyfikacją IEEE:
    - IEEE 802.3ae — 10Gbps Ethernet
    - IEEE 802.3ad Link Aggregation
    - CPU Offload
  - Szybkość transferu danych: 10 Gbps
  - Tryb działania w sieci : Pełny dupleks

Gwarancja:

- Minimum 5 letnia gwarancja (serwis) producenta. Gwarancja musi zapewniać dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego w trybie 24x7 na wszystkie elementy i licencje. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

XIV. LICENCJA PRZEDŁUŻAJĄCA WSPARCIE O 3 LATA DLA URZĄDZENIA UTM – 2 szt

Wymagania minimalne:

- Ogólne:
  - Licencja musi przedłużyć wsparcie o 3 lata na urządzeniu UTM firmy Fortinet – FortiGate 600E które posiada zamawiający (sn: FG6H0ETB20901833, FG6H0ETB20901777)
  - Wsparcie i ochrona w trybie 24x7 musi być na moduły: FortiCare plus Application Control, IPS, AV, Web Filtering and Antispam, FortiSandbox Cloud
  - Według producenta musi być kompatybilna z numerem SKU: #FC-10-F6H0E-950-02-36

XV. WKŁADKA SFP+ DO PRZEŁĄCZNIKA SIECI LAN (typ 1) – 16 SZT

Wymagania minimalne:

- Ogólne:
  - Typ wkładki SFP+: 10GBASE-SR
  - Kompatybilna z urządzeniem HPE Aruba 8320 48 10/6 40 X472 5 2 Bdl które posiada zamawiający
  - Nowe i nie refabrykowane
- Gwarancja:
  - 12 miesięczna producenta

XVI. WKŁADKA SFP+ DO PRZEŁĄCZNIKA SIECI LAN (typ 2) – 10 SZT

Wymagania minimalne:

- Ogólne:
  - Typ wkładki SFP+: 10GBASE-T
  - Kompatybilna z urządzeniem HPE Aruba 8320 48 10/6 40 X472 5 2 Bdl które posiada zamawiający
  - Nowe i nie refabrykowane
- Gwarancja:
  - 12 miesięczna producenta

Zakres wdrożenia:

Ogólnie:

- Sieć LAN i SAN należy zbudować w siedzibie zamawiającego w oparciu o nowo wybudowaną infrastrukturę światłowodową kablem wielomodowym OM4, gdzie najdłuższe połączenia nie przekraczają 300 mb. Infrastruktura jest ułożona w topologii podwójnej gwiazdy z 7 lokalnymi punktami dystrybucyjnymi i 2 głównymi. Pomiędzy lokalnym, a każdym głównym punktem dystrybucyjnym jest ułożone 6 włókien światłowodu, natomiast główne punkty dystrybucyjne połączone są 48 włóknami.
- Przełączniki CORE, SAN, macierze i półki serwerów NAS należy zamontować w obecnych szafach RACK, które znajdują się w serwerowniach z głównymi punktami dystrybucyjnymi. Przełączniki LAN accesowe należy zamontować w lokalnych i zdalnych punktach dystrybucyjnych w obecnych szafach RACK. Lokalizacje zdalne znajdują się na terenie miasta Płocka.
- Oferowane produkty muszą spełniać wszystkie parametry określone w niniejszym załączniku oraz być fabrycznie nowe, pochodzić z legalnego źródła, muszą być dostarczone przez autoryzowany kanał sprzedaży producenta na terenie kraju i objęte standardowym pakietem usług gwarancyjnych zawartych w cenie urządzenia i oprogramowania świadczonych przez sieć serwisową producenta na terenie Polski. Zamawiający zastrzega sobie prawo do żądania potwierdzenia źródła pochodzenia urządzenia w postaci oświadczenia producenta.
- Zamawiający zastrzega sobie prawo do żądania przedstawienia certyfikatów, deklaracji, norm i oświadczeń wymienionych w szczegółach specyfikacji.
- Usługi należy wykonać w sposób i w czasie ograniczającym do minimum wpływ na produkcyjne działanie systemu informatycznego zamawiającego.
- Stare (wymieniane) urządzenia pozostają w Urzędzie Miasta Płocka.

Zabezpieczenie sieci Zamawiającego:

- Dokonanie instalacji fizycznej wszystkich wymaganych urządzeń teletechnicznych oraz dostarczanego sprzętu. Wszystkie urządzenia muszą zostać podłączone i uruchomione.
- Wykonawca dostarczy odpowiednią ilość wkładek SFP, SFP+ i QSFP+, patchcordów światłowodowych i UTP niezbędną do wykonania fizycznych połączeń.
- Analiza oraz przeniesienie aktualnej konfiguracji przełączników LAN, optymalizacja, a w przypadku braku odpowiednich funkcjonalności - ponowna konfiguracja.

Sieć LAN i urządzenia:

- Instalacja przełączników w 9 punktach dystrybucyjnych w głównej siedzibie zamawiającego i 4 lokalizacjach zdalnych, przełączników CORE w 2 głównych punktach dystrybucyjnych.
- Podłączenie przełączników dostępowych do 2 urządzeń CORE.
- Podłączenie przełączników CORE między sobą i do obecnych 2 UTM-ów (Fortigate 600E)

- Upgrade do najnowszej obecnej wersji (jeżeli jest dostępna), konfiguracja połączeń typu stack.
- Konfiguracja dostępu SSH, VLAN, loop protect, STP, UDLD, arp protect, dhcp spoofnig, trunks.
- Konfiguracja 802.1x, podłączenie przełączników do oprogramowania zarządzającego.
- Instalacja AP, upgrade, konfiguracja wirtualnego zarządczy AP.
- Konfiguracja sieci bezprzewodowych.
- Konfiguracja sieci gościnnej z zewnętrznym Captive Portalem.

Sieć SAN i urządzenia:

- Dostawa i montaż urządzeń w 2 serwerowniach.
- Konfiguracja przełączników SAN.
- Montaż kart HOST BUS ADAPTER FIBRE CHANNEL w 4 serwerach i podłączenie do przełączników SAN.
- Wstępna konfiguracja i zainicjowanie macierzy dyskowych – uruchomienie replikacji
- Konfiguracja zoningu na potrzeby replikacji macierzy.
- Konfiguracja zoningu/inicjatorów macierz-serwery.
- Utworzenie pierwszego LUN i zaprezentowanie go do maszyn Vmware.
- Testowa migracja maszyny wirtualnej, weryfikacja replikacji po stronie macierzy.
- Symulacja awarii macierzy.
- Utworzenie procedury uruchomienia/odtworzenia w przypadku wystąpienia awarii.
- Zamawiający wymaga aby osoba instalująca macierz posiadała ważne certyfikaty techniczne (wymagane poniżej dokumenty dołączyć do oferty):
  - VMware wydany przez producenta oprogramowania,
- Zamawiający wymaga dostarczenia oświadczenia Producenta macierzy:
  - potwierdzającego, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

System kontroli dostępu do sieci (NAC):

- Instalacja instancji NAC na platformie Vmware 6.7.
- Integracja ze środowiskiem zamawiającego – AD 2012R2, LDAP, SMTP, SNMP.
- Konfiguracja serwisów 802.1X, MAC authentication, Captive Portal.
- konfiguracja portów na przełączniku referencyjnym.
- Konfiguracja funkcjonalności sprawdzania stanu urządzenia końcowego.
- Konfiguracja serwisów TACACS+.

System zarządzania urządzeniami sieciowymi:

- Instalacja serwera wirtualnego na platformie Vmware 6.7 dostarczonej przez zamawiającego.
- Konfiguracja SSH, SNMP, Dodanie przełączników LAN.
- Utworzenie topologii połączenia urządzeń sieciowych.
- Konfiguracja autobackapów switchy
- Integracja z domeną AD 2012R2

Półki dyskowe i karty rozszerzeń do serwerów NAS:

- Montaż półek w 2 serwerowniach w obecnych szafach RACK.
- Montaż dysków w półkach i podłączenie do obecnych serwerów Synology RS3618xs.
- Montaż kart rozszerzeń w serwerach Synology
- Podłączenie sieci LAN światłowodem MM do przełącznika dostępowego
- Konfiguracja nowych volumenów

Dokumentacja powykonawcza:

- Wykonawca dostarczy dokumentację powykonawczą z opisem wykonanych prac w wersji papierowej i elektronicznej.

Szkolenia:
Wykonawca przeprowadzi jednodniowe szkolenie dla 3 administratorów sieci w siedzibie Zamawiającego z obsługi wdrażanego systemu.