Załącznik nr 1 do SWZ

Numer sprawy: BZP-3942-51/2021

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem postępowania jest **zakup, montaż i konfiguracja urządzeń sieci LAN, kopii zapasowej, storage dyskowego, cyfrowych urządzeń telewizji dozorowej oraz systemu SSWiN, KD dla Akademii Sztuk Pięknych im. Jana Matejki w Krakowie**, z podziałem zamówienia na 4 części, jak następuje:

Część 1: zakup, montaż i konfiguracja urządzeń sieci LAN: urządzeń brzegowych, przełączników, kontrolera, punktów dostępowych.

Część 2: zakup, montaż i konfiguracja zasobów dyskowych.

Cześć 3: zakup, montaż i konfiguracja urządzeń oraz oprogramowania do wykonywania kopii zapasowych offline.

Część 4: zakup, montaż i konfiguracja cyfrowych urządzeń telewizji dozorowej oraz zakup, montaż i konfiguracja systemu SSWiN, KD.

2. Szczegółowy opis dla poszczególnej części zamówienia znajduje się w niniejszym dokumencie (załącznik nr 1 do SWZ).

3. Przedmiot zamówienia dotyczy projektu: „Realizacja wydatków niekwalifikowanych towarzyszących pozostałym projektom współfinansowanym ze środków europejskich - Cyfrowa dostępność oraz cyfrowe bezpieczeństwo Akademii Sztuk Pięknych im. Jana Matejki w Krakowie".

4. Sprzęt objęty przedmiotem zamówienia określonym w części nr 1, 2, 3, 4, będzie dostarczany, montowany oraz konfigurowany w budynkach Akademii Sztuk Pięknych im. Jana Matejki w Krakowie w następujących lokalizacjach:

a) Plac Jana Matejki 13, Kraków

b) ul. Humberta 3, Kraków

c) ul. Marszałka J. Piłsudskiego 21, Kraków

d) ul. Marszałka J. Piłsudskiego 38, Kraków

e) Plac Jana Matejki 4, Kraków

f) ul. Smoleńsk 9, Kraków

g) ul. Lea 27/29, Kraków

h) ul. Karmelicka 16, Kraków

i) ul. Harenda 16, Zakopane

Za wyjątkiem lokalizacji przy ul. Lea 27/29 i ul. Karmelicka 16 w Krakowie oraz ul. Harenda 16 w Zakopanem, Zamawiający **nie zapewnia miejsc parkingowych.** Możliwa (po uprzednim uzgodnieniu z Zamawiającym) dostawa i zmagazynowanie czasowe sprzętu w godzinach poza funkcjonowaniem strefy ograniczonego parkowania.

Zamawiający nie zapewnia żadnej formy uprawnienia do wjazdu w strefę ograniczonego ruchu/parkowania w Krakowie.

5. W związku z brakami sprzętu IT na rynku oraz bardzo długimi czasami dostaw Zamawiający dopuszcza w części 1 dostawę równoważnego sprzętu zastępczego w oczekiwaniu na dostawę sprzętu właściwego. W protokole odbioru zostanie zawarta informacja o sprzęcie zastępczym oraz terminie dostawy sprzętu właściwego. W przypadku braku dostawy sprzętu docelowego w uzgodnionym terminie naliczone zostaną kary umowne.

6. Na podstawie art. 83 ust. 1 pkt 26) ustawy o podatku od towarów i usług w związku z art. 83 ust. 14 tej ustawy Zamawiający wystąpi o możliwość zastosowania stawki podatku VAT 0% dla sprzętu określonego w części nr 1 i 2 przedmiotowego zamówienia.

Część 1: zakup, montaż i konfiguracja urządzeń sieci LAN: urządzeń brzegowych, przełączników, kontrolera, punktów dostępowych.

Wymagania dotyczące proponowanych urządzeń

Sprzęt dostarczony w ramach realizacji umowy będzie sprzętem nowym, nieużywanym oraz niedostarczanym wcześniej w żadnym innych projektach. W ramach realizacji umowy dostarczony sprzęt będzie posiadał gwarancję świadczoną bezpośrednio przez Producenta sprzętu. W przypadku wątpliwości, podmiot sprzedający (kupujący sprzęt od partnera handlowego Producenta) ma obowiązek przedstawić oficjalny dokument Producenta, który będzie poświadczał, że sprzęt dostarczony w ramach realizacji umowy będzie sprzętem zakupionym w oficjalnym kanale sprzedaży oraz zarejestrowanym na użytkownika końcowego (kupującego sprzęt w od partnera handlowego Producenta). Zamawiający zastrzega sobie prawo sprawdzenia poprzez numery seryjne czy dostarczony sprzęt spełnia wszystkie wyżej wymienione warunki. W przypadku niespełnienia przez sprzęt któregokolwiek z wyżej wymienionych warunków Zamawiający zastrzega sobie prawo zwrotu całego dostarczonego sprzętu (na koszt dostawcy), jak również obciążenia dostawcy – Oferent - karą umowną za niedotrzymanie warunków umowy. W ramach składanej oferty, Oferent zobowiązany jest do wyszczególnienia wszystkich numerów seryjnych produktów (licencje, sprzęt i oprogramowanie). Lista ta będzie podlegała weryfikacji przez Zamawiającego lub niezależną firmę zewnętrzną, wskazaną przez Zamawiającego, w celu weryfikacji z wymaganiami i zgodnością z SWZ. Zamawiający wymagam także, aby Oferent był bezpośrednio oficjalnym partnerem handlowym Producenta oferowanych urządzeń, a możliwość zweryfikowania tego faktu była publicznie dostępna poprzez stronę Producenta. Razem z ofertą należy dostarczyć dokument zawierający adres URL ze strony Producenta, gdzie taka weryfikacja może zostać przeprowadzona.

Specyfikacja prac wdrożeniowych w ramach projektu

Przed rozpoczęciem prac należy ustalić plan adresacji i wykorzystania adresów. Ustalenia te będą prowadzone z wyznaczonymi do tego celu pracownikami Zamawiającego. Przed rozpoczęciem prac Wykonawca musi przeprowadzić analizę stanu sieci, serwerów i jego usług oraz ustalić harmonogram prac. Konfiguracja będzie obejmowała nowo dostarczone oprogramowanie i sprzęt oraz już znajdujące się urządzenia w infrastrukturze Zamawiającego. Ze względów bezpieczeństwa, szczegółowy zakres prac zostanie udostępniony tylko wyłonionemu Wykonawcy. Cały sprzęt musi zostać wcześniej prekonfigurowany i sprawdzony u Wykonawcy, tak aby zminimalizować ilość prac realizowanych w siedzibie Zamawiającego.

Wykonawca zobowiązany jest do wykonania wizji lokalnej w każdym z oddziałów w celu ustalenia rozmieszczenia punktów dostępowych sieci bezprzewodowej. Prace montażowe, instalacyjne i wdrożeniowe Wykonawca będzie realizował na terenie kilku lokalizacji krakowskich i jednej lokalizacji w Zakopanem.

Usługa konfiguracji dostarczonych urządzeń zawierać będzie m.in.:

- konfigurację IPsec VPN (IKEv2) pomiędzy wszystkimi lokalizacjami,
- konfigurację zaawansowanych funkcji ochrony przed złośliwym oprogramowanie, filtrowaniem URL oraz ochrony przed zagrożeniami IPS (Instrusion Prevention System),
- konfigurację usługi VPN Remote Access,
- konfiguracja reguł ACL na urządzeniach brzegowych (Zamawiający zastrzega, że w tym zakresie ma bardzo złożone wymagania, które dotyczą dużej ilości usług, jaka hostowana jest w ramach infrastruktury),
- integrację punktów dostępowych z kontrolerem sieci bezprzewodowej oraz wykreowanie wszystkich potrzebnych sieci bezprzewodowych z odpowiednią obsługą uwierzytelnienia i VLAN,
- integrację usług uwierzytelnienia VPN i sieci WiFi ze wskazanym serwerem RADIUS,
- uruchomienie obsługi EDUROAM w ramach sieci WiFi,
- protokoły VLAN, Trunk, STP, RSTP, MSTP, LACP, adresację IP, konfigurację DNS, routingu,
- baner logowania, usługa NTP, SSH, wbudowane mechanizmy RBAC oraz konta użytkowników,
- automatyczne wykonywanie kopii zapasowej z przełączników po każdym zapisaniu konfiguracji do wskazanego serwera FTP,
- wysyłanie zdarzeń syslog do wskazanego serwera Syslog,
- mechanizmy bezpieczeństwa: Port Security, IP DHCP Snooping, IP Source Guard i Dynamic ARP Inspection lub w pełni równoważne,
- hardening urządzeń sieciowych według najlepszych praktyk Producenta,
- personalizacja ustawień do przedstawionych wymagań,
- integrację urządzeń z obecnymi w infrastrukturze,
- integrację urządzeń z systemem do monitorowania Zabbix oraz usługą zbierania zdarzeń i plików,
- aktualizację wszystkich topologii w systemie monitorowania Zabbix,
- konfigurację innych funkcjonalności dostarczonych urządzeń i oprogramowania, które okażą się potrzebne w trakcie wdrożenia, gdy Wykonawca uzna zasadności ich aktywacji oraz skonfigurowania.

Obecna infrastruktura sieciowa Zamawiającego zbudowana jest w dużej większości na urządzeniach firmy Cisco Systems, do których należą m.in. produkty: Cisco WLC, Cisco Air, Cisco Catalyst, Cisco ASA-X, Cisco UCS, Cisco Nexus i Cisco ISR G2. W ramach prac będzie wymagana integracja dostarczonego rozwiązania z tymi produktami oraz migracja z niektórych produktów Cisco Systems, konfiguracji i polityk, do nowo dostarczonych urządzeń. Stąd wymaga się od Wykonawcy znajomości rozwiązania, jakie oferuje oraz dodatkowo posiadania minimum następujących certyfikatów Producenta Cisco Systems: Cisco Certified Network Professional Enterprise, Cisco Certified Network Professional Security i Cisco Certified Network Professional Data Center. Aby spełnić warunek znajomości oferowanych urządzeń, personel Wykonawcy musi posiadać certyfikaty równoważne do wskazanych wyżej, wystawione przez Producenta oferowanych urządzeń. Dodatkowo, wszystkie oferowane urządzenia mają zostać zintegrowane z usługami zbierania logów i plików konfiguracyjnych, jakie działają w ramach dwóch systemów RHEL (Red Hat Enterprise Linux) oraz systemem do monitorowania Zabbix. Inżynier wykonujący te prace musi posiadać certyfikat RHCE (Red Hat Certified

Engineer). Wszystkie certyfikaty należy dołączyć do oferty, gdyż ich brak zostanie uznany jako niespełnienie postawionych warunków i będzie skutkował odrzuceniem oferty.

Wykonawca zobowiązany jest zutylizować wymieniany w trakcie realizacji projektu stary sprzęt sieciowy, wskazany przez Zamawiającego.

Wykonawca przeprowadzi instruktaż (do 4 godzin lekcyjnych) u Zamawiającego dla 5 osób. Szkolenie ma dotyczyć zmian zaistniałych w sieci, wykorzystanych technologii, sposobu działania nowego systemu, procedur aktualizacji oprogramowania na dostarczonych urządzeniach.

Wykonawca zobowiązany jest do zapewnienia gwarancji na wdrożoną konfigurację przez okres do 1 miesiąca po zamknięciu wdrożenia lub do momentu oddania pełnego dostępu do interfejsu zarządzającego dostarczonych urządzeń i oprogramowania. Wykonawca zobowiązany jest do udokumentowania zmian przeprowadzonych w systemie informatycznym Zamawiającego w dokumentacji powdrożeniowej. Dokumentacja ta powinna obejmować topologię oraz tabele adresacji. Wszelkie materiały i dokumentacje mają być w języku polskim.

Specyfikacja dodatkowych modułów i okablowania:

Zamawiający wymaga dostarczenia modułów i okablowania, które muszą być kompatybilne z dostarczonymi urządzeniami:

- 40x moduł MM SFP+
- 8x moduł SM SFP+
- 2x moduł SM SFP+ (bidirectionl)
- 10x twinax 2 metrowe 10G
- 4x twinax 5 metrowe 10G
- 4 x patchcord SM długości 2 metry
- 20 x patchcord MM długości 2 metry

Specyfikacja przełącznika typu 1 - Ilość: 1 sztuka.

1. Przełącznik posiada:
    a. 48 portów 1/10/25GE SFP+ bezpośrednio w obudowie przełącznika lub na karcie liniowej przełącznika modularnego.
    b. 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps.
    c. Minimum 64 GB pamięci Flash.
    d. Minimum 24 GB pamięci DRAM.
2. Parametry wydajnościowe:
    a. Prędkość przełączania „wirespeed” dla każdego portu przełącznika.
    b. Urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.
    c. Obsługiwana łączna przepływność (pasmo) min. 3 Tbps.
    d. Obsługiwana łączna przepustowość pakietowa przełącznika min. 1 bpps.
    e. Opóźnienie przełączania pakietów nie większe niż 2 µs.
3. Przełącznik posiada następującą funkcjonalność warstwy L2:
    a. Trunking IEEE 802.1Q VLAN.
    b. Wsparcie dla min. 4000 sieci VLAN.
    c. Funkcjonalność izolowania portów znajdujących się w tym samym VLAN.

d. Wsparcie sprzętowe dla minimum 90 tysięcy adresów MAC.
e. IEEE 802.1w Rapid Spanning Tree (RST).
f. IEEE 802.1s Multiple Spanning Tree (MST).
g. Wsparcie sprzętowe dla tunelowania QinQ.
h. Statyczny i dynamiczny NAT.
i. Zabezpieczenie przeciwko incydentom w topologii Spanning Tree.
j. Internet Group Management Protocol (IGMP) Versions 2, 3.
k. Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach.
l. Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce.
m. Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów).

4. Przełącznik posiada następująca funkcjonalność warstwy L3:
    a. Sprzętowe przełączanie pakietów w warstwie L3.
    b. Routing w oparciu o trasy statyczne.
    c. Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6.
    d. Policy Based Routing (PBR) dla IPv4 i IPv6.
    e. Możliwość uruchomienia sprzętowego load balancera dla protokołów IPv4 i IPv6 ze wsparciem dla tworzenia grup serwerów i adresów VIP, próbkowania serwerów, wyboru ruchu na podstawie protokołu/portu L4 i poprzez filtra ACL.
    f. VRRP v3.
    g. Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol).
    h. Wsparcie sprzętowe dla minimum 768 000 prefixów LPM/ wpisów hosta w tablicy routingu IP.
    i. Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast).
    j. Wsparcie dla IGMPv3 oraz MSDP.
    k. Wsparcie dla Microsoft NLB.
    l. Wsparcie sprzętowe dla minimum 32,000 tras multicastowych.
    m. Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking).
    n. Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP).
    o. Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list.
    p. Jeśli funkcjonalność opisana powyżej w pkt 4. wymaga dostarczenia dodatkowej licencji, to jest ona wymagana na tym etapie.
5. Przełącznik posiada możliwość dołączania zewnętrznych, wyniesionych modułów lub przełączników GigabitEthernet oraz 10 GigabitEthernet. Dołączenie modułów lub przełączników nie jest realizowane z wykorzystaniem mechanizmów L2 (Spanning Tree), ani L3, a jedynie w ramach domeny fizycznej bądź stosu urządzeń. Porty modułu wyniesionego są udostępniane do zarządzania i monitorowania z poziomu przełącznika macierzystego.
6. Przełącznik posiada sprzętowe wsparcie dla szyfrowania portów Ethernet z wykorzystaniem technologii MacSec IEEE 802.1ad na blokach 128 bit oraz 256 bit oraz wykorzystaniem trybu GCM-AES-XPN. Jeśli funkcjonalność ta wymaga dostarczenia dodatkowej licencji, to nie jest ona wymagana na tym etapie.
7. Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN:
    a. Sprzętowa implementacja VTEP (VXLAN Tunnel Endpoint).
    b. Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway).
    c. Wymiana ruchu z co najmniej 255 innymi sprzętowymi VTEP.

d. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP.
e. Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast).
f. Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol).
g. Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).
h. Jeśli funkcjonalność opisana powyżej w pkt 7. wymaga dostarczenia dodatkowej licencji, to nie jest ona wymagana w trakcie tego postępowania.

8. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
   a. Layer 2 IEEE 802.1p (CoS).
   b. Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4; klasyfikacja ruchu musi odbywać się w zależności, od co najmniej: interfejsu, typu ramki Ethernet, sieci VLAN, priorytetu w warstwie 2 (802.1p), adresów MAC, adresów IP, wartości pola ToS/DSCP w nagłówkach IP, portów TCP i UDP.
   c. Kolejkowanie na wyjściu w oparciu o CoS 802.1p.
   d. Bezwzględne (strict-priority) kolejkowanie na wyjściu.
   e. Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający.
   f. Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych.
   g. Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych.
   h. Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.
   i. Urządzenie musi posiadać architekturę pamięci przystosowaną dla obsługi buforów, QoS oraz ruchu typu microburst, zapewniając skuteczną obsługę zarówno małych jak i bardzo dużych przepływów danych. Urządzenie musi potrafić monitorować wykorzystanie buforów i sygnalizować przekraczanie zdefiniowanych przez użytkownika progów wielkości przepływu przypadku zaistnienia zjawiska microburst (chwilowe wzrosty ruchu).
9. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:
   a. Wejściowe ACL (standardowe oraz rozszerzone).
   b. Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC, typ protokołu.
   c. Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP).
   d. ACL oparte o VLAN-y (VACL).
   e. ACL oparte o porty (PACL).
   f. DHCP Snooping.
   g. ARP Inspection.
   h. IP Source Guard.
   i. Prewencja niekontrolowanego wzrostu ilości ruchu (storm control) dla ruchu unicast, multicast, broadcast.

10. Funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika:
    a. Port zarządzający 100/1000 Mbps;
    b. Port konsoli CLI.
    c. Zarządzanie In-band.
    d. SSHv2.
    e. Authentication, authorization, and accounting (AAA).
    f. RADIUS.
    g. TACACS+.
    h. Syslog.
    i. SNMP v1, v2, v3.
    j. RMON (przynajmniej grupy Events, Alarms).
    k. sFlow lub netFlow.
    l. Wsparcie sprzętowe dla telemetrii przepływów z możliwością eksportu z wykorzystaniem protokołu gRPC.
    m. IEEE 802.1ab LLDP.
    n. 802.1x i dynamiczny przydział VLAN do portu.
    o. Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback).
    p. Role-Based Access Control RBAC.
    q. Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing).
    r. Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (Mirror.)
    s. Network Time Protocol (NTP).
    t. Precision Time Protocol IEEE 1588.
    u. Diagnostyka procesu BOOT.
    v. Ping.
    w. Traceroute.
11. Narzędzia programowania i zarządzania przełącznikiem:
    a. Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API.
    b. Wbudowana powłoka bash do zarządzania systemem Linux przełącznika.
    c. Wsparcie dla kontenerów Docker wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych.
    d. Interfejs programistyczny REST API wraz z upublicznionym SDK.
    e. Możliwość zainstalowania klienta Chef.
    f. Możliwość zainstalowania agenta Puppet.
    g. Wsparcie dla NETCONF i zarządzania poprzez XML.
    h. Wsparcie dla OpenStack Neutron plugin.
12. Przełącznik musi być wyposażony w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut ciepłego powietrza od strony portów liniowych.
13. Obudowa o rozmiarach maksymalnie 1RU (rack unit), przeznaczona do montażu w szafie rackowej 19”. W wypadku zastosowania przełącznika modularnego dopuszcza się większy rozmiar urządzenia.
14. Urządzenie objęte 3-letnim serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia,

wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.

Specyfikacja przełącznika typu 2 - Ilość: 9 sztuk.

1. Przełącznik stakowalny wyposażony w minimum 48 portów 10/100/1000BaseT.
2. Przełącznik musi dysponować mocą 740W dostępnych dla PoE/PoE+ oraz wspierać możliwość rozbudowy PoE/PoE+ do 1440W.
3. Przełącznik musi zasilić 48 portów z mocą PoE+.
4. Przełącznik musi posiadać minimum 4-portowy moduł/porty osadzone w urządzeniu 10Gigabit Ethernet SFP+. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH).
5. Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów:
    a. Przepustowość w ramach stosu min. 80Gb/s.
    b. Minimum 8 urządzeń w stosie.
    c. Stos widoczny jako jeden node dla procesu spanning-tree.
    d. Zarządzanie poprzez jeden adres IP.
    e. Możliwość tworzenia połączeń cross-stack link aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad.
    f. Przełączniki muszą umożliwiać współdzielenie mocy zasilaczy tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie).
6. Urządzenie musi posiadać możliwość instalacji podtrzymania zasilania pomimo restartu urządzenia (następuję tylko programowy reset).
7. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate).
8. Urządzenie posiada 6MB bufor pamięci współdzielony przez wszystkie porty.
9. Minimum 2GB pamięci DRAM i 4GB pamięci flash.
10. Urządzenie musi zapewniać przepustowość nie mniejszą niż 175 Gbps.
11. Szybkość przełączania urządzenia musi wynosić minimum 125 Mpps.
12. Obsługa minimum:
    a. 1024 sieci VLAN;
    b. 16.000 adresów MAC;
    c. 8.000 tras IPv4;
    d. 1.500 tras IPv6.
13. Obsługa protokołu NTP.
14. Obsługa IGMPv1/2/3.
15. Wszystkie porty na przełączniku muszą obsługiwać standard 802.1AE (szyfrowanie ruchu) 128-bit z prędkością linerate dla każdego z interfejsów.
16. System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy.
17. System operacyjny przełącznika jest konfigurowalny poprzez API za pomocą m.in protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz umożliwia eksportowanie zdefiniowanych według potrzeb danych do zewnętrznych systemów.

18. Przełącznik zapewnia widoczność aplikacyjną, klasyfikowanie ruchu w warstwach 4-7 i na jego podstawie zapewnia budowanie polityk bezpieczeństwa czy jakości usług.
19. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree;
    b. Per-VLAN Rapid Spanning Tree (PVRST+);
    c. IEEE 802.1s Multi-Instance Spanning Tree;
    d. Obsługa minimum 128 instancji protokołu STP.
20. Obsługa protokołu IEEE 802.1ab LLDP i LLDP-MED.
21. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
22. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
23. Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
    a. Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level).
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL.
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
    g. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem.
    h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
    i. Minimum 1000 wpisów dla list kontroli dostępu (ACE).
    j. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www).
    k. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
    l. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard).
    m. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+.
    n. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia).
24. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    b. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek.

c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting). Możliwość skonfigurowania do 1000 ograniczeń per przełącznik.
f. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

25. Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4(OSPF) oraz funkcjonalności Policy-based routingu. Urządzenie musi mieć możliwość zapewnienia wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, ISIS) i IPv6 (OPSFv3), routingu multicast (PIM-SM, PIM-SSM) poprzez wgranie odpowiedniej licencji.
26. Możliwość wsparcia dla protokołu LISP zgodnie z RFC 6830.
27. Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN).
28. Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 16.000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow.
29. Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez Producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
30. Dedykowany port Ethernet do zarządzania out-of-band.
31. Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.
32. Urządzenie musi być wyposażone w port konsoli USB.
33. Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
34. Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
35. Urządzenie musi posiadać wbudowany analizator pakietów.
36. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
37. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
38. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.
39. Możliwość montażu w szafie rack 19”. Wysokość urządzenia nie może przekraczać 1 RU.
40. Oferowany przełącznik musi być wyposażony w zasilacz podstawowy o mocy minimum 1KW.
41. Razem z urządzeniem wymaga się dostarczenia świadczonego przez Producenta 3-letniego serwisu 8X5XNBD.

42. Wraz z urządzeniem muszą być dostarczone licencje umożliwiające uruchomienie Flexible NetFlow, Wireshark.

Specyfikacja przełącznika typu 3 - Ilość: 3 sztuki.

1. Przełącznik musi być wyposażony w 48 porty 10/100/1000BaseT RJ-45 + uplink 4x10G SFP/SFP+.
2. Porty SFP muszą mieć możliwość obsadzenia następującymi rodzajami wkładek:
    a. Gigabit Ethernet 1000Base-SX.
    b. Gigabit Ethernet 1000Base-LX/LH.
    c. 10Gigabit Ethernet 10GBase-SR.
    d. 10Gigabit Ethernet 10GBase-LR.
    e. 10Gigabit Ethernet typu twinax (SFP+ - SFP+).
3. Urządzenie musi posiadać funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi.
4. Urządzenie musi być wyposażone w wbudowany zasilacz AC 230V. W przypadku portów PoE przełącznik musi podtrzymywać zasilanie na portach PoE podczas restartu urządzenia.
5. Parametry wydajnościowe (co najmniej):
    a. Przepustowość przełącznika: 176 Gb/s (full duplex).
    b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 130 Mpps.
    c. Pamięć DRAM – 512 MB.
    d. Pamięć flash – 256 MB.
    e. Wielkość bufora pakietów - 1.5 MB.
    f. Obsługa 256 aktywnych sieci VLAN.
    g. Obsługa 15000 adresów MAC.
    h. Obsługa 16 statycznych tras IPv4.
    i. Obsługa 16 statycznych tras IPv6.
    j. Obsługa 64 interfejsów SVI L3.
    k. Obsługa MTU-L3 9198B.
    l. Obsługa ramek Ethernet Jumbo 10240B.
    m. Obsługa 1024 grupy IGMP.
    n. Obsługa 6 połączeń zagregowanych typu „port channel”.
    o. Obsługa 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
    p. Obsługa Ilość wpisów w listach kontroli dostępu Security ACL – 600.
    q. Obsługa ilość wpisów w listach kontroli dostępu QoS ACL – 600.
6. Porty dostępowe przełącznika muszą posiadać zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet).
7. Przełącznik musi posiadać obsługę protokołu NTP.
8. Przełącznik musi posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping.
9. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree.
    b. Per-VLAN Rapid Spanning Tree (PVRST+).
    c. IEEE 802.1s Multi-Instance Spanning Tree.
    d. Obsługa 64 instancji protokołu STP.

e. Przełącznik musi obsługiwać protokoły LLDP i LLDP-MED.
f. Przełącznik musi obsługiwać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
g. Przełącznik musi wspierać połączenia link aggregation zgodnie z IEEE 802.3ad.
h. Przełącznik musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.

10. Przełącznik musi obsługiwać następujące mechanizmy związane z bezpieczeństwem sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level).
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL.
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
    g. Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication).
    h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
    i. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania - 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www).
    j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
    k. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.
    l. Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP).
    m. Funkcja Private VLAN.
11. Przełącznik musi obsługiwać następujące mechanizmy zapewniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    a. sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
    b. bezpieczna sekwencja uruchamiania,
    c. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
12. Przełącznik musi obsługiwać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek.
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).

d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń.
f. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

13. Przełącznik musi obsługiwać mechanizmy routingu statycznego dla IPv4 i IPv6.
14. Przełącznik musi umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących.
15. Przełącznik musi obsługiwać funkcjonalność wzorców konfiguracji portów zawierających prekonfigurowane ustawienia rekomendowane przez Producenta, zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
16. Przełącznik musi obsługiwać protokół sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow.
17. Przełącznik musi posiadać następujące funkcjonalności związane z zarządzaniem:
    a. Port konsolowy.
    b. Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika.
    c. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.
    d. Obsługa protokołów SNMPv3, SSHv2, https, syslog.
    e. Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia.
    f. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki.
18. Przełącznik musi posiadać gwarancję, która zapewnia wymianę sprzętu na drugi dzień roboczy oraz wsparcie Producenta w wymiarze 8x5 (5 dni w tygodniu, 8 godzin) w okresie pierwszych 12 miesięcy. Dodatkowo przełącznik musi zostać objęty gwarancją z wymianą sprzętu do 14 dni, w okresie do 3 lat od opublikowania ogłoszenia o wycofaniu produktu ze sprzedaży przez Producenta.

Specyfikacja przełącznika typu 4 - Ilość: 1 sztuka

1. Przełącznik musi być wyposażony w 48 porty 10/100/1000BaseT RJ-45 + uplink 4x1G SFP.
2. Porty SFP muszą mieć możliwość obsadzenia następującymi rodzajami wkładek:
    a. Gigabit Ethernet 1000Base-SX,
    b. Gigabit Ethernet 1000Base-LX/LH.
3. Urządzenie musi posiadać funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi.

4. Urządzenie musi być wyposażone w wbudowany zasilacz AC 230V. W przypadku portów PoE przełącznik musi podtrzymywać zasilanie na portach PoE podczas restartu urządzenia.
5. Parametry wydajnościowe (co najmniej):
    a. Przepustowość przełącznika: 104 Gb/s (full duplex).
    b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 77 Mpps.
    c. Pamięć DRAM – 512 MB.
    d. Pamięć flash – 256 MB.
    e. Wielkość bufora pakietów - 1.5 MB.
    f. Obsługa 256 aktywnych sieci VLAN.
    g. Obsługa 15000 adresów MAC.
    h. Obsługa 16 statycznych tras IPv4.
    i. Obsługa 16 statycznych tras IPv6.
    j. Obsługa 64 interfejsów SVI L3.
    k. Obsługa MTU-L3 9198B.
    l. Obsługa ramek Ethernet Jumbo 10240B.
    m. Obsługa 1024 grupy IGMP.
    n. Obsługa 6 połączeń zagregowanych typu „port channel”.
    o. Obsługa 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
    p. Obsługa Ilość wpisów w listach kontroli dostępu Security ACL – 600.
    q. Obsługa ilość wpisów w listach kontroli dostępu QoS ACL – 600.
6. Porty dostępowe przełącznika muszą posiadać zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet).
7. Przełącznik musi posiadać obsługę protokołu NTP.
8. Przełącznik musi posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping.
9. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree.
    b. Per-VLAN Rapid Spanning Tree (PVRST+).
    c. IEEE 802.1s Multi-Instance Spanning Tree.
    d. Obsługa 64 instancji protokołu STP.
    e. Przełącznik musi protokoły LLDP i LLDP-MED.
    f. Przełącznik musi obsługiwać funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
    g. Przełącznik musi wspierać połączenia link aggregation zgodnie z IEEE 802.3ad.
    h. Przełącznik musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
10. Przełącznik musi obsługiwać następujące mechanizmy związane z bezpieczeństwem sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level).
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL.
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.

e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
g. Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication).
h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
i. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania - 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www).
j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
k. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.
l. Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP).
m. Funkcja Private VLAN.

11. Przełącznik musi obsługiwać następujące mechanizmy zapewniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    a. sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
    b. bezpieczna sekwencja uruchamiania,
    c. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
12. Przełącznik musi obsługiwać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek.
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
    d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
    e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń.
    f. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
    g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
13. Przełącznik musi obsługiwać mechanizmy routingu statycznego dla IPv4 i IPv6.
14. Przełącznik musi umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących.
15. Przełącznik musi obsługiwać funkcjonalność wzorców konfiguracji portów zawierających prekonfigurowane ustawienia rekomendowane przez Producenta, zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
16. Przełącznik musi obsługiwać protokół sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow.
17. Przełącznik musi posiadać następujące funkcjonalności związane z zarządzaniem:

a. Port konsolowy.
b. Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika.
c. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.
d. Obsługa protokołów SNMPv3, SSHv2, https, syslog.
e. Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia.
f. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki.

18. Przełącznik musi posiadać gwarancję, która zapewnia wymianę sprzętu na drugi dzień roboczy oraz wsparcie Producenta w wymiarze 8x5 (5 dni w tygodniu, 8 godzin) w okresie pierwszych 12 miesięcy. Dodatkowo przełącznik musi zostać objęty gwarancją z wymianą sprzętu do 14 dni, w okresie do 3 lat od opublikowania ogłoszenia o wycofaniu produktu ze sprzedaży przez Producenta.

<u>Specyfikacja przełącznika typu 5 - Ilość: 4 sztuki.</u>

1. Przełącznik musi być wyposażony w 48 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x10G SFP/SFP+. Dla technologii PoE przełącznik musi być w stanie dostarczyć minimum 370W (30W dla dowolnych 12 portów jednocześnie lub 15W dla dowolnych 24 portów jednocześnie). Porty SFP muszą mieć możliwość obsadzenia następującymi rodzajami wkładek:
    a. Gigabit Ethernet 1000Base-SX,
    b. Gigabit Ethernet 1000Base-LX/LH,
    c. 10Gigabit Ethernet 10GBase-SR,
    d. 10Gigabit Ethernet 10GBase-LR,
    e. 10Gigabit Ethernet typu twinax (SFP+ - SFP+).
2. Urządzenie musi posiadać funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi.
3. Urządzenie musi być wyposażone w wbudowany zasilacz AC 230V. W przypadku portów PoE przełącznik musi podtrzymywać zasilanie na portach PoE podczas restartu urządzenia.
4. Parametry wydajnościowe (co najmniej):
    a. Przepustowość przełącznika: 176 Gb/s (full duplex).
    b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 130 Mpps.
    c. Pamięć DRAM – 512 MB.
    d. Pamięć flash – 256 MB.
    e. Wielkość bufora pakietów - 1.5 MB.
    f. Obsługa 256 aktywnych sieci VLAN.
    g. Obsługa 15000 adresów MAC.
    h. Obsługa 16 statycznych tras IPv4.
    i. Obsługa 16 statycznych tras IPv6.
    j. Obsługa 64 interfejsów SVI L3.
    k. Obsługa MTU-L3 9198B.

l. Obsługa ramek Ethernet Jumbo 10240B.
m. Obsługa 1024 grupy IGMP.
n. Obsługa 6 połączeń zagregowanych typu „port channel”.
o. Obsługa 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
p. Obsługa Ilość wpisów w listach kontroli dostępu Security ACL – 600.
q. Obsługa ilość wpisów w listach kontroli dostępu QoS ACL – 600.

5. Porty dostępowe przełącznika muszą posiadać zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet).
6. Przełącznik musi posiadać obsługę protokołu NTP.
7. Przełącznik musi posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping.
8. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree.
    b. Per-VLAN Rapid Spanning Tree (PVRST+).
    c. IEEE 802.1s Multi-Instance Spanning Tree.
    d. Obsługa 64 instancji protokołu STP.
    e. Przełącznik musi protokoły LLDP i LLDP-MED.
    f. Przełącznik musi obsługiwać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
    g. Przełącznik musi wspierać połączenia link aggregation zgodnie z IEEE 802.3ad.
    h. Przełącznik musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
9. Przełącznik musi obsługiwać następujące mechanizmy związane z bezpieczeństwem sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level).
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL.
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
    g. Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication).
    h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
    i. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania - 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www).
    j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
    k. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.

l. Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP).
m. Funkcja Private VLAN.

10. Przełącznik musi obsługiwać następujące mechanizmy zapewniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    a. sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
    b. bezpieczna sekwencja uruchamiania,
    c. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
11. Przełącznik musi obsługiwać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek.
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
    d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
    e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń.
    f. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
    g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
12. Przełącznik musi obsługiwać mechanizmy routingu statycznego dla IPv4 i IPv6.
13. Przełącznik musi umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących.
14. Przełącznik musi obsługiwać funkcjonalność wzorców konfiguracji portów zawierających prekonfigurowane ustawienia rekomendowane przez Producenta, zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
15. Przełącznik musi obsługiwać protokół sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow.
16. Przełącznik musi posiadać następujące funkcjonalności związane z zarządzaniem:
    a. Port konsolowy.
    b. Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika.
    c. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.
    d. Obsługa protokołów SNMPv3, SSHv2, https, syslog.
    e. Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia.
    f. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki.

17. Przełącznik musi posiadać gwarancję, która zapewnia wymianę sprzętu na drugi dzień roboczy oraz wsparcie Producenta w wymiarze 8x5 (5 dni w tygodniu, 8 godzin) w okresie pierwszych 12 miesięcy. Dodatkowo przełącznik musi zostać objęty gwarancją z wymianą sprzętu do 14 dni, w okresie do 3 lat od opublikowania ogłoszenia o wycofaniu produktu ze sprzedaży przez Producenta.

Specyfikacja przełącznika typu 6 - Ilość: 5 sztuk.

1. Przełącznik musi być wyposażony w 48 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x1G SFP. Dla technologii PoE przełącznik musi być w stanie dostarczyć minimum 370W (30W dla dowolnych 12 portów jednocześnie lub 15W dla dowolnych 24 portów jednocześnie). Porty SFP muszą mieć możliwość obsadzenia następującymi rodzajami wkładek:
    a. Gigabit Ethernet 1000Base-SX,
    b. Gigabit Ethernet 1000Base-LX/LH.
2. Urządzenie musi posiadać funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi.
3. Urządzenie musi być wyposażone w wbudowany zasilacz AC 230V. W przypadku portów PoE przełącznik musi podtrzymywać zasilanie na portach PoE podczas restartu urządzenia.
4. Parametry wydajnościowe (co najmniej):
    a. Przepustowość przełącznika: 104 Gb/s (full duplex).
    b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 77 Mpps.
    c. Pamięć DRAM – 512 MB.
    d. Pamięć flash – 256 MB.
    e. Wielkość bufora pakietów - 1.5 MB.
    f. Obsługa 256 aktywnych sieci VLAN.
    g. Obsługa 15000 adresów MAC.
    h. Obsługa 16 statycznych tras IPv4.
    i. Obsługa 16 statycznych tras IPv6.
    j. Obsługa 64 interfejsów SVI L3.
    k. Obsługa MTU-L3 9198B.
    l. Obsługa ramek Ethernet Jumbo 10240B.
    m. Obsługa 1024 grupy IGMP.
    n. Obsługa 6 połączeń zagregowanych typu „port channel”.
    o. Obsługa 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
    p. Obsługa Ilość wpisów w listach kontroli dostępu Security ACL – 600.
    q. Obsługa ilość wpisów w listach kontroli dostępu QoS ACL – 600.
5. Porty dostępowe przełącznika muszą posiadać zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet).
6. Przełącznik musi posiadać obsługę protokołu NTP.
7. Przełącznik musi posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping.
8. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree.
    b. Per-VLAN Rapid Spanning Tree (PVRST+).
    c. IEEE 802.1s Multi-Instance Spanning Tree.

d. Obsługa 64 instancji protokołu STP.
e. Przełącznik musi protokoły LLDP i LLDP-MED.
f. Przełącznik musi obsługiwać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
g. Przełącznik musi wspierać połączenia link aggregation zgodnie z IEEE 802.3ad.
h. Przełącznik musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.

9. Przełącznik musi obsługiwać następujące mechanizmy związane z bezpieczeństwem sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level).
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL.
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
    g. Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication).
    h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
    i. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania - 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www).
    j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
    k. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.
    l. Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP).
    m. Funkcja Private VLAN.
10. Przełącznik musi obsługiwać następujące mechanizmy zapewniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    a. sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
    b. bezpieczna sekwencja uruchamiania,
    c. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
11. Przełącznik musi obsługiwać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek.
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).

d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń.
f. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.

12. Przełącznik musi obsługiwać mechanizmy routingu statycznego dla IPv4 i IPv6.
13. Przełącznik musi umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących.
14. Przełącznik musi obsługiwać funkcjonalność wzorców konfiguracji portów zawierających prekonfigurowane ustawienia rekomendowane przez Prodecenta, zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
15. Przełącznik musi obsługiwać protokół sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow.
16. Przełącznik musi posiadać następujące funkcjonalności związane z zarządzaniem:
    a. Port konsolowy.
    b. Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika.
    c. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.
    d. Obsługa protokołów SNMPv3, SSHv2, https, syslog.
    e. Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia.
    f. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki.
17. Przełącznik musi posiadać gwarancję, która zapewnia wymianę sprzętu na drugi dzień roboczy oraz wsparcie Producenta w wymiarze 8x5 (5 dni w tygodniu, 8 godzin) w okresie pierwszych 12 miesięcy. Dodatkowo przełącznik musi zostać objęty gwarancją z wymianą sprzętu do 14 dni, w okresie do 3 lat od opublikowania ogłoszenia o wycofaniu produktu ze sprzedaży przez Producenta.

<u>Specyfikacja przełącznika typu 7 - Ilość: 1 sztuka.</u>

1. Przełącznik musi być wyposażony w 24 porty 10/100/1000BaseT RJ-45 PoE+ (zgodne z IEEE 802.3at) + uplink 4x1G SFP. Dla technologii PoE przełącznik musi być w stanie dostarczyć minimum 195W (30W dla dowolnych 6 portów jednocześnie lub 15W dla dowolnych 13 portów jednocześnie). Porty SFP muszą mieć możliwość obsadzenia następującymi rodzajami wkładek:
    c. Gigabit Ethernet 1000Base-SX,
    d. Gigabit Ethernet 1000Base-LX/LH.

2. Urządzenie musi posiadać funkcjonalność zarządzania przez 1 adres IP grupą (klastrem) do 8 urządzeń pochodzących z tej samej rodziny przełączników połączonych portami uplinkowymi.
3. Urządzenie musi być wyposażone w wbudowany zasilacz AC 230V. W przypadku portów PoE przełącznik musi podtrzymywać zasilanie na portach PoE podczas restartu urządzenia.
4. Parametry wydajnościowe (co najmniej):
    a. Przepustowość przełącznika: 56 Gb/s (full duplex).
    b. Prędkość przesyłania (forwarding rate) dla 64 bajtowych pakietów L3: 41 Mpps.
    c. Pamięć DRAM – 512 MB.
    d. Pamięć flash – 256 MB.
    e. Wielkość bufora pakietów - 1.5 MB.
    f. Obsługa 256 aktywnych sieci VLAN.
    g. Obsługa 15000 adresów MAC.
    h. Obsługa 16 statycznych tras IPv4.
    i. Obsługa 16 statycznych tras IPv6.
    j. Obsługa 64 interfejsów SVI L3.
    k. Obsługa MTU-L3 9198B.
    l. Obsługa ramek Ethernet Jumbo 10240B.
    m. Obsługa 1024 grupy IGMP.
    n. Obsługa 6 połączeń zagregowanych typu „port channel”.
    o. Obsługa 16 linków w ramach jednego połączenia zagregowanego typu „port channel” LACP.
    p. Obsługa Ilość wpisów w listach kontroli dostępu Security ACL – 600.
    q. Obsługa ilość wpisów w listach kontroli dostępu QoS ACL – 600.
5. Porty dostępowe przełącznika muszą posiadać zgodność ze standardem IEEE 802.3az EEE (Energy Efficient Ethernet).
6. Przełącznik musi posiadać obsługę protokołu NTP.
7. Przełącznik musi posiadać obsługę protokołu IGMPv1/2/3 i MLDv1/2 Snooping.
8. Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. IEEE 802.1w Rapid Spanning Tree.
    b. Per-VLAN Rapid Spanning Tree (PVRST+).
    c. IEEE 802.1s Multi-Instance Spanning Tree.
    d. Obsługa 64 instancji protokołu STP.
    e. Przełącznik musi protokoły LLDP i LLDP-MED.
    f. Przełącznik musi obsługiwać funkcjonalność Layer 2 traceroute umożliwiającą śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
    g. Przełącznik musi wspierać połączenia link aggregation zgodnie z IEEE 802.3ad.
    h. Przełącznik musi obsługiwać funkcję Voice VLAN umożliwiającą odseparowanie ruchu danych i ruchu głosowego. Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
9. Przełącznik musi obsługiwać następujące mechanizmy związane z bezpieczeństwem sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level).
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL.

d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
g. Możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem (multidomain authentication).
h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
i. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania - 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www).
j. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
k. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.
l. Obsługa list kontroli dostępu Port ACL umożliwiające kontrolę ruchu wchodzącego (inbound) na poziomie portów L2 przełącznika, filtracja na bazie informacji L2 (adresy MAC) jak również na bazie informacji L3 (adresy IP).
m. Funkcja Private VLAN.

10. Przełącznik musi obsługiwać następujące mechanizmy zapewniające autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym:
    a. sprawdzanie autentyczności oprogramowania przed uruchomieniem urządzenia,
    b. bezpieczna sekwencja uruchamiania,
    c. sprzętowy układ umożliwiający sprawdzenie autentyczności urządzenia.
11. Przełącznik musi obsługiwać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 4 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek.
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
    d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
    e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z możliwością skonfigurowania minimum 64 różnych ograniczeń.
    f. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
    g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
12. Przełącznik musi obsługiwać mechanizmy routingu statycznego dla IPv4 i IPv6.
13. Przełącznik musi umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizm SPAN z możliwością obsługi do 4 sesji monitorujących.
14. Przełącznik musi obsługiwać funkcjonalność wzorców konfiguracji portów zawierających prekonfigurowane ustawienia rekomendowane przez Producenta, zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).

15. Przełącznik musi obsługiwać protokół sFlow dla wszystkich portów fizycznych uplinkowych i downlinkowych dla ruchu w kierunku wejściowym i wyjściowym z możliwością skonfigurowania 2 różnych kolektorów ruchu sFlow.
16. Przełącznik musi posiadać następujące funkcjonalności związane z zarządzaniem:
    a. Port konsolowy.
    b. Dostęp bezprzewodowy Bluetooth do interfejsu zarządzającego urządzenia (telnet, ssh) przez zastosowanie zewnętrznego urządzenia Bluetooth podłączonego do portu USB przełącznika.
    c. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.
    d. Obsługa protokołów SNMPv3, SSHv2, https, syslog.
    e. Port USB umożliwiający podłączenie zewnętrznego nośnika danych np. w celu upgradu oprogramowania urządzenia.
    f. Wbudowany graficzny interfejs zarządzania przełącznikiem dostępny z poziomu przeglądarki.
17. Przełącznik musi posiadać gwarancję, która zapewnia wymianę sprzętu na drugi dzień roboczy oraz wsparcie Producenta w wymiarze 8x5 (5 dni w tygodniu, 8 godzin) w okresie pierwszych 12 miesięcy. Dodatkowo przełącznik musi zostać objęty gwarancją z wymianą sprzętu do 14 dni, w okresie do 3 lat od opublikowania ogłoszenia o wycofaniu produktu ze sprzedaży przez Producenta.

<u>Specyfikacja przełącznika typu 8 - Ilość: 1 sztuka.</u>

1. 1Typ i liczba portów: 16 portów 1/10G SFP+.
2. Slot na moduł rozszerzeń (możliwość instalacji/wymiany „na gorąco” – ang. hot swap) z możliwością obsadzenia modułami (zależnie od potrzeb):
    a. 8x1/10G SFP+,
    b. 2x40G QSFP.
2. Porty SFP+/QSFP możliwe do obsadzenia szerokim wachlarzem wkładek zależnie od potrzeb:
    a. Porty SFP+ – wkładki Gigabit Ethernet – w tym 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-EX, 1000Base-ZX, 1000Base-BX-D/U oraz 10Gigabit Ethernet – w tym 10GBase-SR, 10GBase-LR, 10GBase-LRM, 10GBase-ER, 10GBase-ZR, 10GBase-BX-D/U, twinax.
    b. Porty QSFP – wkładki 40Gigabit Ethernet w tym 40G-SR4, 40G-LR4, 40G-ER4, 40G-SR-BD, twinax.
3. Zasilanie i chłodzenie:
    a. Redundantne i wymienne moduły wentylatorów.
    b. Możliwość instalacji zasilacza redundantnego AC 230V. Zasilacze wymienne (możliwość instalacji/wymiany „na gorąco” – ang. hot swap).
4. Parametry wydajnościowe:
    a. Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate).
    b. Bufor pakietów – 32MB.
    c. Pamięć DRAM – 16GB.
    d. Pamięć flash – 16GB.
    e. Obsługa:

- 4.000 sieci VLAN,
- 64.000 adresów MAC,
- 64.000 tras IPv4,
- 32.000 tras IPv6.

5. Obsługa protokołu NTP.
6. Obsługa IGMPv1/2/3 i MLDv1/2 Snooping.
7. Przełącznik wspiera następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
    a. EEE 802.1w Rapid Spanning Tree.
    b. Per-VLAN Rapid Spanning Tree (PVRST+).
    c. IEEE 802.1s Multi-Instance Spanning Tree.
    d. Obsługa 128 instancji protokołu STP.
8. Obsługa protokołu LLDP i LLDP-MED.
9. Funkcjonalność Layer 2 traceroute umożliwiająca śledzenie fizycznej trasy pakietu o zadanym źródłowym i docelowym adresie MAC.
10. Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego.
11. Możliwość uruchomienia funkcji serwera DHCP.
12. Mechanizmy związane z bezpieczeństwem sieci:
    a. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik umożliwia zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level).
    b. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN.
    c. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL.
    d. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X.
    e. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC.
    f. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X.
    g. Możliwość uwierzytelniania wielu użytkowników na jednym porcie oraz możliwość jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem.
    h. Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176.
    i. 18 000 wpisów dla list kontroli dostępu (Security ACE).
    j. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www).
    k. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard.
    l. Zapewnienie podstawowych mechanizmów bezpieczeństwa IPv6 na brzegu sieci (IPv6 FHS) – w tym minimum ochronę przed rozgłaszaniem fałszywych komunikatów Router Advertisement (RA Guard) i ochronę przed dołączeniem nieuprawnionych serwerów DHCPv6 do sieci (DHCPv6 Guard).
    m. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS i TACACS+.
    n. Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia).

o. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE (MACSec) dla wszystkich portów przełącznika (dla połączeń switch-switch i switch-host) kluczami o długości 128-bitów (gcm-aes-128).
p. Wbudowane mechanizmy ochrony warstwy kontrolnej przełącznika (CoPP – Control Plane Policing).
q. Punkcja Private VLAN.

13. Technologie umożliwiające zapewnienie autentyczności sprzętu i oprogramowania:
    a. Trust Anchor Module - odporne na manipulacje, zabezpieczone kryptograficzne rozwiązanie zapewniające autentyczność sprzętu w celu jednoznacznej identyfikacji produktu – daje pewność, że produkt jest oryginalny.
    b. Secure Boot – zabezpiecza proces sekwencji startowej zapewniając, że mamy niezmieniony sprzęt oraz zapewniając warstwową ochronę przed próbą załadowania nielegalnego/zmodyfikowanego oprogramowania systemowego.
    c. Image signing - obrazy podpisane kryptograficznie zapewniają, że oprogramowanie systemowe (firmware), BIOS i inne oprogramowanie są autentyczne i niezmodyfikowane. Podczas uruchamiania systemu sygnatury oprogramowania są sprawdzane pod kątem integralności.
14. Mechanizmy związane z zapewnieniem jakości usług w sieci:
    a. Implementacja 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi.
    b. Implementacja algorytmu Shaped Round Robin dla obsługi kolejek.
    c. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority).
    d. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP.
    e. Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate limiting).
    f. Kontrola sztormów dla ruchu broadcast/multicast/unicast.
    g. Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP.
15. Obsługa protokołów routingu:
    a. Routing statyczny dla IPv4 i IPv6.
    b. Routing dynamiczny – RIP, OSPF.
    c. Policy-based routing (PBR).
    d. Obsługa protokołu redundancji bramy (VRRP).
16. Przełącznik umożliwia lokalną i zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego – mechanizmy SPAN, RSPAN.
17. Przełącznik posiada wzorce konfiguracji portów zawierające prekonfigurowane ustawienia rekomendowane przez Producenta, zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.).
18. Zarządzanie:
    a. Port konsoli.
    b. Dedykowany port Ethernet do zarządzania out-of-band.
    c. Plik konfiguracyjny urządzenia możliwy do edycji w trybie off-line (możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC).

Po zapisaniu konfiguracji w pamięci nieulotnej możliwość uruchomienia urządzenia z nową konfiguracją.

d. Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
e. Możliwość konfiguracji za pomocą protokołu NETCONF (RFC 6241) i modelowania YANGa (RFC 6020) oraz eksportowania zdefiniowanych według potrzeb danych do zewnętrznych systemów.
f. Przełącznik posiada diodę umożliwiającą identyfikację konkretnego urządzenia podczas akcji serwisowych.
g. Przełącznik posiada wbudowany tag RFID w celu łatwiejszego zarządzania infrastrukturą.
h. Port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie ma możliwość uruchomienia z nośnika danych umieszczonego w porcie USB.

19. Możliwość montażu w szafie rack 19”. Wysokość urządzenia 1 RU.
20. Możliwość próbkowania i eksportu statystyk ruchu do zewnętrznych kolektorów danych (bez samplowania) ze wsparciem sprzętowym - NetFlow – obsługa 128 000 strumieni.
21. Możliwość tworzenia skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie.
22. Możliwość tworzenia i uruchamiania skryptów Python bezpośrednio na przełączniku.
23. Wyposażenie urządzenia:
    a. Moduł uplink 8x1/10G SFP+.
    b. Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy.
24. Urządzenie objęte 3-letnim serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.

Urządzenie musi umożliwić uruchomienie poniższych funkcjonalności poprzez zmianę licencji. Bez zmian w części sprzętowej urządzenia.

25. Możliwość połączenia dwóch przełączników w stos (z wykorzystaniem standardowych modułów optycznych/twinax) celem stworzenia pojedynczego logicznego przełącznika z zapewnieniem następujących funkcjonalności:
    a. Zarządzanie poprzez jeden adres IP.
    b. Możliwość tworzenia połączeń cross-stack Link Aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z IEEE 802.3ad.
    c. Możliwość aktualizacji oprogramowania w trakcie pracy stosu (ISSU – In Service Software Upgrade).
26. Wsparcie dla protokołu LISP zgodnie z RFC 6830.
27. Obsługa MPLS – w tym L3 VPN i Multicast VPN (mVPN).
28. Obsługa zaawansowanych protokołów routingu:
    a. IS-IS i BGP dla IPv4 i IPv6,
    b. EIGRP (rfc7868),
    c. Routing multicastów - PIM-SM, PIM-SSM,
    d. Multicast Source Discovery Protocol (MSDP),
    e. VRF-Lite.
29. Możliwość szyfrowania ruchu zgodnie z IEEE 802.1AE kluczami o długości 256-bitów (gcm-aes-256).
30. System operacyjny przełącznika umożliwia wgrywanie poprawek bez konieczności restartowania platformy.

31. Możliwość enkapsulacji ruchu w pakiety VXLAN.
32. Wsparcie dla IEEE 1588v2 (PTP – Precision Time Protocol).
33. Wsparcie dla IEEE 802.1BA (AVB – Audio Video Bridging).
34. Funkcjonalność bramy dla usług mDNS.
35. Wbudowany analizator pakietów.
36. Możliwość zdalnej obserwacji ruchu z określonych portów lub sieci VLAN polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego poprzez sieć IP (ERSPAN).
37. Przełącznik zapewnia widoczność i kontrolę ruchu na poziomie aplikacji (klasyfikowanie ruchu w warstwach 4-7).
38. Możliwość eksportu dodatkowych pół w ramach statystyk NetFlow – w tym IDP (Initial Data Pacekt) oraz SPLT (Sequence of Packet Lengths and Times) niezbędnych do analizy zagrożeń w ruchu szyfrowanym (wykrywanie malware, audyt wykorzystywanych algorytmów bezpieczeństwa).

Specyfikacja urządzenia typu Firewall Nowej Generacji typu 1 - ilość: 1 sztuka.

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3. Urządzenie wyposażone w 8 portów 1 Gigabit Ethernet, minimum 2 porty SFP oraz 2 porty SFP+.
4. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN.
5. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
6. Urządzenie wyposażone w port USB 2.0.
7. Możliwość montażu w szafie rack 19" (dołączone niezbędne elementy montażowe).
8. Wysokość urządzenia 1RU.
9. Przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 5.2Gb/s, a dla modułów AVC oraz systemu IPS na poziomie 4.8Gb/s.
10. Wydajność dla ruchu rzeczywistego http dla modułów AVC lub IPS na poziomie 5Gb/s.
11. Maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 500 000 z możliwością zestawiania co najmniej 26 000 nowych połączeń na sekundę.
12. Wsparcie dla VPN IPSec na poziomie 2.4 Gb/s.
13. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
14. Możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentnym.
15. Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP).
16. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
17. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT).
18. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
19. Urządzenie zapewnia funkcjonalność tzw. Firewall'a Next-Generation w zakresie:

a. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),
b. systemu IPS (Intrusion Prevention System).

20. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelnienie.
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu.
    c. Wiedza o urządzeniach mobilnych.
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta.
    e. Wiedza o podatnościach.
    f. Wiedza o bieżących zagrożeniach.
    g. Baza danych URL.
21. System posiada otwarte API dla współpracy z systemami zewnętrznymi, w tym co najmniej z systemami SIEM.
22. Urządzenie umożliwia konfiguracją IPsec IKEv2 oraz SSL VPN Remote Access z możliwością uwierzytelniania w serwerze RADIUS/LDAP/AD. W ramach połączenia VPN system umożliwia stworzenie kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruch jak i również tzw. „Split tunelingu" (funkcja ta jest konfigurowana per grupa VPN RA).
23. System wykrywania aplikacji AVC zapewniający:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji;
    b. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług;
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji;
    d. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.
24. System IPS zapewniający:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system);
    b. możliwość pracy w trybie pasywnym (IDS);
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        i. złośliwe oprogramowanie,
        ii. skanowanie sieci,
        iii. ataki na usługę VoIP,
        iv. próby przepełnienia bufora,
        v. ataki na aplikacje P2P,
        vi. zagrożenia dnia zerowego, itp.;
    d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna);
    e. wiele sposobów wykrywania zagrożeń w tym:
        i. sygnatury ataków opartych na exploitach,
        ii. reguły oparte na zagrożeniach,
        iii. mechanizm wykrywania anomalii w protokołach,
        iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego;

f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu;
g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives);
h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń;
i. wiele możliwości reakcji na zdarzenia w tym takie, jak:
    i. tylko monitorowanie,
    ii. blokowanie ruchu zawierającego zagrożenia,
    iii. zastąpienie zawartości pakietów,
    iv. zapisywanie pakietów;
j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6;
k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
    i. systemach operacyjnych,
    ii. serwisach,
    iii. otwartych portach, aplikacjach,
    iv. zagrożeniach;
l. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych;
m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.;
n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji;
o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego;
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne;
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie;
r. obsługę reguł Snort;
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS;
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise);
u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa.

25. System filtracji URL zapewniający:
    a. kategoryzację stron – w co najmniej 70 kategoriach,
    b. bazę URL o wielkości nie mniejszej niż 250 mln URL.
26. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:

a. pliki systemowe,
b. pliki graficzne,
c. pliki PDF,
d. pliki wykonywalne,
e. pliki multimedialne,
f. pliki pakietu Office,
g. pliki skompresowane.

27. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.
28. Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez:
    a. sprawdzenie reputacji plików w systemie globalnym,
    b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze),
    c. statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
29. Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
    a. pliki wolne od złośliwego kodu,
    b. pliki zawierające złośliwy kod,
    c. pliki podejrzane,
    d. pliki o własnej, zdefiniowanej przez użytkownika kategorii.
30. Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).
31. Urządzenie objęte 3-letnim serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 3 lat.
32. Należy dostarczyć również odpowiednie licencje dla połączeń VPN RA. 100 sztuk licencji pozwalających na autoryzację komputerów. Wsparcie na licencje również powinno być dostarczone na 3 lata.

<u>Specyfikacja urządzenia typu Firewall Nowej Generacji typu 2 - ilość: 2 sztuki.</u>

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3. Urządzenie wyposażone w 8 portów 1 Gigabit Ethernet oraz 4 porty SFP.
4. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN.
5. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
6. Urządzenie wyposażone w port USB 2.0.

7. Możliwość montażu w szafie rack 19” (dołączone niezbędne elementy montażowe).
8. Wysokość urządzenia 1RU.
9. Przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall’a oraz kontroli aplikacji (AVC) na poziomie 2.2Gb/s, a dla modułów AVC oraz systemu IPS na poziomie 2.2Gb/s.
10. Wydajność dla ruchu rzeczywistego http dla modułów AVC lub IPS na poziomie 2Gb/s.
11. Maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 200 000 z możliwością zestawiania co najmniej 14 000 nowych połączeń na sekundę.
12. Wsparcie dla VPN IPSec na poziomie 1.1 Gb/s.

Zamawiający nie wymaga dostarczenia licencji na system Next-Generation firewall z zakresie Intrusion Prevention System, filtrowania URL oraz kontroli i weryfikowania plików.

13. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
14. Możliwość uruchomienia urządzenia w trybie firewall’a L3, jak i w trybie transparentnym.
15. Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP).
16. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
17. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT).
18. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
19. Urządzenie zapewnia funkcjonalność tzw. Firewall’a Next-Generation w zakresie:
    a. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),
    b. systemu IPS (Intrusion Prevention System).
20. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:
    a. Wiedza o użytkownikach – uwierzytelnienie.
    b. Wiedza o urządzeniach – pasywne skanowanie ruchu.
    c. Wiedza o urządzeniach mobilnych.
    d. Wiedza o aplikacjach wykorzystywanych po stronie klienta.
    e. Wiedza o podatnościach.
    f. Wiedza o bieżących zagrożeniach.
    g. Baza danych URL.
21. System posiada otwarte API dla współpracy z systemami zewnętrznymi, w tym co najmniej z systemami SIEM.
22. Urządzenie umożliwia konfiguracją IPsec IKEv2 oraz SSL VPN Remote Access z możliwością uwierzytelniania w serwerze RADIUS/LDAP/AD. W ramach połączenia VPN system umożliwia stworzenie, kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruch jak i również tzw. „Split tunelingu” (funkcja ta jest konfigurowana per grupa VPN RA).
23. System wykrywania aplikacji AVC zapewniający:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji;
    b. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług;
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji;

d. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.

24. System IPS zapewniający:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system);
    b. możliwość pracy w trybie pasywnym (IDS);
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        i. złośliwe oprogramowanie,
        ii. skanowanie sieci,
        iii. ataki na usługę VoIP,
        iv. próby przepełnienia bufora,
        v. ataki na aplikacje P2P,
        vi. zagrożenia dnia zerowego, itp.;
    d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna);
    e. wiele sposobów wykrywania zagrożeń w tym:
        i. sygnatury ataków opartych na exploitach,
        ii. reguły oparte na zagrożeniach,
        iii. mechanizm wykrywania anomalii w protokołach,
        iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego;
    f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu;
    g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives);
    h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń;
    i. wiele możliwości reakcji na zdarzenia w tym takie, jak:
        i. tylko monitorowanie.
        ii. blokowanie ruchu zawierającego zagrożenia.
        iii. zastąpienie zawartości pakietów.
        iv. zapisywanie pakietów;
    j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6;
    k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
        i. systemach operacyjnych,
        ii. serwisach,
        iii. otwartych portach, aplikacjach,
        iv. zagrożeniach;
    l. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych;
    m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.;

n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji;
o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego;
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne;
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie;
r. obsługę reguł Snort;
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS;
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise);
u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa.

25. System filtracji URL zapewniający:
    a. kategoryzację stron – w co najmniej 70 kategoriach.
    b. bazę URL o wielkości nie mniejszej niż 250 mln URL.
26. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe,
    b. pliki graficzne,
    c. pliki PDF,
    d. pliki wykonywalne,
    e. pliki multimedialne,
    f. pliki pakietu Office,
    g. pliki skompresowane.
27. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.
28. Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez:
    a. sprawdzenie reputacji plików w systemie globalnym,
    b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze),
    c. statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
29. Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
    a. pliki wolne od złośliwego kodu,
    b. pliki zawierające złośliwy kod,
    c. pliki podejrzane,
    d. pliki o własnej, zdefiniowanej przez użytkownika kategorii.
30. Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).

31. Urządzenie objęte 3-letnim serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 3 lat.

Specyfikacja urządzenia typu Firewall Nowej Generacji typu 3 - ilość: 4 sztuki.

Architektura urządzenia, obudowa, interfejsy:

1. Urządzenie będące dedykowaną platformą sprzętową – nie dopuszcza się rozwiązań „serwerowych" bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.
2. Urządzenie pełniące rolę ściany ogniowej (firewall) typu statefull inspection i ściany ogniowej nowej generacji (NG Firewall).
3. Urządzenie wyposażone w 8 portów 1 Gigabit Ethernet.
4. Urządzenie obsługuje interfejsy VLAN (802.1Q) na interfejsach fizycznych – minimum 1.000 sieci VLAN.
5. Urządzenie wyposażone w dedykowany port konsoli oraz dedykowany port Gigabit Ethernet do zarządzania Out-of-Band.
6. Urządzenie wyposażone w port USB 2.0.
7. Możliwość montażu w szafie rack 19" (dołączone niezbędne elementy montażowe).
8. Wysokość urządzenia 1RU.
9. Przepustowość teoretyczna urządzenia dla uruchomionych modułów firewall'a oraz kontroli aplikacji (AVC) na poziomie 850 Mb/s, a dla modułów AVC oraz systemu IPS na poziomie 850 Mb/s.
10. Wydajność dla ruchu rzeczywistego http dla modułów AVC lub IPS na poziomie 850 Mb/s.
11. Maksymalna liczba sesji (z kontrolą aplikacji) na poziomie 100 000 z możliwością zestawiania co najmniej 6 000 nowych połączeń na sekundę.
12. Wsparcie dla VPN IPSec na poziomie 250 Mb/s.

Zamawiający nie wymaga dostarczenia licencji na system Next-Generation firewall z zakresie Intrusion Prevention System, filtrowania URL oraz kontroli i weryfikowania plików.

13. Urządzenie nie posiada ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej.
14. Możliwość uruchomienia urządzenia w trybie firewall'a L3, jak i w trybie transparentnym.
15. Urządzenie obsługuje routing statyczny i dynamiczny (RIP, OSPF, BGP).
16. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory.
17. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT).
18. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby.
19. Urządzenie zapewnia funkcjonalność tzw. Firewall'a Next-Generation w zakresie:
    a. systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),
    b. systemu IPS (Intrusion Prevention System).
20. System posiada możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. System ma tworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów:

a. Wiedza o użytkownikach – uwierzytelnienie.
b. Wiedza o urządzeniach – pasywne skanowanie ruchu.
c. Wiedza o urządzeniach mobilnych.
d. Wiedza o aplikacjach wykorzystywanych po stronie klienta.
e. Wiedza o podatnościach.
f. Wiedza o bieżących zagrożeniach.
g. Baza danych URL.

21. System posiada otwarte API dla współpracy z systemami zewnętrznymi, w tym co najmniej z systemami SIEM.
22. Urządzenie umożliwia konfiguracją IPsec IKEv2 oraz SSL VPN Remote Access z możliwością uwierzytelniania w serwerze RADIUS/LDAP/AD. W ramach połączenia VPN system umożliwia stworzenie, kilku różnych grup dostępowych do sieci. System musi posiadać możliwość definiowania powitalnego banneru dla połączenia VPN RA oraz możliwości tunelowania całego ruch jak i również tzw. „Split tunelingu" (funkcja ta jest konfigurowana per grupa VPN RA).
23. System wykrywania aplikacji AVC zapewniający:
    a. możliwość klasyfikacji ruchu i wykrywania co najmniej 4000 aplikacji;
    b. możliwość tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług;
    c. wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji;
    d. współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.
24. System IPS zapewniający:
    a. możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system);
    b. możliwość pracy w trybie pasywnym (IDS);
    c. możliwość wykrywania i blokowania szerokiej gamy zagrożeń w tym:
        i. złośliwe oprogramowanie,
        ii. skanowanie sieci,
        iii. ataki na usługę VoIP,
        iv. próby przepełnienia bufora,
        v. ataki na aplikacje P2P,
        vi. zagrożenia dnia zerowego, itp.;
    d. możliwość wykrywania modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna);
    e. wiele sposobów wykrywania zagrożeń w tym:
        i. sygnatury ataków opartych na exploitach,
        ii. reguły oparte na zagrożeniach,
        iii. mechanizm wykrywania anomalii w protokołach,
        iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego;
    f. możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu;
    g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives);

h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń;
i. wiele możliwości reakcji na zdarzenia w tym takie, jak:
    i. tylko monitorowanie,
    ii. blokowanie ruchu zawierającego zagrożenia,
    iii. zastąpienie zawartości pakietów,
    iv. zapisywanie pakietów;
j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6;
k. możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o:
    i. systemach operacyjnych,
    ii. serwisach,
    iii. otwartych portach, aplikacjach,
    iv. zagrożeniach;
l. możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych;
m. możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.;
n. możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji;
o. możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego;
p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne;
q. możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie;
r. obsługę reguł Snort;
s. możliwość wykorzystania informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS;
t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise);
u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa.

25. System filtracji URL zapewniający:
    a. kategoryzację stron – w co najmniej 70 kategoriach,
    b. bazę URL o wielkości nie mniejszej niż 250 mln URL.
26. Urządzenie zapewnia możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:
    a. pliki systemowe,
    b. pliki graficzne,
    c. pliki PDF,
    d. pliki wykonywalne,
    e. pliki multimedialne,

f. pliki pakietu Office,
g. pliki skompresowane.

27. Urządzenie posiada możliwość monitorowania jak i kontrolowania transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download.
28. Wbudowany podsystem wykrywania oprogramowania złośliwego (malware) i jego propagacji w strefie chronionej poprzez:
    a. sprawdzenie reputacji plików w systemie globalnym,
    b. sprawdzenie plików w sandbox (realizowanym lokalnie lub w chmurze),
    c. statyczną analizę struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
29. Urządzenie zapewnia możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
    a. pliki wolne od złośliwego kodu,
    a. pliki zawierające złośliwy kod,
    b. pliki podejrzane,
    c. pliki o własnej, zdefiniowanej przez użytkownika kategorii.
30. Podsystem wykrywania oprogramowania złośliwego zawiera narzędzia analizy historycznej dla plików przesłanych w przeszłości, a rozpoznanych jako oprogramowanie złośliwe (analiza retrospektywna).
31. Urządzenie objęte 3-letnim serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 3 lata.

System centralnego zarządzania Firewall – 1 zestaw.

1. Wraz z urządzeniami typu firewall zostanie dostarczona dedykowana platforma zarządzająca dla wszystkich firewall zamawianych przez Zamawiającego. Platforma zarządzająca może mieć formę maszyny wirtualnej pracującej pod kontrolą VMware ESXi i spełnia następujące wymagania:
    a. umożliwia agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym;
    b. jest dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego;
    c. zapewnia interfejs, który może zostać dostosowany do wymagań użytkownika. W szczególności administrator posiada możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria;
    d. ma możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm;
    e. ma możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Ma możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami;
    f. zapewnia zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany;

g. zapewnia funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS;
h. zapewnia grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją;
i. ma możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak, aby ułatwić czynności monitorowania sieci;
j. daje możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszenie reakcji na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta;
k. ma możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora;
l. zapewnia możliwość automatycznego uaktualniania reguł publikowanych przez Producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS;
m. ma możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń bezpieczeństwa, jak i platformy zarządzającej;
n. zapewnia funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia, poprzez odpowiedzi, aż do rozwiązania;
o. zapewnia możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu;
p. zapewnia możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP;
q. zapewnia możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze;
r. zapewnia szerokie możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika;
s. zapewnia informowanie o zagrożeniach poprzez:
    i. wysłanie e-maila,
    ii. wysłanie trap SNMP,
    iii. przesłanie informacji do serwera Syslog,
    iv. uruchomienie skryptu użytkownika,
    v. wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze;
t. posiada zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy:
    i. aktualnego stanu danego urządzenia,
    ii. podglądu historii dostępnych zasobów,
    iii. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing);
u. ma możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym;
v. ma możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
    i. dozwolone porty i protokoły,
    ii. dozwolone aplikacje według różnych kategorii,
    iii. dozwolone kategorie stron internetowych (URL filtering),
    iv. dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej,

v. sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne;

w. w ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie ma możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji jest zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia.

2. Oprogramowanie musi być objęte 3-letnim serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wsparcia telefonicznego i mailowego w zakresie konfiguracji oprogramowania oraz do aktualizacji oprogramowania. Dostęp do aktualizacji sygnatur IPS, mechanizmów filtrowania webowego i aktualizacji filtrów antymalware'owych przez okres 3 lat.

<u>Specyfikacja punktów dostępowych typu 1 - ilość: 31 sztuk.</u>

Punkt dostępu bezprzewodowego:

1. Obsługa standardów 802.11a/b/g/n/ac/ax:
    a. obsługa MU-MIMO – min. 4x4:4;
    b. obsługa kanałów 20, 40 MHz dla 802.11n;
    c. obsługa kanałów 20, 40, 80, 160 MHz dla 802.11ac/ax;
    d. obsługa prędkości PHY do 3,47 Gbps (ac);
    e. obsługa prędkośći PHY do 5,38 Gbps (ax);
    f. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx);
    g. obsługa beamforming dla klientów 802.11a/g/n/ac/ax;
    h. obsługa MRC (Maximal Ratio Combining).
2. Obsługa szerokiego zakresu kanałów radiowych:
    a. dla zakresu 2.4 GHz: min. 13 kanałów;
    b. dla zakresu 5GHz (UNII-1 i UNII-2): min. 8 kanałów;
    c. dla zakresu 5GHz (extended UNII-2): min. 8 kanałów.
3. Konfigurowalna moc nadajnika:
    a. dla zakresu 2.4 GHz: do 100 mW;
    b. dla zakresu 5GHz (UNII-1 i UNII-2): do 200 mW;
    c. dla zakresu 5GHz (extended UNII-2): do 200 mW.
4. Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
    a. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN;
    b. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany);
    c. obsługa min. 16 BSSID;
    d. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID;
    e. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w;
    f. obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN);

g. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników;
h. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6;
i. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego (wykrywanie obcych punktów dostępowych i klientów WLAN, wireless IDS);
j. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h;
k. obsługa IPv6;
l. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r;
m. obsługa mechanizmów QoS:
    i. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik;
    ii. obsługa WMM, TSPEC, U-APSD;
n. współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne;
o. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM;
p. wsparcie IEEE 802.11i, WPA2, WPA;
q. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP).

5. Interfejs MultiGigabit Ethernet (100/1000/2500) - IEEE 802.3bz.
6. Interfejs konsoli RJ45.
7. Port USB 2.0 (funkcjonalność dostępna w przyszłych wersjach oprogramowania).
8. 2 GB RAM, 1 GB Flash.
9. Zasilanie przez PoE+ (IEEE 802.3at).
10. Anteny zintegrowane o zysku:
    a. dla modułu 2,4 GHz 3 dBi,
    b. dla modułu 5 GHz: min. 4dBi.
11. Obudowa przystosowana do pracy w zakresie temperatur 0 – 50oC.
12. Diodowa sygnalizacja stanu urządzenia z możliwością dezaktywacji.
13. Wbudowane radio Bluetooth Low Energy (BLE) 5.0.
14. Urządzenie musi zostać dostarczone z licencją, która umożliwia podłączenie go do systemu centralnego zarządzania Cisco Prime, jaki działa u zamawiającego.

Zamawiający wymaga dostarczenia licencji do kontrolera. Ilość licencji musi być równa licznie dostarczanych punktów dostępowych.

Urządzenie objęte 12 miesięcznym serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.

<u>Specyfikacja punktów dostępowych typu 2 - ilość: 31 sztuk.</u>

Punkt dostępu bezprzewodowego:

1. Obsługa standardów IEEE 802.11a/b/g/n/ac/ax:
    a. obsługa OFDMA (uplink/downlink), TWT, BSS Coloring;
    b. obsługa MU-MIMO – min. 2x2:2;

c. obsługa kanałów 20, 40 MHz dla 802.11n;
d. obsługa kanałów 20, 40, 80 MHz dla 802.11ac/ax;
e. obsługa prędkości PHY do 866,7 Mbps (ac);
f. obsługa prędkośći PHY do 1,488 Gbps (ax);
g. obsługa agregacji ramek A-MPDU (Tx/Rx), A-MSDU (Tx/Rx);
h. obsługa beamforming 802.11ac/ax;
i. obsługa MRC (Maximal Ratio Combining).

2. Konfigurowalna moc nadajnika:
   a. dla zakresu 2.4 GHz: do 100 mW,
   b. dla zakresu 5GHz: do 100 mW.
3. Zgodność z protokołem CAPWAP (RFC 5415), zarządzanie przez kontroler WLAN z funkcjonalnościami:
   a. automatyczne wykrywanie kontrolera i konfiguracja poprzez sieć LAN;
   b. optymalizacja wykorzystania pasma radiowego (ograniczanie wpływu zakłóceń, kontrola mocy, dobór kanałów, reakcja na zmiany);
   c. obsługa min. 16 BSSID;
   d. definiowanie polityk bezpieczeństwa (per SSID) z możliwością rozgłaszania lub ukrycia poszczególnych SSID;
   e. uwierzytelnianie ruchu kontrolnego 802.11 (z możliwością wykrywania użytkowników podszywających się pod punkty dostępowe) – IEEE 802.11w;
   f. obsługa trybów pracy Split-MAC (tunelowanie ruchu klientów do kontrolera i centralne terminowanie do sieci LAN) oraz Local-MAC (lokalne terminowanie ruchu do sieci LAN);
   g. możliwość pracy po utracie połączenia z kontrolerem, z lokalnym przełączaniem ruchu do sieci LAN – przełączenie nie może powodować zerwania sesji użytkowników;
   h. obsługa tunelowania ruchu od AP do routera za pomocą EoGREv4 oraz EoGREv6
   i. jednoczesna obsługa transferu danych użytkowników końcowych oraz monitorowania pasma radiowego pod kątem zagrożeń bezpieczeństwa (wykrywanie obcych AP oraz klientów);
   j. obsługa Dynamic Frequency Selection (DFS) i Transmit Power Control (TPC) zgodnie z 802.11h;
   k. obsługa IPv6;
   l. obsługa szybkiego roamingu użytkowników pomiędzy punktami dostępowymi – IEEE 802.11r ;
   m. obsługa mechanizmów QoS:
      i. ograniczanie ruchu do użytkownika, z możliwością konfiguracji per użytkownik, per SSID;
      ii. obsługa WMM, TSPEC, U-APSD;
   n. współpraca z urządzeniami i oprogramowaniem realizującym usługi lokalizacyjne;
   o. wsparcie dla metod EAP: EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-GTC, EAP-SIM;
   p. obsługa modyfikacji autoryzacji w wyniku uwierzytelnienia AAA (RADIUS): ustawienie parametrów takich jak: VLAN, lista kontroli dostępu, ustawienia QoS, czas sesji, profil aplikacyjny, kontrakt rate-limiting;
   q. wsparcie IEEE 802.11i, WPA2, WPA3;
   r. wbudowany suplikant 802.1X – możliwość uwierzytelnienia AP do infrastruktury przewodowej (wsparcie dla EAP-FAST, EAP-TLS, EAP-PEAP);
   s. obsługa szyfrowania ruchu kontrolnego i danych między AP a kontrolerem za pomocą DTLS;

t. obsługa blokowania ruchu Peer-to-Peer;
u. obsługa mechanizmów zapewniających autentyczność uruchamianego oprogramowania oraz hardware urządzenia w tym: cyfrowy podpis oprogramowania, bezpieczna sekwencja uruchamiania, sprzętowy układ umożliwiający sprawdzenie autentyczności hardware urządzenia;
v. obsługa polityki kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa (secure tag) za pomocą mechanizmu out-of-band, który przekazuje za pośrednictwem kontrolera do AP mapowania aktualnych adresów IP stacji i przypisanego im znacznika bezpieczeństwa.

4. Interfejs GigabitEthernet (10/100/1000).
5. Interfejs konsoli RJ45.
6. Zabezpieczenie typu Kensington przed kradzieżą/demontażem.
7. Pełna funkcjonalność AP przy zasilaniu przez PoE.
8. Anteny zintegrowane o zysku min. 4 dBi dla pasma 2,4 GHz oraz 5 dBi dla pasma 5 GHz.
9. Obudowa przystosowana do pracy w zakresie temperatur 0 – 50oC.
10. Diodowa sygnalizacja stanu urządzenia z możliwością dezaktywacji.
11. Wbudowane radio Bluetooth Low Energy (BLE) 5.
12. Urządzenie musi zostać dostarczone z licencją, która umożliwia podłączenie go do systemu centralnego zarządzania Cisco Prime, jaki działa u zamawiającego.

Zamawiający wymaga dostarczenia licencji do kontrolera. Ilość licencji musi być równa licznie dostarczanych punktów dostępowych.

Urządzenie objęte 12 miesięcznym serwisem świadczonym bezpośrednio przez Producenta w reżimie 8x5xNBD uprawniającym do wymiany sprzętu w przypadku zdiagnozowania awarii urządzenia, wsparcia telefonicznego i mailowego w zakresie konfiguracji urządzenia oraz do aktualizacji oprogramowania urządzenia.

Specyfikacja kontrolera punktów dostępowych – ilość: 1 sztuka.

1. Urządzenie umożliwiające centralną kontrolę punktów dostępu bezprzewodowego:
    a. zarządzanie politykami bezpieczeństwa;
    b. wykrywanie zagrożeń w sieci bezprzewodowej;
    c. zarządzanie pasmem radiowym;
    d. zarządzanie mobilnością;
    e. zarządzanie jakością transmisji;
    f. zgodnie z protokołem CAPWAP (RFC 5415).
2. Obsługa 6000 punktów dostępowych.
3. Wspierane tryby uruchomienia:
    a. na platformach wirtualizacyjnych (chmura prywatna): ESXi, KVM, Hyper-V,
    b. w chmurze publicznej: AWS (Amazon Web Services), GCP (Google Cloud Platform).
4. Wydajność centralnego przełączania ruchu 1,5 Gbps (dotyczy platform ESXi, KVM, HyperV), przy zastosowaniu SR-IOV wydajność do 5Gbps (dotyczy platform ESXi, KVM).
5. W przypadku uruchomienia na AWS i GCP: wsparcie dla lokalnego przełączania ruchu do sieci przewodowej na AP (bez obsługi tunelowania ruchu do kontrolera oraz obsługi usług wymagających ruchu do kontrolera).
6. Obsługa 64000 klientów sieci bezprzewodowej.
7. Zarządzanie pasmem radiowym punktów dostępowych:

a. automatyczna adaptacja do zmian w czasie rzeczywistym;
b. optymalizacja mocy punktów dostępowych (wykrywanie i eliminacja obszarów bez pokrycia);
c. dynamiczne przydzielanie kanałów radiowych;
d. wykrywanie, eliminacja i unikanie interferencji;
e. równoważenie obciążenia punktów dostępowych;
f. tworzenie profili RF (parametry konfiguracyjne) dla grup punktów dostępowych;
g. automatyczna dystrybucja klientów pomiędzy punkty dostępowe;
h. mechanizmy wspomagające priorytetyzację zakresu 5GHz dla klientów dwuzakresowych;
i. dynamiczny wybór szerokości kanału (20, 40, 80, 160 MHz) w paśmie 5 GHz w oparciu o parametry radiowe.

8. Mapowanie SSID do segmentów VLAN w sieci przewodowej:
   a. 1:1;
   b. 1:n (SSID mapowane do wielu segmentów VLAN, ruch użytkowników rozkładany pomiędzy segmenty);
   c. możliwość tunelowania ruchu klientów do kontrolera (dotyczy platform ESXi, KVM, HyperV) oraz lokalnego terminowania do sieci przewodowej na poziomie AP (konfigurowane per SSID).
9. Obsługa sieci kratowych (dotyczy platform ESXi, KVM, HyperV):
   a. komunikacja między punktami dostępowymi bez medium kablowego;
   b. separacja trybu pracy poszczególnych zakresów radiowych (jeden dedykowany do obsługi klientów, drugi do komunikacji między punktami dostępowymi);
   c. automatyczne formowanie sieci kratowej między punktami dostępowymi (optymalizacja tras z uwzględnieniem parametrów jakościowych połączenia, minimalizacja interferencji z możliwością awaryjnego przełączenia na inne pasmo);
   d. automatyczne włączanie nowych punktów do sieci (bez konieczności konfiguracji punktów dostępowych w miejscu instalacji);
   e. autoryzacja punktów dostępowych w oparciu o certyfikaty, adresy MAC.
10. Obsługa mechanizmów bezpieczeństwa:
    a. 802.11i, WPA3, WPA2, WPA;
    b. 802.1x z EAP (m.in. PEAP, EAP-TLS, EAP-FAST);
    c. obsługa serwerów autoryzacyjnych – RADIUS, TACACS+, wbudowana lokalna baza użytkowników;
    d. kreowanie różnych polityk bezpieczeństwa w ramach pojedynczego SSID;
    e. obsługa profilowania użytkowników:
       i. przydział sieci VLAN,
       ii. przydział list kontroli dostępu (ACL);
    f. uwierzytelnianie (podpis cyfrowy) ramek zarządzania 802.11 – wsparcie dla IEEE 802.11w;
    g. uwierzytelnianie punktów dostępowych w oparciu o certyfikaty;
    h. obsługa list kontroli dostępu (ACL);
    i. obsługa list kontroli dostępu opartych o nazwy domenowe (DNS ACL);
    j. obsługa indywidualnych kluczy PSK per klient dla sieci SSID, która nie wykorzystuje mechanizmów 802.1X;
    k. wykrywanie i dezaktywacja obcych punktów dostępowych;

l. możliwość budowania reguł klasyfikacji obcych punktów dostępowych w oparciu o nazwę SSID, wybrany ciąg znaków w SSID, siłę sygnału RSSI, minimalną ilość podłączonych urządzeń;
m. ochrona kryptograficzna (DTLS) ruchu użytkowników (dotyczy platform ESXi, KVM, HyperV) oraz ruchu kontrolnego CAPWAP;
n. DHCP proxy, wsparcie dla DHCP Option 82;
o. obsługa polityk kontroli ruchu i segmentacji logicznej w oparciu o znaczniki bezpieczeństwa z wykorzystaniem mechanizmu out-of-band, który przekazuje mapowania aktualnych adresów IP stacji i znacznika (dotyczy platform ESXi, KVM, HyperV).

11. Zabezpieczenia zapewniające autentyczność sprzętową oraz software'ową:
    a. kryptograficzne podpisywanie obrazów oprogramowania,
    b. bezpieczny proces sekwencji startowej (bootowanie) elementów systemowych.
12. Profilowanie urządzeń podłączających się do sieci bezprzewodowej w oparciu o informacje z HTTP, DHCP oraz przydzielanie na tej podstawie odpowiednich uprawnień i parametrów dostępowych, takich jak: VLAN, polityka QoS, lista kontroli dostępu, czas trwania sesji.
13. Obsługa ruchu unicast IPv4 i IPv6.
14. Zgodność z funkcjonalnościami IPv6 pod kątem RFC: 4191, 6980, 8200, 8201 (dotyczy platform ESXi, KVM, HyperV).
15. Obsługa ruchu multicast IPv4 i IPv6 (dotyczy platform ESXi, KVM, HyperV).
16. IGMP / MLD snooping.
17. Optymalizacja dystrybucji ruchu multicast w sieci przewodowej (między kontrolerem, a punktem dostępowym).
18. Obsługa konwersji ruchu multicast do unicast.
19. Obsługa mobilności (roaming-u) użytkowników (IPv4 i IPv6, w ramach i pomiędzy kontrolerami (dotyczy platform ESXi, KVM, HyperV).
20. Obsługa mechanizmów wspomagania roamingu: IEEE 802.11r oraz 802.11k.
21. Obsługa mechanizmów QoS:
    a. 802.1p;
    b. WMM, TSpec, U-APSD;
    c. ograniczanie pasma per użytkownik;
    d. Call Admission Control, SIP CAC, Call Snooping;
    e. równomierna obsługa klientów sieci bezprzewodowej w oparciu o utylizację czasu antenowego;
    f. kontrola przydziału czasu antenowego (od AP do klienta mobilnego) dla danego SSID;
    g. zbiór wbudowanych profili do automatycznej konfiguracji ustawień QoS.
22. Analiza ruchu przechodzącego przez kontroler pozwalająca na identyfikację oraz klasyfikację na poziomie aplikacji (warstwa 7); obsługa markowania, limitowania lub odrzucania ruchu; rozpoznawanie ponad 1000 aplikacji; współpraca z serwerami autoryzacyjnymi w celu przypisania odpowiednich polityk kontroli ruchu aplikacji per użytkownik/grupa użytkowników (dotyczy platform ESXi, KVM, HyperV).
23. Obsługa protokołu Bonjour poprzez wbudowany mDNS (multicast DNS) Gateway, zbierający ogłoszenia o dostępności danych usług i odpowiadający na zapytania klientów (dotyczy platform ESXi, KVM, HyperV).
24. Obsługa dostępu gościnnego (IPv4 i IPv6):
    a. przekierowanie użytkowników do strony logowania na kontrolerze (z możliwością personalizacji strony);
    b. przekierowanie użytkowników do strony logowania na zewnętrznym serwerze;

c. obsługa kreowania użytkowników za pomocą dedykowanego portalu WWW (działającego na kontrolerze) z określeniem czasu ważności konta;
d. obsługa konfiguracji jako dedykowany kontroler do obsługi ruchu gości – całość ruchu z SSID dostępu gościnnego zebranego na pozostałych kontrolerach musi być przesyłana do tego kontrolera w sposób zapewniający logiczną separację od ruchu wewnętrznego (dotyczy platform ESXi, KVM, HyperV).

25. Obsługa NTP (IPv4 oraz IPv6), możliwość ustawienia różnych serwerów NTP dla wybranych grup AP.
26. Możliwość definiowania polityk dostępu do sieci bezprzewodowej na podstawie czasu logowania (dni tygodnia, godziny).
27. Obsługa EoGRE w celu tunelowania ruchu z kontrolera do dedykowanego koncentratora (np. na routerze) (dotyczy platform ESXi, KVM, HyperV).
28. Wsparcie dla IEEE 802.11u.
29. Obsługa Hotspot 2.0 (dotyczy platform ESXi, KVM, HyperV).
30. Obsługa redundancji rozwiązania (N+1).
31. Obsługa redundancji 1:1 (Active/Standby) zapewniającej (dotyczy platform ESXi, KVM, HyperV):
    a. utrzymanie sesji punktów dostępowych oraz urządzeń mobilnych na wypadek awarii aktywnego kontrolera,
    b. synchronizację konfiguracji oraz informacji o użytkownikach sieci bezprzewodowej.
32. Zarządzanie przez HTTPS, SNMP, SSH, NETCONF, wirtualny port konsoli.
33. Obsługa logowania Syslog, wsparcie dla IPSec w celu zabezpieczenia Syslog (dotyczy platform ESXi, KVM, HyperV).
34. Obsługa API: wsparcie NETCONF (RFC4741 oraz RFC4742) oraz modeli YANGa (RFC6020).
35. Wbudowana baza najlepszych praktyk (best practice) konfiguracji z możliwością łatwej ich implementacji (lub cofnięcia zmian) jednym przyciskiem.
36. Urządzenie musi zostać dostarczone z licencją, która umożliwia podłączenie go do systemu centralnego zarządzania Cisco Prime, jaki działa u zamawiającego.
37. Urządzenie wyposażone jest w licencje subskrypcyjną na wymagane funkcjonalności na okres 3 lat.
38. Urządzenie dostarczone w formie maszyny wirtualnej na platformę: ESXi.

Część 2: zakup, montaż i konfiguracja zasobów dyskowych.

1. Specyfikacja obudowy dla urządzenia pamięci masowej typu rack:

a) Obudowa musi zawierać minimum 12 slotów przeznaczonych na dysk twardy 3.5" hot-swappable SAS/SATA oraz minimum 2 sloty przeznaczone na dysk hot-swappable typu SAS, SATA lub SSD umieszone w tylnej części obudowy urządzenia pamięci masowej typu rack.

b) Obudowa musi posiadać redundantne zasilanie typu hot-plug. Zaoferowane zasilacze urządzenia pamięci masowej typu rack nie mogą być gorszej klasy niż Platinum, pracującej o częstotliwości 50/60Hz, wspierające napięcie 100-240V AC.

c) Oferowane zasilacze do urządzenia pamięci masowej typu rack muszą być dedykowane przez producenta oraz zostać dostarczone wraz z dwoma fabrycznie nowymi kablami zasilającymi typu C13 – C14, o długości nie krótszej niż 2 metry.

d) Obudowa zamontowana w szafie typu rack nie może przekraczać wysokości 2U.

d) Zaoferowana obudowa musi posiadać ramkę zabezpieczającą dyski twarde zamawiającego przed nieautoryzowanym wyciągnięciem, znajdujące się z przodu obudowy. Ramka zabezpieczająca musi oferować umożliwienie jej zablokowania dedykowanym przez producenta kluczykiem - dostarczonym wraz z urządzeniem pamięci masowej typu rack.

2. Specyfikacja urządzenia pamięci masowej typu rack:

a) Zaproponowane procesory muszą być dedykowane do pracy w serwerach wieloprocesorowych, które z oferowanym urządzeniem umożliwiają osiągnięcie dla dwóch procesorów wyniku minimum 127 w teście SPECrate2017_int_base dostępnym na stronie www.spec.org.

b) Serwer musi posiadać dwa procesory o minimalnym taktowaniu 2,40GHz z liczbą rdzeni 10 oraz liczbą wątków 20, oferując pamięć cache 13,75 MB każdy.

c) Pamięć operacyjna: wykorzystane kości pamięci operacyjnej RAM nie mogą być gorsze niż DDR4 3200MT/s w modułach dwubankowych z zabezpieczeniem ECC oraz typem DIMM typu RDIMM. Pamięć operacyjna RAM musi dostarczać funkcjonalność Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling.

d) Łączna pamięć operacyjna w oferowanym urządzeniu pamięci masowej nie może być mniejsza niż 64GB ze specyfikacją nie gorszą niż w punkcie 2-c.

e) Urządzenia pamięci masowej powinny zawierać dodatkowe niewypełnione złącza pamięci pozwalające na jej rozszerzenie do co najmniej 256GB bez konieczności wyciągania zainstalowanej już pamięci.

f) Oferowane urządzenie musi posiadać fizyczną kartę RAID umożliwiającą utworzenie RAID typu 0, 1, 5, 6, 10, 50 ,60, wspierające interfejsy 12Gb/s SAS, 6Gb/s SAS/SATA wraz z Cache Memory o wielkości nie gorszej niż 8GB.

g) Zaoferowane urządzenie musi zostać wyposażone w minimum cztery porty 1 GbE Base-T oraz minimum dwa porty 10G SFP+.

h) Urządzenie pamięci masowej musi mieć możliwość zdalnego zarządzania oraz dostęp do wirtualnej myszki, klawiatury, wideo (KVM) przez dedykowany port zarządzający będącym osobnym portem, nie będący jednocześnie portem wliczonym w punkt 2-g.

i) Zarządzanie urządzeniem pamięci masowej oraz konfiguracja musi być możliwa przez interfejs WWW.

j) Urządzenie pamięci masowej musi posiadać minimum dwa porty USB3.0.

k) Urządzenie pamięci masowej musi posiadać wbudowany port VGA, Serial oraz być wyposażone w specjalne diody LED znajdujące się na przodzie oraz tyle urządzenia które umożliwi Zamawiającemu prostą i szybką lokalizacje bądź identyfikacje w szafie rack zamawiającego.

l) Obsługa dysków. Urządzenie pamięci masowej dostarczone musi zostać z:

- 2 dyskami typu SSD 2.5" o pojemności nie mniejszej 480GB i interfejsie SATA3 z DWPD (Drive Writes Per Day) nie gorszym niż na poziomie 1 DWPD (Drive Writes Per Day) zamontowanymi w tylnej części urządzenia.

- 6 dyskami SAS 12Gb/s o prędkości talerzowej nie wolniejszej niż 7200 obr./min z obsługą formatu 512e oraz pojemnością nie mniejszą niż 8TB.

m) Temperatura robocza powinna wynosić 10°C ~ 35°C (50°F ~ 95°F).

n) Oferowane urządzenie musi zostać wyposażone w wbudowany moduł TPM 2.0 (Trusted Platform Module 2.0) oraz wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.

o) Urządzenie musi posiadać zintegrowaną kartę graficzną umożliwiająca wyświetlenie rozdzielczości min. 1920x1200.

3. Urządzenie musi być przeznaczone do montażu w szafie typu rack oraz musi posiadać wszystkie elementy niezbędne do montażu w szafie rack wraz z dedykowanym wysięgnikiem do mocowania kabli.

4. Gwarancja na urządzenie pamięci masowej wraz z dyskami nie może być krótsza niż trzy lata. Musi być realizowana w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia oraz umożliwiać zgłaszanie awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Proponowane urządzenie musi oferować możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć wraz z dostawą. Wymagane jest dołączenie do oferty oświadczenie Producenta potwierdzające, że serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

5. Dostarczone urządzenie pamięci masowej musi pochodzić z oficjalnego kanału dystrybucyjnego producenta w Polsce i tym samym zapewniać realizację uprawnień gwarancyjnych.

6. Oferowane urządzenie pamięci masowej musi zapewniać wsparcie dla systemów operacyjnych taki jak SUSE Linux Enterprise Server, Canonical Ubuntu LTS, Citrix XenServer, Red Hat Enterprise Linux, VMware ESXi, a w szczególności Microsoft Windows Server z Hyper-V. Oferowane urządzenie musi również znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2 x64, Microsoft Windows 2016, Microsoft Windows 2019.

Cześć 3: zakup, montaż i konfiguracja urządzeń oraz oprogramowania do wykonywania kopii zapasowych offline.

1. Specyfikacja biblioteki taśmowej typu rack:

a) Biblioteka taśmowa musi umożliwiać montaż w szafie rack i nie przekraczać wysokości 1U, wraz z urządzeniem. Wykonawca zobowiązany jest dostarczyć dedykowany przez producenta zestaw niezbędny do montażu urządzenia w szafie rack Zamawiającego.

b) Zaoferowana biblioteka musi wspierać taśmy LTO-8 dostarczające natywnie 12TB oraz oferujące uzyskanie do 30TB poprzez wykorzystanie kompresji.

c) Biblioteka musi umożliwiać wykonywanie kompresji wykonując ją per kartridż w stosunku 2.5:1.

d) Oferowana biblioteka musi posiadać minimum jeden napęd taśmowy oraz musi umożliwiać instalację w dedykowanym do tego magazynie minimum dla 9 taśm LTO-8 Half-High,

e) Biblioteka taśmowa musi umożliwiać data transfer rate dla pojedynczej taśmy nie gorszy niż do 300 Mbps przy natywnym wykorzystaniu taśmy LTO-8.

f) Zaoferowana biblioteka musi oferować możliwość przechowywania danych:

- 108TB przy natywnym wykorzystaniu taśm LTO-8,

- 270TB przy wykorzystaniu kompresji 2.5:1,

g) Biblioteka taśmowa musi posiadać dedykowany port zarządzający, wykorzystujący port sieciowy Base-T Ethernet, oraz port umożliwiający połączenie z urządzeniem typu serwer Zamawiającego - typu SAS o prędkości nie gorszej niż 6 Gbps.

h) Oferowane urządzenie musi wspierać zasilanie 110/220 volt AC.

i) Oferowana biblioteka musi być wyposażona w panel operacyjny oferujący monochromatyczny ekran LCD wraz z odpowiednimi przyciskami umożliwiającymi wyświetlanie komend lub wykonywanie poleceń na urządzeniu.

j) Biblioteka taśmowa musi posiadać diody LED na froncie urządzenia informujące:

- o stanie zasilania urządzenia (Power ON/OFF),

- o wymaganiu czyszczenia napędu taśmowego,

- o poprawności zainstalowanego kartridża,

- o pojawieniu się błędu w systemie / urządzeniu.

k) Biblioteka musi umożliwiać zarządzanie urządzeniem przy wykorzystaniu protokołu http, który musi dostarczać możliwość:

- wyświetlenia statusu urządzenia i kondycji,

- wyświetlenia wersji firmware dla bilbioteki i taśm,

- konfiguracji dostępu dla użytkowników oraz ich kont,

- definiowania polityki złożoności hasła,

- konfiguracji sieci umożliwiając wykorzystanie dynamiczne i statyczne adresacji IPv4 oraz IPv6,

- konfiguracji usługi czasu przy wykorzystaniu serwerów NTP Zamawiającego,

- konfigurację szyfrowania, którego celem będzie zabezpieczenie danych znajdujących się na taśmach,

- konfigurację powiadomień realizowanych poprzez protokoły zarówno SMTP oraz SNMP.

i) Oferowane urządzenie musi posiadać dokumentację w języku angielskim, w której zawarte zostały informacje dotycząca:

- instalacji wraz z konfiguracją rozruchową,

- obsługi urządzenia,

- podstawowego troubleshootingu urządzenia.

j) Zaoferowany producent urządzenia musi wspierać oprogramowanie kopii zapasowej Zamawiającego tj. Veeam Backup & Replication.

k) Urządzenie nie powinno generować poziomu hałasu większego niż 6.8 dBA, a w czasie bezczynności 6.6 dBA.

l) Temperatura pracy urządzenia musi wynosić od 10 do 38 stopni Celsjusza (od 50 do 100 stopni Fahrenheita).

m) Biblioteka taśmowa musi zapewniać wsparcie i umożliwiać wykorzystanie taśm jedno oraz wielokrotnego zapisu.

2.Dostarczona biblioteka taśmowa musi pochodzić z oficjalnego kanału dystrybucyjnego producenta w Polsce i być dostarczona przez oficjalnego partnera, który tym samym zapewnia realizację uprawnień gwarancyjnych. W przypadku wątpliwości Zamawiający zastrzega sobie prawo do otrzymania wyjaśnień w celu ustalenia prawidłowości realizacji zamówienia.

3. Zaoferowane urządzenie musi posiadać wsparcie dla systemów operacyjnych Red Hat Enterprise Linux, Ubuntu, Novell SUSE Linux Enterprise, a w szczególności Microsoft Windows Server 2016, 2019 lub nowszy.

4. Wraz z urządzeniem taśmowym Zamawiający wymaga dostarczenia:

- ośmiu taśm LTO-8 o natywnej pojemności 12TB wyprodukowanych przez tego samego producenta co oferowane urządzenie,

- jednej taśmy czyszczącej wyprodukowanej przez tego samego producenta co oferowane urządzenie.

5. Zamawiający posiada już w swojej infrastrukturze serwer Supermicro oparty o platformę Supermicro SSG-6029P-E1CR12T. Wykonawca musi dostarczyć kompatybilną kartę HBA SAS z serwerem Zamawiającego, która posiadać będzie minimum dwa zewnętrze złącza mini-SAS o przepustowości 12 Gb/s. Karta musi umożliwiać montaż full oraz low profile.

6. Dostarczona biblioteka taśmowa wraz z dedykowaną kartą SAS HBA do posiadanego przez Zamawiającego serwera musi zostać dostarczona z kompatybilnym dla obu urządzeń dedykowanym do tych celów kablem połączeniowym mini SAS o długości nie krótszej niż 1m.

7. Dostarczona biblioteka taśmowa musi posiadać wsparcie producenta na okres nie krótszy niż 36 miesięcy i umożliwiać zgłaszanie awarii przez 5 dni w roboczych (pn-pt), przez 11 godzin (5x11 on-site).

Część 4: zakup, montaż i konfiguracja cyfrowych urządzeń telewizji dozorowej oraz zakup, montaż i konfiguracja systemu SSWiN, KD.

Nazwa przedmiotu	
Kamera monitoringu przemysłowego	
Typ	IP
Przeznaczenie	zewnętrzna/wewnętrzna
design	sześcian
Typ mocowania	ściana/sufit/słup
Technologia łączności	przewodowa sieć LAN
Tryb nocny	Tak
Technologia trybu nocnego	diody IR z mechanicznym filtrem IR
Rozdzielczość	min. 1080p Full HD (1920x1080)
Kompresja wideo	H.264
Suma megapikseli	min. 2 MP
Ilość klatek	max. 25 fps
Długość stalej ogniskowej	min. 3,4 mm
Wielkość czujnika CCD	min. 25,4 / 2,7 mm (1 / 2.7")
Wbudowany mikrofon	Tak
Kąt widzenia (poziomy) bez korekcji	min. 87,4°
Kąt widzenia (pionowy) bez korekcji	min. 47°
Kąt widzenia, przekątna bez korekcji	min. 104°
Kąt widzenia (poziomy) z korekcją	min. 80°
Kąt widzenia (pionowy) z korekcją	min. 46°
Kąt widzenia, przekątna z korekcją	min. 92°
Wbudowany mikrofon	Tak
Zasilanie	802.3af PoE
Zużycie mocy	max. 4W
Zakres pracy w temp.	min. -20 °C, max. 50 °C
Zakres wilgotności względnej	min. 20%, max. 90%
Szerokość produktu	max. 48 mm
Głębokość produktu	max. 48 mm
Wysokość produktu	max. 107,5 mm
Waga produktu bez opakowania	max. 170 g
Współpraca z aplikacjami mobilnymi	UniFi Protect, iOS i Android
Ilość	**48**
Model wzorcowy	**Ubiquiti Networks G3-FLEX, lub równoważny**

Nazwa przedmiotu	
Kamera monitoringu przemysłowego	
Typ	IP
Przeznaczenie	zewnętrzna/wewnętrzna

Typ mocowania	ściana/sufit/słup
Materiał obudowy	alumienium/poliwęglan
Technologia łączności	przewodowa sieć LAN
Tryb nocny	Tak
Technologia trybu nocnego	diody IR z mechanicznym filtrem IR Cut
Rozdzielczość	min. 1080p Full HD (1920x1080)
Kompresja wideo	H.264
Suma megapikseli	min. 4 MP
Ilość klatek	max. 30 fps
Długość stalej ogniskowej	min. 3,6 mm
Wielkość czujnika CCD	min. 25,4 / 3 mm (1 / 3")
Wbudowany mikrofon	Tak
Kąt widzenia (poziomy) bez korekcji	min. 85°
Kąt widzenia (pionowy) bez korekcji	min. 44,8°
Kąt widzenia, przekątna bez korekcji	min. 98,1°
Kąt widzenia (poziomy) z korekcją	min. 72°
Kąt widzenia (pionowy) z korekcją	min. 42,9°
Kąt widzenia, przekątna z korekcją	min. 80,4°
Wbudowany mikrofon	Tak
Zasilanie	802.3af PoE
Zużycie mocy standalone	max. 4W
Zużycie mocy z IR	max. 9W
Zakres pracy w temp.	min. -20 °C, max. 50 °C
Zakres wilgotności względnej	min. 20%, max. 90%
Średnica produktu	max. 75 mm
Długość produktu	max. 140 mm
Waga produktu bez opakowania	max. 300 g
Współpraca z aplikacjami mobilnymi	UniFi Protect, iOS i Android
Ilość	**14**
Model wzorcowy	**Ubiquiti Networks G3-BULLET, lub równoważny**

Nazwa przedmiotu	
Kontroler sieciowy	
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
Standardy komunikacyjne	IEEE 802.3af
Przycisk reset	Tak
Ilość portów Ethernet LAN (RJ-45)	min. 1
Materiał obudowy	aluminium
Szerokość produktu	max. 131,2 mm
Głębokość produktu	max. 27,1 mm

Wysokość produktu	max. 134,2 mm
Waga produktu bez opakowania (netto)	max. 582 g
Obsługa PoE	Tak
Zakres temperatur (eksploatacja)	min. 0°C, max. 35 °C
Zakres wilgotności względnej	min. 20, max. 80%
Procesor wbudowany	Tak
Wewnętrzna pamięć masowa	2.5" SATA HDD
Pojemność dysku	min. 1 TB
eMMC	Tak
Pojemność pamięci eMMC	min. 32 GB
CPU Mark in PassMark Software	min. 1796
Ilość rdzeni procesora	min. 8
Taktowanie procesora	min. 1,8 MHz
Pamięć RAM	min. 3GB RAM
Zasilanie	Standard 802.3af PoE i Quick Charge 2.0/3.0 Power Adapter (9VDC, 2A)
Zakres napięcia	Standard 802.3af PoE lub 9VDC, 2A
Pobór mocy	max. 12,95W
Panel sterowania	Nie
Certyfikaty	CE, FCC, IC
Ilość	**3**
Model wzorcowy	**Ubiquiti Networks Cloud Key Gen2, lub równoważny**

Nazwa przedmiotu	
Dysk twardy	
Rodzaj dysku	wewnętrzny
Typ dysku	HDD
Format fizyczny	2,5"
Interfejs	min. SATA III
Pobór mocy w czasie pracy	max, 2,1 W
Pobór mocy standalone	max. 1,1 W
Pamięć podręczna	min. 128 MB
Pojemność	min. 4 TB, max. 5 TB
Przepustowość	min. 5Gb/s, max. 6 Gb/s
Ilość	**5**
Model wzorcowy	**HDD 2,5 Seagate BarraCuda ST5000LM000 5TB Sata 128MB, lub równoważny**

Nazwa przedmiotu	
Sieciowy rejestrator wideo	
Prędkość transferu danych przez Ethernet LAN	10,100,1000 Mbit/s
Ilość portów Ethernet LAN (RJ-45)	min. 1
Ilość gniazd na wkładki SFP	min. 1
Szerokość produktu	max. 442,2 mm
Głębokość produktu	max. 325 mm
Wysokość produktu	max. 43,7 mm
Waga produktu bez opakowania (netto)	max. 5,11 kg
Zużycie mocy	max. 100W
Pobór mocy	max. 75W
Napięcie wejściowe AC	100 - 240 V
Prąd wyjściowy	max. 2A
Częstotliwość wejściowa AC	50 - 60 Hz
Zakres temperatur (eksploatacja)	min. -5°C, max. 40 °C
Zakres wilgotności względnej	min. 5%, max. 95%
Procesor wbudowany	Tak
CPU Mark in PassMark Software	min. 1343
Ilość rdzeni procesora	min. 4
Taktowanie procesora	min. 1,7 MHz
Ilość obsługiwanych dysków	min. 4
Kompatybilonośc dysków twardych	2.5" lub 3,5" SATA HDD
Pamięć RAM	min. 4 GB
Usługa RAID	Tak
Obsługiwany RAID	1 i 5
Ochrona ESD/EMP	Tak
Certyfikaty	CE, FCC, IC
Ilość	**1**
Model wzorcowy	**Ubiquiti Networks UniFi Network Video Recorder (UNVR), lub równoważny**