Warmia i Mazury
Sp. z o.o.

WIM.ZOST.LAN.CCTV.2.2024 Szymany, dn.2024-12-05 r.

.....
(*Pieczęć Zamawiającego)*

ZAPYTANIE OFERTOWE

(niniejsze zapytanie nie stanowi zapytania ofertowego w rozumieniu ustawy pzp i stanowi rozeznanie rynku)

Zwracamy się z prośbą o przesłanie oferty na poniżej opisany przedmiot zamówienia:
Dostawa dwóch przełączników dostępowych sieci LAN zgodnie ze specyfikacja techniczną zawartą w załączniku nr 1.

Termin realizacji zamówienia: dn. 31-12-2024 r.

Kryterium oceny ofert: cena 100%

Uwagi: Wycena ma na celu przeprowadzenie analizy rynku oraz wyłonienia Wykonawcy.

Ofertę prosimy przesłać pocztą na adres: m.kucman@mazuryairport.pl

Termin składania ofert: 13.12..2024 r. do godz. 15:00

Zatwierdzam:

KWALIFIKOWANY PRACOWNIK ZABEZPIECZENIA TECHNICZNEGO
Lista Komendy Wojewódzkiej Policji w Olsztynie
nr PZT-20176
Marek Kucman

.....
(Podpis Kierownika Komórki Organizacyjnej)

Załącznik nr 1 do zapytania ofertowego: Dostawa dwóch przełączników dostępowych sieci LAN

Szczegółowy opis przedmiotu zamówienia

Wymagania techniczne

1. Wysokość urządzenia 1U
2. Przełącznik posiadający minimum 16 portów 100Mb / 1Gb / 10GBASE-X SFP+
3. Nieblokującą architekturę o wydajności przełączania min. 320 Gb/s
4. Szybkość przełączania minimum 238 Milionów pakietów na sekundę
5. Przełącznik musi posiadać wsparcie Energy Efficient Ethernet IEEE 802.3az
6. Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management
7. Wbudowany port USB oraz port konsoli
8. Przełącznik musi posiadać dwa wbudowane zasilacze zapewniające redundancję źródeł zasilania
9. Możliwość łączenia do 8 przełączników w stos. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych
10. Tablica MAC adresów minimum 16k
11. Pamięć operacyjna: minimum 1GB pamięci DRAM
12. Pamięć flash: minimum 4GB pamięci Flash oraz bufora pakietów minimum 2MB
13. Obsługa sieci wirtualnych IEEE 802.1Q – minimum 4094
14. Wsparcie dla ramek Jumbo Frames (minimum 9216 bajtów)
15. Obsługa Quality of Service (IEEE 802.1p, DiffServ, 8 kolejek priorytetów na każdym porcie wyjściowym)
16. 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
17. Możliwość monitorowania zajętości CPU
18. Pojemność tabeli routingu IPv4 minimum 480 wpisów
19. Routing statyczny
20. Obsługa routingu dynamicznego IPv4

a. RIPv1/v2

b. OSPFv2 – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania

21. Policy Based Routing dla IPv4
22. Pojemność tabeli routingu IPv6 min. 240 wpisów
23. Routing statyczny
24. Obsługa routingu dynamicznego dla IPv6

a. RIPng

b. OSPFv3 – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania

25. Policy Based Routing dla IPv6
26. Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)
27. Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping
28. Obsługa protokołu PIM-SM – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
29. Obsługa Network Login
    a. IEEE 802.1x
    b. Web-based Network Login
    c. MAC based Network Login

30. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www)
31. Obsługa wielu klientów (minimum 12) Network Login na jednym porcie (Multiple supplicants)
32. Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC
33. Przydział sieci VLAN, ACL/QoS podczas logowania Network Login
34. Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma
35. Urządzenie musi wspierać profile bezpieczeństwa definiowane dla każdego użytkownika indywidualnie. Profil bezpieczeństwa oznacza połączenie:
    a. definicji sieci VLAN,
    b. reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,
    c. realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,
    d. realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4.
36. Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication
37. Bezpieczeństwo MAC adresów:
    a. ograniczenie liczby MAC adresów na porcie
    b. zatrzaśnięcie MAC adresu na porcie
    c. możliwość wpisania statycznych MAC adresów na port/vlan
    d. możliwość wyłączenia MAC learning
38. Zabezpieczenie przełącznika przed atakami DoS
    a. Networks Ingress Filtering RFC 2267
    b. SYN Attack Protection
    c. Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania
39. Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika – wire-speed)
40. Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation
41. Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard
42. Obsługa redundancji routingu VRRP (RFC 2338) i VRRPv2 (RFC 3768) – jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
43. Obsługa STP, RSTP, MSTP, PVST+
44. Obsługa protokołu MVRP
45. Obsługa EAPS (RFC 3619)
46. Obsługa protokołu ERPS lub równoważnego oraz ITU G.8032
47. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – minimum 128 grup po 8 portów
48. Obsługa IEEE 802.3ah Ethernet OAM
49. Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników
50. Musi mieć możliwość zarządzania za pomocą SSH/Telnet, SNMP, dedykowanego interfejsu przeglądarkowego, oraz systemu zarządzania dostarczonego przez producenta (zarówno wersji on-site jak i interfejsu chmurowego)
51. Obsługa protokołu Zero Touch Provisioning (ZTP), pozwalającego na automatyczną konfigurację urządzeń z centralnego punktu zarządzania
52. Zarządzanie przez SNMP v1/v2/v3
53. Obsługa SYSLOG z możliwością definiowania wielu serwerów
54. Sprzętowa obsługa sFlow lub protokołu równoważnego

55. Obsługa RMON (RFC 1757) i RMON2 (RFC 2021)
56. Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych)
57. Możliwość uruchamiania skryptów:
    a. Ręcznie
    b. O określonym czasie lub co wskazany okres czasu
    c. Na podstawie wpisów w logu systemowym
58. Obsługa XML API poprzez Telnet/SSH i HTTP/HTTPS
59. Obsługa protokołu MACSEC (IEEE 802.1AE) – jeżeli funkcjonalność ta wymaga dodatkowych modułów lub licencji Zamawiający nie wymaga ich dostarczenia w ramach tego postępowania
60. Wsparcie dla protokołów przeznaczonych do przesyłania w czasie rzeczywistym sygnałów audio, wideo oraz innych przez sieć Ethernet (np. RAVENNA, AVB) - jeżeli funkcjonalność ta wymaga dodatkowej licencji Zamawiający nie wymaga jej dostarczenia w ramach tego postępowania
61. Minimum roczny kontrakt serwisowy zapewniający:
    - wymianę uszkodzonego urządzenia z dostawą następnego dnia roboczego po zgłoszeniu,
    - aktualizacje oprogramowania układowego (firmware),
    - wsparcie techniczne producenta (TAC) działające w trybie 24⁄7 poprzez telefon, email oraz portal WWW
    - dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.
    Po jego wygaśnięciu dożywotnia gwarancja producenta (rozumiana co najmniej jako data zakończenia sprzedaży (EOS) + dodatkowe 5 lat) uwzględniająca:
    - wymianę uszkodzonego urządzenia z wysyłką następnego dnia roboczego,
    - aktualizacje oprogramowania układowego (firmware),
    - dostęp do bazy wiedzy oraz dokumentacji technicznej producenta.

Wymagania aplikacyjne

Urządzenie musi być kompatybilne z posiadanym przez Zamawiającego systemem zarządzania urządzeniami sieciowymi firmy Extreme Networks (XMC) co najmniej z poniższymi funkcjonalnościami:

- pobieranie konfiguracji przez nowo podłączane urządzenia z systemu zarządzania za pomocą funkcjonalności ZTP;
- centralna konfiguracja polityk bezpieczeństwa i ich dystrybucja do nowych urządzeń za pomocą narzędzia Policy Manager;

Instalacja, zarządzanie i nadzorowanie pracy urządzenia

Urządzenia muszą zostać dołączone do posiadanego przez Zamawiającego systemu zarządzania NMS-ADV. Urządzenia muszą zostać fizycznie połączone poprzez stacking z istniejącymi przełącznikami firmy Extreme Networks.

Wymagania dodatkowe

Wszystkie wymagane przez producenta kable, elementy mocujące, śruby, szyny musza być w zakresie dostawy.