**OPIS PRZEDMIOTU ZAMÓWIENIA(OPZ)**

**BLOK nr 1**

**Dostawa sprzętu sieciowego –
przełącznik dostępowy**

**2025 r.**

Spis treści

1. [**WSTĘP** 3](#_Toc202960807)
2. [**PRZEDMIOT ZAMÓWIENIA** 3](#_Toc202960808)
3. [**SPECYFIKACJA ZAMÓWIENIA** 3](#_Toc202960809)
4. [**MIEJSCE DOSTAWY** 6](#_Toc202960810)
5. [**GWARANCJA, SERWIS** 6](#_Toc202960811)
6. [**PROCEDURY ODBIORU** 7](#_Toc202960812)
7. [**WZORY FORMULARZY** 7](#_Toc202960813)

# **WSTĘP**

Straż Graniczna działająca na podstawie Ustawy o Straży Granicznej wykorzystuje w codziennej służbie systemy teleinformatyczne niezbędne w procesie kontroli ruchu granicznego, ochrony granicy państwowej oraz w części granicy zewnętrznej Unii Europejskiej. Straż Graniczna wykorzystuje sieć teleinformatyczną w całości zbudowaną w oparciu o platformę sprzętową firmy Cisco Systems, Palo Alto, F5, Citrix. Zastosowane urządzenia umożliwiają przenoszenie wszelkiego rodzaju usług typu dane, głos, video
w oparciu o protokół IP oraz implementację elementów ochrony. Wszystkie jednostki Straży Granicznej tj. Komenda Główna SG, Oddziały SG oraz inne placówki połączone są hierarchicznie siecią WAN za pomocą dynamicznych tuneli VPN (DMVPN) obsługiwanych przez routery CISCO opartych na protokołach GRE, NHRP i IPSEC oraz protokołach routingu EIGRP,OSPF i trasach statycznych. Na bazie wymienionych urządzeń sieciowych oraz protokołów, w tym w szczególności protokołu DMVPN Straż Graniczna wdrożyła, skonfigurowała sieć teleinformatyczną.

Infrastruktura techniczna Platformy Teleinformatycznej SG obejmuje między innymi routery Cisco serii 2900, 3900, 7200, 9200 ASR1000 przełączniki Catalyst serii 6500, 4500, 3750, 2960 oraz przełączniki Nexus 7706 z kartami F3, system telefonii IP zarządzany serwerami Cisco Unified Communication Manager 10.5 oraz urządzenia bezpieczeństwa sieciowego Cisco Firepower 4120, Firepower 2130, ASA5585. Administracja częścią infrastruktury sieciowej odbywa się za pomocą systemów Prime Infrastructure 2.1 zwanych dalej systemami zarządzania. Całość rozwiązania zarządzana jest centralnie z Centrum Zarządzania Siecią w Warszawie przez odpowiednio przeszkolonych inżynierów systemowych Straży Granicznej w oparciu o system kontroli dostępu realizowany przez urządzenia Cisco ACS 5.5 z wykorzystaniem protokołu TACACS+ zapewniającego rozliczalność komend. Uwierzytelnianie stacji końcowych jest realizowane przez Centralny System Uwierzytelniania Stacji Końcowych oparty o oprogramowanie Cisco ISE 2.4 wdrożone w modelu dystrybucyjnym. Straż Graniczna posiada również system SDN firmy Cisco ACI 4.0 wdrożony w modelu multipod oparty
na przełącznikach N9K-C93180YC-EX (leaf), N9K-C93180YC-EX (Spine) oraz kontrolerach APIC-Serve-M2.

# **PRZEDMIOT ZAMÓWIENIA**

Przedmiotem zamówienia jest dostawa fabrycznie nowych przełączników dostępowych wraz z 3 letnimi licencjami - 2 kpl.

# **SPECYFIKACJA ZAMÓWIENIA**

W celu realizacji zadania w zakresie zapewnienia właściwego działania sieci lokalnej Zamawiającego niezbędne jest dostarczenie przełączników wraz z licencjami spełniających poniższe wymagania:

Przełącznik musi zapewniać przełączanie w warstwie drugiej.

Przełącznik musi obsługiwać co najmniej 100 sieci VLAN

System operacyjny (licencja) wspierający SSH.

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. W pamięci nieulotnej musi być możliwość przechowywania przynajmniej 4 plików konfiguracyjnych.

Przełącznik musi umożliwiać zestawianie połączeń typu trunk w standardzie IEEE 802.1Q.

Przełącznik musi umożliwiać wyczyszczenie tablicy adresów MAC (wpisów nauczonych dynamicznie) z poziomu linii poleceń. Wymagana jest możliwość usunięcia wszystkich adresów nauczonych dynamicznie, konkretnego adresu nauczonego dynamicznie, adresów nauczonych dynamicznie dla konkretnej sieci VLAN lub portu.

Przełącznik musi umożliwiać lokalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do urządzenia monitorującego przyłączonego do innego portu.

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.

Przełącznik musi umożliwiać skonfigurowanie i określenie sieci VLAN służącej
do zarządzania przełącznikiem tzw. VLAN zarządzający (Management VLAN).

Przełącznik musi zapewniać na jednym porcie jednoczesny dostęp do sieci typu voice
 i data z wykorzystaniem telefonów Zamawiającego.

Przełącznik musi wspierać funkcjonalność przekazywania znakowania QoS od urządzeń typu telefon pracujących w sieci Straży Granicznej.

Przełącznik musi wspierać funkcjonalność Link Layer Discovery Protocol.

Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

* 1. IEEE 802.1w Rapid Spanning Tree,
	2. IEEE 802.1s Multi-Instance Spanning Tree,
	3. możliwość grupowania do min. 8 portów tego samego typu w jeden kanał logiczny zgodnie ze specyfikacją IEEE 802.3ad (LACP),
	4. możliwość grupowania w kanały IEEE 802.3ad (LACP) portów tego samego typu fizycznie znajdujących się na różnych przełącznikach tworzących stos.

Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

* 1. wiele poziomów dostępu administracyjnego poprzez konsolę,
	2. zalogowanie się administratora z konkretnym poziomem dostępu zgodnie
	z odpowiedzią serwera autoryzacji (privilage-level), dostęp do urządzenia przez SNMPv3 i SSHv2,
	3. wyłączenie sieci VLAN nr 1 dla portu typu trunk,
	4. funkcjonalność prywatnego VLAN-u, czyli możliwość blokowania ruchu pomiędzy portami w obrębie jednego VLAN-u (tzw. porty izolowane) z pozostawieniem możliwości komunikacji z portem nadrzędnym,
	5. funkcjonalność dynamicznej inspekcji protokołu ARP, czyli możliwość zablokowania przesyłania przez dołączone stacje pakietów tzw. gratitious ARP (GARP), umożliwiających przejęcie ruchu innych stacji komunikujących się między sobą
	w obrębie tej samej podsieci IP,
	6. funkcjonalność inspekcji adresów źródłowych pakietów IP, czyli możliwość zablokowania przesyłania przez dołączone stacje pakietów IP ze źródłowymi adresami IP do nich nie należących (tzw. IP spoofing),
	7. autoryzację użytkowników/portów w oparciu o IEEE 802.1x wraz z obsługą funkcjonalności MAC Authentication Bypass umożliwiającą podłączenia do portów
	z autentykacją 802.1x urządzeń nie wyposażonych w suplikanta 802.1x (np. drukarki, telefony IP) i autentykację tych urządzeń na bazie adresu MAC,
	8. funkcjonalność inspekcji adresów źródłowych pakietów IP (IP Source Guard), czyli możliwość zablokowania przesyłania przez dołączone stacje pakietów IP
	ze źródłowymi adresami IP do nich nie należących (tzw. IP spoofing),

W zakresie SpanningTree przełącznik musi obsługiwać mechanizmy:

* 1. Spanning-tree PortFast: natychmiastowe przejście portu dostępowego L2 do trybu „forwarding” z pominięciem fazy „listening” oraz „learning”,
	2. PortFast Guard: zamknięcie / wyłączenie (shutdown) portu w trybie PortFast
	po otrzymaniu ramki BPDU,
	3. urządzenia muszą współpracować z systemem zarządzania wykorzystywanym
	w Straży Granicznej, a w szczególności:
* wgrywania, aktualizacji, ściągania i analizy konfiguracji;
* inwentaryzacji;
* zmiany oprogramowania.

Urządzenie musi być wyposażone w minimum 1 port konsoli do czynności administratorskich.

Dostarczone urządzenia muszą posiadać aktualną dostępną na rynku wersję firmware.

W celu usprawnienia diagnostyki urządzenia oraz połączeń sieciowych wymaga się, aby przełącznik był wyposażony w lampki sygnalizacyjne LED umożliwiające wizualne określenie dla każdego z portów statusu portu tj. wyłączony, aktywny, prędkość, full-duplex.

Urządzenie musi posiadać możliwość konfiguracji 802.1x na portach w oparciu o Centralny System Uwierzytelnień (Cisco Identity Service Engine w wersji 2.4).

Urządzenie musi posiadać możliwość aplikowania na porty przełącznika dynamicznych list ACL (dACL), przesyłanych z Centralnego Systemu Uwierzytelnień (listy dACL są w pełni przesyłane w komunikatach Radius z serwera, nie muszą być wcześniej wysyłane na przełączniki w osobnym trybie administracyjnym. Nie dopuszcza się rozwiązania w którym lista ACL jest wcześniej skonfigurowana na przełączniku, a komunikat Radius zawiera tylko nazwę statycznej listy ACL.)

Dynamiczne listy ACL (dACL) powinny być przypisywane na port niezależnie dla każdego urządzenia uwierzytelnionego na porcie (każde urządzenie powinno mieć możliwość "otrzymania" w momencie uwierzytelnienia różnej listy dACL i taka dACL powinna działać tylko dla tego urządzenia rozpoznawanego poprzez jego adres IP)

Możliwość konfiguracji portów przełącznika w co najmniej 3 trybach 802.1x:

* 1. "tryb otwarty" (konfiguracja 802.1x która jest na porcie pracuje w trybie "monitoringu" - błędne uwierzytelnienie lub jego brak nie wpływa na ruch realizowany przez dany port przełącznika. Zdarzenia z portu są pokazywane przez Centralny System Uwierzytelnień) ;
	2. "tryb otwarty z listą ACL" (tryb monitoringu, z dodatkowym ograniczeniem,
	że w przypadku braku uwierzytelnienia lub jego błędu ruch na porcie jest ograniczany zgodnie ze statyczną listą ACL skonfigurowaną przez administratora przełącznika
	na porcie);
	3. "tryb zamknięty" (ruch poprzez port przełącznika jest dozwolony tylko w przypadku poprawnego uwierzytelnienia przez Centralny System Uwierzytelnień).

Możliwość wykorzystania jednej konfiguracji na wszystkich portach przełącznika pozwalającej realizować uwierzytelnienie w oparciu o Centralny System Uwierzytelnień
z wykorzystaniem MAB oraz różnych metod EAP (np. PEAP, TLS). Wybór metody powinna określać konfiguracja Centralnego Systemu Uwierzytelnień, nie konfiguracja portu (tzn. różne urządzenia podłączane do tego samego portu powinny mieć możliwość realizacji różnej formy uwierzytelniania).

Możliwość wykonywania przez Centralny System Uwierzytelnia zmiany stanu uwierzytelniania tzw. CoA (Change of Authorization) umożliwiając co najmniej:

* 1. zdalne wymuszenie ponownego uwierzytelnienia pojedynczego urządzenia przyłączonego do portu przełącznika;
	2. zdalne wyłączenie portu przełącznika;
	3. zmiany stanu uwierzytelnia związanego z ponownym przypisaniem dynamicznej listy dACL lub zmiany VLAN.

Konfiguracja portu przełącznika w trybie 802.1x powinna mieć możliwość regularnego, automatycznego wymuszania ponownego uwierzytelniania, niezależnie od konfiguracji Centralnego Systemu Uwierzytelnień lub działań administratorów.

Przełącznik powinien poprawnie pracować w sytuacji której:

* 1. na wszystkich jego portach są przyłączone komputery poprzez telefon IP;
	2. na wszystkich portach jest skonfigurowane 802.1x;
	3. na wszystkich portach są przypisane dACL różne dla każdego urządzenia przyłączonego do danego portu przełącznika;
	4. na wszystkich portach przełącznika zostały przypisane listy dACL o długości
	co najmniej 30 linii. Przełącznik w takiej sytuacji powinien pracować z pełną wydajnością przełączania pakietów opisanej w dokumentacji. Nie dopuszcza się degradacji wydajności pracy związanej z przypisanymi dACL;

Przełącznik musi być wyposażony w minimum 48 portów 10/100/1000.

Przełącznik musi być wyposażony w minimum 4 interfejsy TenGigabit Ethernet.

Porty dostępowe 10/100/1000 muszą zapewniać wsparcie dla zasilania przez sieć LAN zgodnie z IEEE 802.3af oraz IEEE 802.3at na wszystkich portach jednocześnie
z maksymalna mocą. Budżet mocy dla PoE musi wynosić co najmniej 740 W.

Urządzenie musi posiadać min. 512MB pamięci DRAM i min. 128MB pamięci flash.

Urządzenie posiadać funkcjonalność łączenia w stos z innymi przełącznikami tego samego typu oraz innymi należącymi do tej samej rodziny przełączników.

Urządzenie musi posiadać na wyposażeniu moduły i kabel do łączenia w stos (STACK-KIT).

Urządzenia tworzące stos z punktu widzenia zarządzania muszą stanowić jedno logiczne urządzenie.

Funkcjonalność łączenia w stos musi umożliwiać pracę min. 8 urządzeń w stosie.

Dla funkcjonalności łączenia urządzeń w stos musi być dostępny mechanizm redundancji 1:N polegający na tym, że w przypadku, gdy awarii ulega jednostka główna tj. jednostka sterująca stosem (przełącznik, który logicznie steruje, zarządza pracą stosu) wówczas inny z przełączników tworzących stos może zastąpić jednostkę główną i przejąć jej zadania.

Urządzenie musi być przygotowane do montażu w szafie 19” umożliwiające zasilanie prądem przemiennym 230V z wtyczką DIN49441.

Licencja umożliwiająca korzystanie z podstawowych funkcji zarządzania siecią , takich jak wizualizacja, raportowanie i automatyzacja sieci.

# **MIEJSCE DOSTAWY**

Zamawiający wymaga dostarczenia przedmiotu zamówienia w dni robocze w godzinach 7.30 – 14.30 do niżej wymienionej lokalizacji, w której będzie użytkowany:

|  |  |
| --- | --- |
| **Jednostka organizacyjna Straży Granicznej** | **Adres** |
| Ośrodek Szkoleń Specjalistycznych SG | ul. Wojska Polskiego 259-800 Lubań |

#

# **GWARANCJA, SERWIS**

1. Zamawiający wymaga, aby dostarczone urządzenia objęte były gwarancją przez okres minimum 36 miesięcy począwszy od daty podpisania Protokołu odbioru dostawy.
2. Zamawiający wymaga aby całość dostarczanego sprzętu pochodziła z autoryzowanego kanału sprzedaży producentów co zostanie potwierdzone oświadczeniem Producenta.
3. Zamawiający wymaga aby całość dostarczanego sprzętu była fabrycznie nowa, nie używana we wcześniejszych projektach i wyprodukowana nie wcześniej niż 12 miesięcy przed dostawą co zostanie potwierdzone oświadczeniem Producenta.
4. Nie dopuszcza się dostarczania i wykorzystywania przez Wykonawcę sprzętu refabrykowanego (ang. refurbished), używanego czy też powtórnie wprowadzonego na rynek sprzedaży. Nie dopuszcza się rozwiązań prototypowych.
5. Urządzenia objęte ofertą Wykonawcy nie mogą być urządzeniami dla których ogłoszono koniec życia produktu.
6. Zamawiający wymaga, aby serwis dostarczonych urządzeń był realizowany przez Producenta oferowanych urządzeń lub autoryzowanego partnera serwisowego Producenta urządzeń.
7. Gwarancja obejmuje co najmniej:
8. wady fabryczne i materiałowe;
9. bezpłatną wymianę uszkodzonego sprzętu w terminie do 30 dni roboczych po zgłoszeniu awarii.
10. Gwarancja musi być świadczona w miejscu użytkowania sprzętu.
11. Gwarancja nie może ograniczać praw Zamawiającego do zmiany miejsca instalacji sprzętu w obrębie siedziby Zamawiającego, instalowania i wymiany w dostarczonym sprzęcie standardowych podzespołów i urządzeń, zgodnie z zasadami sztuki, przez wykwalifikowany personel Zamawiającego lub przez autoryzowanego przez producenta sprzętu inżyniera innego Wykonawcy.
12. Przez pojęcie dnia roboczego należy rozumieć dni od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy.
13. Proces zgłaszania oraz rozpatrywania napraw i reklamacji będzie realizowany poprzez zgłoszenie RMA (Return Merchandise Authorization) na platformie internetowej Wykonawcy.
14. W przypadku konieczności przekazania urządzenia do Wykonawcy należy stosować Protokół przekazania urządzenia zgodnie ze wzorem zawartym w treści Działu nr VII OPZ.
15. Wykonawca jest zobowiązany do odebrania uszkodzonych urządzeń z miejsc użytkowania urządzeń i do dostarczenia naprawionych/wymienianych urządzeń do miejsca instalacji urządzeń na własny koszt i ryzyko. Wykonawca pokrywa także koszty transportu oraz koszty dojazdu serwisu w przypadku konieczności wymiany lub naprawy w miejscu użytkowania. Miejsca użytkowania urządzeń znajduje się w Dziale nr IV OPZ.
16. W przypadku niedotrzymania terminu wymiany uszkodzonego sprzętu, o którym mowa w pkt. 7 ppkt b Wykonawca zapłaci Zamawiającemu karę umowną za opóźnienie w naprawie gwarancyjnej na zasadach określonych w § 7 Umowy.

# **PROCEDURY ODBIORU**

**Procedura odbioru dostawy**

1. Dostawa oznacza dostarczenie przedmiotu umowy do wskazanej lokalizacji Zamawiającego w terminach uzgodnionych z Zamawiającym.
2. Osobami odpowiedzialnymi za podpisywanie Protokołu odbioru dostawy są upoważnione osoby Zamawiającego oraz Wykonawcy.
3. Wykonawca powiadomi Zamawiającego o gotowości do rozpoczęcia odbioru.
4. Odbiór przedmiotu umowy polega na sprawdzeniu pod względem zgodności z zapisami Umowy oraz w szczególności pod względem ilości dostarczonych urządzeń. W przypadku stwierdzenia rozbieżności w dostawie urządzeń Zamawiający poinformuje o stwierdzonych rozbieżnościach Wykonawcę. W takim przypadku procedura odbioru dostawy zostanie przerwana. Nowa procedura odbioru dostawy zostanie rozpoczęta po usunięciu rozbieżności i nieścisłości przez Wykonawcę.
5. Wzory koniecznych dokumentów umieszczone są w OPZ.
6. Rezultatem realizacji przedmiotu umowy w odpowiednim zakresie będą:
	* dostarczony przedmiot umowy;
	* podpisany Protokół odbioru dostawy, który zostanie przygotowany przez Wykonawcę i uzyska akceptację Zamawiającego.

# **WZORY FORMULARZY**

**PROTOKÓŁ ODBIORU DOSTAWY**

na podstawie umowy nr ……………….. zawartej w dniu …………………..

pomiędzy

Ośrodkiem Szkoleń Specjalistycznych Straży Granicznej w Lubaniu

a firmą ……………………………………………………………

Wykonawca ……………………………………………….. oświadcza, iż przedmiot umowy został zrealizowany. W związku z powyższym przedstawiamy do akceptacji niniejszy Protokół Odbioru Dostawy.

1. Wykaz dostarczonych urządzeń:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa urządzenia** | **Model/Typ/Symbol** | **Ilość** | **Numer seryjny** |
|   |   |   |   |  |
|   |   |   |   |  |

1. W czasie odbioru dostawy dokonano sprawdzenia pod względem zgodności z zapisami umowy oraz sprawdzenia ilościowego dostarczonych urządzeń.
2. Uwagi Zamawiającego:

…………………………………………………………………………………………………

…………………………………………………………………………………………………

|  |  |
| --- | --- |
|   |   |
| Podpis osoba upoważniona Zamawiającego (data, pieczęć, czytelny podpis)  | Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)  |

**PROTOKÓŁ PRZEKAZANIA SPRZĘTU**

na podstawie umowy nr ………… zawartej w dniu …………..

pomiędzy

Ośrodkiem Szkoleń Specjalistycznych Straży Granicznej w Lubaniu

a firmą ………………………………………….……….

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Lp.** | **Nazwa urządzenia** | **Model/Typ/Symbol** | **Numer seryjny** | **Ilość** |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |
|   |   |   |   |   |

W dniu ………………. strona …………………….. (Wydający) przekazała stronie …………………… (Przyjmujący) ww. urządzenia w celu ……………………..…………

Uwagi:

…………………………………………………………………………………………………

…………………………………………………………………………………………………

…………………………………………………………………………………………………

|  |  |
| --- | --- |
|   |   |
| Podpis osoba upoważniona Zamawiającego (data, pieczęć, czytelny podpis)  | Podpis osoba upoważniona Wykonawcy (data, pieczęć, czytelny podpis)  |