Postępowanie ozn. ZP.272.2.2024

Realizacja w ramach umowy o powierzenie grantu o numerze:
FERC.02.02.-CS.01-001/23/0222/
FERC.02.02.-CS.01-001/23/2024

Fundusze Europejskie Na Rozwój Cyfrowy 2021-2027 (FERC)
Priorytet II: Zaawansowane usługi cyfrowe
Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa
Konkurs grantowy w ramach Projektu grantowego „**Cyberbezpieczny Samorząd**” o numerze FERC.02.02-CS.01-001/23

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA /minimalne wymagania Zamawiającego/ na DOSTAWĘ NA POTRZEBY STAROSTWA POWIATOWEGO W KOSZALINIE PRZEŁĄCZNIKÓW SIECIOWYCH WRAZ Z OPROGRAMOWANIEM DO ZARZĄDZANIA PRZEŁĄCZNIKAMI SIECIOWYMI

Przedmiot zamówienia stanowi dostawę na potrzeby Starostwa Powiatowego w Koszalinie 7 przełączników sieciowych spełniających wymagania określone przez Zamawiającego (2 przełączniki CORE oraz 5 przełączników dostępowych) wraz z oprogramowaniem do zarządzania przełącznikami sieciowymi.

Przedmiot zamówienia obejmuje również transport przełączników do Starostwa Powiatowego w Koszalinie oraz ich wniesienie do wskazanego pomieszczenia oraz wdrożenie przełączników i oprogramowania.

Przełączniki sieciowe muszą być fabrycznie nowe, wykonane z fabrycznie nowych elementów. Przedmiot zamówienia musi być wolny od wad prawnych oraz fizycznych.

Przełączniki sieciowe muszą spełniać następujące minimalne parametry i wymogi Zamawiającego:

1. Przełącznik CORE - 2 szt.

Lp.	Parametry wyposażenia
1.	Wysokość urządzenia 1U wraz z zestawem do montażu urządzenia w szafie serwerowej 19".
2.	Przełącznik posiadający minimum 24 porty 10GBase-X (SFP+).
3.	Przełącznik posiadający minimum 2 porty QSFP28 wraz z 2 przewodami umożliwiającymi wykonanie stack’u przełączników.
4.	Przełącznik posiadający miejsce na dodatkowy moduł mogący, w zależności od potrzeb, być obsadzonym: • 4 portami 1/10GBase-X (SFP+), • 4 portami 10/25GBase-X (SFP28).
5.	Architektura o wydajności przełączania min. 1080 Gb/s.

6.	Szybkość przełączania min. 800 milionów pakietów na sekundę.
7.	Wielkość tablicy MAC minimum 40k wpisów.
8.	Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management .
9.	Wbudowany port USB oraz port konsoli.
10.	Przełącznik musi posiadać wbudowane, redundantne zasilacze 230V AC o mocy minimalnej 250 W, do zasilaczy dołączone 2 przewody zasilające wraz z europejskimi przejściówkami.
11.	Obsługa sieci wirtualnych IEEE 802.1Q – min. 4094.
12.	Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
13.	Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym).
14.	Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora. System musi mieć możliwość dodania nowego modułu lub aktualizacji już zaimplementowanych bez konieczności restartu całego urządzenia.
15.	Możliwość monitorowania zajętości CPU.
16.	Routing statyczny.
17.	Obsługa routingu dynamicznego IPv4: • RIPv1/v2, • OSPFv2, BGP, IS-IS– jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
18.	Policy Based Routing dla IPv4.
19.	Tablica routing IPv4 minimum 15k wpisów.
20.	Obsługa routingu dynamicznego dla IPv6: • RIPng, • OSPFv3, BGP, IS-IS– jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
21.	Policy Based Routing dla IPv6.
22.	Tablica routing IPv6 minimum 7k wpisów.
23.	Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration).
24.	Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping.
25.	Obsługa protokołu PIM-SM.
26.	Obsługa Network Login: • IEEE 802.1x • Web-based Network Login • MAC based Network Login
27.	Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www).

28.	Obsługa wielu klientów (min. 12) Network Login na jednym porcie (Multiple supplicants).
29.	Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC.
30.	Przydział sieci VLAN, ACL/QoS podczas logowania Network Login.
31.	Musi działać w architekturze bezpieczeństwa opartej o role, zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma.
32.	Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie: • definicji sieci VLAN, • reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6, • realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6, • realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
33.	Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication.
34.	Bezpieczeństwo MAC adresów: • ograniczenie liczby MAC adresów na porcie, • zatrzaśnięcie MAC adresu na porcie, • możliwość wpisania statycznych MAC adresów na port/vlan, • możliwość wyłączenia MAC learning.
35.	Zabezpieczenie przełącznika przed atakami DoS: • Networks Ingress Filtering RFC 2267, • SYN Attack Protection, • Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania.
36.	Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika – wire-speed) .
37.	Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation.
38.	Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard.
39.	Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768) .
40.	Obsługa STP, RSTP, MSTP, PVST+.
41.	Obsługa protokołu MVRP.
42.	Obsługa EAPS (RFC 3619).
43.	Obsługa protokołu ERPS lub równoważnego oraz ITU G.8032.
44.	Obsługa Link Aggregation IEEE 802.3ad wraz z LACP.
45.	Obsługa IEEE 802.3ah Ethernet OAM.
46.	Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników.

Postępowanie ozn. ZP.272.2.2024

47.	Musi mieć możliwość zarządzania za pomocą SSH/Telnet, SNMP, oraz systemu zarządzania dostarczonego przez producenta .
48.	Zarządzanie przez SNMP v1/v2/v3.
49.	Obsługa SYSLOG z możliwością definiowania wielu serwerów.
50.	Sprzętowa obsługa sFlow lub protokołu równoważnego.
51.	Obsługa RMON (RFC 1757) i RMON2 (RFC 2021).
52.	Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych).
53.	Możliwość uruchamiania skryptów: • ręcznie, • o określonym czasie lub co wskazany okres, • na podstawie wpisów w logu systemowym.
54.	Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS.
55.	Obsługa Data Center Bridging: • Data Center Bridging Exchange Protocol (DCBx), • Priority Flow Control (PFC).
56.	Obsługa protokołu MACSEC (IEEE 802.1AE) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania.
57.	Usługi wirtualizacji warstwy L2 i L3: • Przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI. • Przełącznik musi zapewniać „multi-tennancy” dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to przypadek, w którym do przełącznika doprowadzone są nakładające się numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie. • Przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN). • Przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2. • Przełącznik musi umożliwiać obsługę usług multicast dla L2, jak i L3 bez konieczności używania protokołu PIM. • Przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej. • Przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.
58.	Wykonawca musi zapewnić **gwarancję producenta na okres 4 lat** uwzględniającą: • wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego po zgłoszeniu awarii przez Zamawiającego, • aktualizacje oprogramowania układowego (firmware), • dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.

59.	W ramach dostawy Wykonawca zobowiązuje się dostarczyć wkładki światłowodowe (minimum 32 sztuki) transceivery SFP+ SingleMode 10Gbps, 1310nm, duplex LC kompatybilne z dostarczanymi urządzeniami oraz 4 szt. transceivery SFP+ MultiMode 10Gbps OM3, 850nm, duplex LC kompatybilne z dostarczanymi urządzeniami.
60.	Urządzenia muszą mieć odblokowane wszystkie porty, jeżeli urządzenie wymaga zakupu dodatkowej licencji w celu umożliwienia korzystania ze wszystkich portów Wykonawca w ramach dostawy urządzeń dostarczy również licencję bezterminową pozwalającą na korzystanie ze wszystkich portów urządzenia.
61.	Urządzenia muszą być kompatybilne z posiadanym przez Zamawiającego rozwiązaniem NACVIEW w zakresie: - MAB (MAC Authentication Bypass), - CoA – obsługa polecenia zmiany autoryzacji RADIUS, - TACACS+ - funkcjonalność autoryzacji administratorów na urządzeniach sieciowych, - Multiautoryzacja – funkcjonalność autoryzowania urządzeń końcowych podłączonych do LAN za pośrednictwem przełącznika niezarządzalnego (Ethernet hub), - IEEE 802.1Q - obsługa vlanów, - IEEE 802.1x – uwierzytelnienie EAP, MAB – obsługa zewnętrznych serwerów RADIUS, - RFC 3576, RFC 5176 – obsługa CoA, - RFC 1157 (v.1), RFC 1441 (v.2), RFC 2570 (v.3) – obsługa monitoring.
62.	Wykonawca musi w ramach przedmiotu zamówienia wykonać wdrożenie w zakresie: uruchomienia, aktualizacji firmware, konfiguracji [połączenia] z posiadanym przez Zamawiającego systemem NACVIEW, konfiguracji VLANów.
63.	Do wykonania czynności opisanych w punkcie 62 Wykonawca musi dysponować minimum 2 osobami posiadającymi certyfikat “Certyfikowany inżynier NACVIEW” potwierdzający wiedzę i doświadczenie w instalacji, konfiguracji oraz wsparcia serwisowego.
64.	Urządzenia muszą być dostarczone w ramach produktów jednego producenta.

2. Przełączniki dostępowe – 5 szt.

Lp.	Parametry wyposażenia
1.	Wysokość urządzenia 1U wraz z zestawem do montażu urządzenia w szafie serwerowej 19".
2.	Wbudowany port konsoli szeregowej RJ45 oraz USB/Micro-USB.
3.	Możliwość łączenia do 8 urządzeń w stos zarządzany z pojedynczego adresu IP, połączenie pomiędzy poszczególnymi urządzeniami musi być możliwe z przepustowością minimum 40Gbps.
4.	Wbudowany system zasilania 230V AC o mocy minimalnej 250 W , do zasilacza dołączony przewód zasilający wraz z europejską przejściówką.
5.	Obsługa sieci wirtualnych IEEE 802.1Q – min. 4000.
6.	Wsparcie dla ramek Jumbo Frames (min. 9K bajtów).
7.	Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym).
8.	Modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
9.	Możliwość monitorowania zajętości CPU.
10.	Pojemność tablicy adresów MAC: minimum 32 000 wpisów.
11.	Możliwość przypisania minimum 1000 ACL (sumarycznie wejściowe i wyjściowe).

12.	Obsługa routingu IPv4/IPv6 minimum w zakresie tras statycznych oraz protokołów RIP i OSPF.
13.	Obsługa protokołów IS-IS, BGP4, MBGP - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
14.	Policy Based Routing dla IPv4 oraz IPv6.
15.	Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration).
16.	Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping.
17.	Obsługa protokołu PIM-SM.
18.	Obsługa protokołów PIM DM oraz PIM SSM - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
19.	Obsługa uwierzytelniania do sieci z wykorzystaniem: • protokołu IEEE 802.1x, • formularza www, • adresu MAC.
20.	Funkcjonalność elastycznego uwierzytelniania z możliwością wyboru kolejności stosowanych mechanizmów – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www).
21.	Obsługa wielu sesji uwierzytelniania (min. 12) na jednym porcie (multiple supplicants).
22.	Możliwość integracji funkcjonalności uwierzytelniania z systemem klasy NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reautentykacji dołączonego klienta z poziomu systemu NAC.
23.	Przydział sieci VLAN, ACL/QoS podczas autentykacji.
24.	Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie: • definicji sieci VLAN, • reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6, • realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6, • realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
25.	Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) wraz z funkcjonalnością *per-command authentication*.
26.	Bezpieczeństwo adresów MAC: • ograniczenie liczby MAC adresów na porcie, • zatrzaśnięcie MAC adresu na porcie, • możliwość wpisania statycznych MAC adresów na port/vlan, • możliwość wyłączenia uczenia MAC adresów.
27.	Zabezpieczenie przełącznika przed atakami DoS: • Networks Ingress Filtering RFC 2267, • SYN Attack Protection, • Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania.
28.	Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika).
29.	Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation.
30.	Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard.
31.	Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768).
32.	Wsparcie dla technologii Ethernet VPN (EVPN) oraz tunelowania GRE - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania.
33.	Obsługa protokołów drzewa rozpinającego (spanning Tree) w zakresie STP, RSTP, MSTP, PVST+.

34.	Obsługa protokołu MVRP.
35.	Obsługa protokołu EAPS (RFC 3619), ERPS (ITU G.8032) lub równoważnego.
36.	Obsługa Link Aggregation IEEE 802.3ad wraz z mechanizmem LACP.
37.	Obsługa IEEE 802.3ah Ethernet OAM.
38.	Obsługa mechanizmu MC-LAG/VSS/MLAG/IRF lub równoważnego umożliwiającego agregację połączeń do dwóch niezależnych przełączników. Urządzenia dołączające się do pary przełączników muszą widzeń je jako pojedyncze urządzenie z punktu widzenia warstwy L2. Nie dopuszcza się stosowania mechanizmów łączenia w stos jako równoważnych.
39.	Zarządzany za pomocą SSH/Telnet, SNMP v1/v2/v3, oraz systemu zarządzania dostarczonego przez producenta.
40.	Obsługa SYSLOG z możliwością definiowania wielu serwerów.
41.	Sprzętowa obsługa sFlow lub protokołu równoważnego.
42.	Obsługa RMON (RFC 1757) i RMON2 (RFC 2021).
43.	Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
44.	Możliwość uruchamiania skryptów: • ręcznie, • o określonym czasie lub co wskazany okres, • na podstawie wpisów w logu systemowym.
45.	Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS.
46.	Obsługa protokołu MACSEC (IEEE 802.1AE) na wszystkich portach urządzenia (zarówno porty miedziane, jak i światłowodowe) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania.
47.	Usługi wirtualizacji warstwy L2 i L3 (Fabric Network): • Przełącznik musi udostępniać możliwość wirtualizacji usług sieciowych w warstwie L2 i L3 modelu OSI. • Przełącznik musi zapewniać „multi-tennancy" dla usług sieciowych zarówno w L2 jak i L3. Rozumiemy przez to przypadek, w którym do przełącznika doprowadzone są nakładające się numery VLAN (vlan overlap) lub podsieci IP (subnet overlap). W takim przypadku przełącznik musi zapewniać izolację tego ruchu od siebie. • Przełącznik musi zapewniać usługi zwirtualizowane L2 i L3 w oparciu o standardowe protokoły sieciowe (SPB 802.1aq lub EVPN). • Przełącznik musi umożliwiać skonfigurowanie usług wirtualizacji w L2. • Przełącznik musi umożliwiać obsługę usług multicast dla L2 jak i L3 bez konieczności używania protokołu PIM. • Przełącznik musi zapewniać możliwość zastosowania dowolnej topologii połączeń przy współpracy z innymi urządzeniami tworzącymi węzły sieci szkieletowej. • Przełącznik musi zapewniać możliwość dokładania nowych węzłów w sieci bez wpływu na już działające usługi sieciowe.
48.	Wykonawca musi zapewnić -**gwarancję producenta na okres 4 lat** uwzględniającą: • wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego po zgłoszeniu awarii przez Zamawiającego, • aktualizacje oprogramowania układowego (firmware), • dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.
49.	Przełącznik wyposażony w: • minimum 48 interfejsów 10/100/1000Base-T RJ45,

	• minimum 8 interfejsów 10GB Base-X SFP+.
50.	Nieblokująca architektura o wydajności przełączania min. 256 Gbps i matrycy przełączającej z szybkością minimum 190 milionów pakietów na sekundę (Mpps).
51.	Pojemność tablicy ARP: minimum 15000 wpisów.
52.	Minimum 12000 wpisów w tablicy routingu IPv4 oraz minimum 6000 wpisów w tablicy routingu IPv6.
53.	Minimum 4000 wpisów multicast (S,G,V).
54.	W ramach dostawy Wykonawca zobowiązuje się dostarczyć wkładki światłowodowe (minimum 4 sztuki) transceivery SFP+ MultiMode 10Gbps OM3, 850nm, duplex LC kompatybilne z dostarczanymi urządzeniami oraz 6 sztuk - transceivery SFP+ SingleMode 10Gbps, 1310nm, duplex LC kompatybilne z dostarczanymi urządzeniami.
55.	Urządzenia muszą mieć odblokowane wszystkie porty, jeżeli urządzenie wymaga zakupu dodatkowej licencji w celu umożliwienia korzystania ze wszystkich portów Wykonawca w ramach dostawy urządzeń dostarczy również licencję bezterminową pozwalającą na korzystanie ze wszystkich portów urządzenia.
56.	Urządzenia muszą być kompatybilne z posiadanym przez Zamawiającego rozwiązaniem NACVIEW w zakresie: - MAB (MAC Authentication Bypass), - CoA – obsługa polecenia zmiany autoryzacji RADIUS, - TACACS+ - funkcjonalność autoryzacji administratorów na urządzeniach sieciowych, - Multiautoryzacja – funkcjonalność autoryzowania urządzeń końcowych podłączonych do LAN za pośrednictwem przełącznika niezarządzalnego (Ethernet hub), - IEEE 802.1Q - obsługa vlanów, - IEEE 802.1x – uwierzytelnienie EAP, MAB – obsługa zewnętrznych serwerów RADIUS, - RFC 3576, RFC 5176 – obsługa CoA, - RFC 1157 (v.1), RFC 1441 (v.2), RFC 2570 (v.3) – obsługa monitoring.
57.	Wykonawca musi w ramach przedmiotu zamówienia wykonać wdrożenie w zakresie: uruchomienia, aktualizacji firmware, konfiguracji [połączenia] z posiadanym przez Zamawiającego systemem NACVIEW, konfiguracji VLANów.
58.	Do wykonania czynności opisanych w punkcie 57 Wykonawca musi dysponować minimum 2 osobami posiadającymi certyfikat “Certyfikowany inżynier NACVIEW” potwierdzający wiedzę i doświadczenie w instalacji, konfiguracji oraz wsparcia serwisowego .
59.	Urządzenia muszą być dostarczone w ramach produktów jednego producenta i tego samego producenta co przełączniki CORE.

3. System do zarządzania przełącznikami sieciowymi

Lp.	Parametry wyposażenia
1.	Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia.
2.	Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji.
3.	Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci.
4.	Musi zapewniać możliwości monitorowania zakupionych urządzeń i wdrażania w nich konfiguracji VLAN.
5.	Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II.
6.	Do obsługi zdalnej nie może wymagać stosowania żadnych klientów, użytkowników końcowych lub oprogramowania typu agent.

7.	Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć.
8.	Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej.
9.	Musi zawierać zintegrowane aplikacje typu plug-in, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania.
10.	Musi mieć możliwość instalacji, jako maszyna wirtualna działająca w środowisku Hyper-V.
11.	Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.
12.	Rozwiązanie musi integrować się ze środowiskiem wirtualnym Hyper-V .
13.	Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci.
14.	Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID).
15.	Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).
16.	Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia.
17.	Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu.
18.	Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu firmware urządzenia.
19.	Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń.
20.	Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych.
21.	Musi zapewniać możliwości analiz na poziomie portu.
22.	Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów.
23.	Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania.
24.	Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB (Management Information Base) z reprezentacji opartej na drzewie oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB.
25.	Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby.
26.	Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware i wielkość pliku konfiguracyjnego.
27.	Musi posiadać możliwość pobierania oprogramowania firmware do jednego urządzenia lub do wielu urządzeń jednocześnie.
28.	Musi mieć możliwość pobierania obrazów boot PROM do jednego urządzenia lub do wielu urządzeń jednocześnie.
29.	Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń.
30.	Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń.
31.	Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania.
32.	Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury.
33.	Musi umożliwiać automatyczną reakcję w czasie rzeczywistym poprzez integrację z rozwiązaniami klasy

	SIEM oraz IPS.
34.	Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym.
35.	Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji.
36.	Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https.
37.	Musi mieć możliwość definiowania polityk: • ograniczających poziom pasma, • ograniczających liczbę nowych połączeń sieciowych, • ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3, • nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania.
38.	Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą aplikacji, dzięki której polityki zostaną rozesłane do wszystkich urządzeń.
39.	Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci.
40.	Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC.
41.	Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p.
42.	Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania.
43.	Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku.
44.	Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 Trap (Inform).
45.	Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS.
46.	Musi zapewniać kompleksową analizę komunikacji sieciowej na warstwach 2-7.
47.	Musi udostępniać panel sterowania umożliwiający przeglądanie informacji o klientach, serwerach, paśmie, przepływach, czasach odpowiedzi sieci, czasach odpowiedzi aplikacji, czasach dostępu do aplikacji.
48.	Musi udostępniać raporty TopN dla klientów i serwerów zużywających najwięcej pasma, z podziałem na aplikacje, i aplikacji z podziałem na użytkowników.
49.	Musi umożliwiać analizę: • opóźnienia w całej sieci w oparciu o TCP, • opóźnienia aplikacji, • wykorzystania zasobów w oparciu o aplikacje, • wykorzystania aplikacji, celów i opóźnienia w podziale na poszczególnych użytkowników.
50.	Musi umożliwiać analizę danych w oparciu o protokół NetFlow i IPFIX.
51.	Musi umożliwiać rozpoznawanie znanych aplikacji.
52.	Musi posiada własną bazę danych sygnatur.
53.	Musi umożliwia modyfikację i dodawanie własnych sygnatur.
54.	Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia.
55.	Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci.
56.	Musi mieć możliwość przypisania „roli kwarantanny” użytkownikowi podłączonemu do portu.
57.	Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych

	użytkowników, aplikacji lub systemów krytycznych dla danej organizacji.
58.	Musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci. Musi posiadać możliwość przypisywania sieci VLAN, reguł filtrowania warstw L2-L4 oraz QoS na warstwach L2-L4 (DSCP i 802.1p) dla każdej maszyny wirtualnej opartej na przełączniku wirtualnym i wirtualnej grupie portów. Reguły filtrowania na warstwach L3-L4 i reguły QoS muszą obsługiwać zarówno IPv4, jak i IPv6.
59.	System w momencie dostawy musi obsługiwać wszystkie urządzenia sieciowe będące przedmiotem postępowania (LAN i WLAN) oraz umożliwiać przyszłą rozbudowę do min. 200 urządzeń sieciowych.
60.	Rozbudowa nie może wiązać się z dodatkowym kosztem w postaci dodatkowej maszyny wirtualnej i/lub serwera sprzętowego – musi być jedynie rozszerzeniem licencyjnym.
61.	W ramach dostawy Wykonawca wykona wdrożenie w zakresie: uruchomienia, aktualizacji firmware, konfiguracji [połączenia] z posiadanym przez Zamawiającego systemem NACVIEW, konfiguracji VLANów.
62.	Jeżeli w oferowanym systemie wyżej wymienione funkcjonalności rozwiązania są ograniczone czasowo, Zamawiający wymaga dostarczenia licencji na okres nie krótszy niż 2 lata.
63.	Wykonawca musi zapewnić **2-letnią gwarancję producenta** obejmującą: - wymianę/naprawę usterki/problemu na następny dzień roboczy po zgłoszeniu awarii przez Zamawiającego, - dostęp do aktualizacji oprogramowania, - wsparcie techniczne przez e-mail, telefon i zdalną sesję.