DT.270.2.5.2019

Załącznik nr 7 do SIWZ SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Zadanie 1:

Wymagania dla przełącznika sieciowego

Przełącznik sieciowy – „typ 1"

1) Montaż w szafie 19" rack. System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19".
2) Liczba portów optycznych minimum 1 Gbps – co najmniej 4 sztuki.
3) Liczba portów Gigabit Ethernet 1000 Base-T – co najmniej 24 z obsługą PoE+ (802.3at), z mocą dla urządzeń PoE na poziomie co najmniej 370W.
4) Wszystkie porty Ethernet (miedziane) muszą być dostępne od przodu urządzenia.
5) Urządzenie musi zapewniać przepustowość magistrali wewnętrznej (switching capacity) co najmniej 56 Gbps
6) Musi istnieć możliwość tworzenia połączeń typu Link Aggregation zgrupowanych na czterech fizycznych portach zgodnych z IEEE 802.3ad (LACP).
   Połączenie urządzeń typu Link Aggregation nie może zmniejszać dostępnej ilości portów Ethernet.
7) Obsługa VLAN 802.1Q i TRUNK na wszystkich portach.
8) Rozmiar tablicy adresów MAC urządzenia - co najmniej 16000.
9) Obsługa co najmniej 1024 sieci VLAN.
10) Wsparcie dla protokołów Spanning Tree: STP, RSTP, MSTP, PVST.
11) Urządzenie musi zapewniać obsługę Jumbo Frame o rozmiarze co najmniej 9198 bajtów.
12) Urządzenie musi wspierać następujące mechanizmy związane z bezpieczeństwem sieci:
    a) Obsługa mechanizmu ip dhcp snooping;

b) Obsługa minimum 1500 wpisów ACL.

c) Obsługa protokołu TACACS+ implementacja powinna umożliwiać:

- Uwierzytelnienie (Authentication) użytkownika.
- Autoryzację (Authorization) i księgowanie (Accounting) każdej z komend wykonywanej przez użytkownika z poziomu SSH i CLI.
- Możliwość zdefiniowania kliku serwerów TACACS+, wraz z automatycznym przełączeniem na inny serwer, w przypadku awarii aktywnego serwera.

d) Obsługa protokołu RADIUS, implementacja powinna umożliwiać:

- Obsługę protokołu 802.1x.
- Obsługę uwierzytelnienia urządzeń nieposiadających wbudowanego suplikanta 802.1x, przy użyciu adresu MAC(MAB).
- Obsługę uwierzytelnienia minimum 5 urządzeń na jednym porcie przełącznika.
- Możliwość wyboru kolejności i priorytetu uwierzytelnienia na porcie (np. 802.1x, MAB).
- Obsługę list kontroli dostępu (ACL) wysyłanych z serwera NAC (per użytkownik /urządzenie).
- Obsługę dynamicznego przydzielania Vlan przez serwer NAC.
- Mechanizm pozwalający na wysyłanie, do serwera NAC, adresu IP (uwierzytelnionego urządzenia) przydzielonego w sposób dynamiczny.
- Mechanizm pozwalający na wysyłanie, do serwera NAC, statycznego adresu IP (uwierzytelnionego urządzenia).

e) Obsługę mechanizmu CoA w zakresie:

- Disconnect – po wysłaniu pakietu CoA, urządzenie zostanie uwierzytelnione ponownie z nowym numerem sesji(SessionID).
- Port-Bounce - po wysłaniu pakietu CoA port, do którego urządzenie jest podłączone zostanie włączony i wyłączony.

f) Uwierzytelnienie klienta poprzez Centralny Portal Uwierzytelniający, poprzez przekierowanie strony www, gdzie link do przekierowania jest wysyłany z serwera NAC,

g) Obsługi mechanizmu ponownego uwierzytelnienia, co określony czas, definiowanego przez serwer NAC.

h) Obsługę uwierzytelnienia telefonu (VLAN VoIP) i urządzenia (VLAN DATA) na jednym fizycznym porcie przełącznika.

i) Obsługi komunikatów o odłączeniu uwierzytelnionego urządzenia od telefonu. Przełącznik w opisanym przypadku powinien wysłać informację do serwera NAC o zakończonej sesji.

13) Możliwości zdefiniowania minimum 5 serwerów RADIUS, wraz z możliwością przełączenia na inny serwer, w przypadku awarii aktywnego serwera.

14) Zarządzanie:

a) CLI;

b) HTTPS;

c) SSHv2;

15) Obsługiwane protokoły

a) ICMP;

b) SNMP;

c) SNMPv2;

d) SNMPv3;

e) NTP – Client;

f) TFTP – Client;

g) DHCP Client;

h) DHCP Relay.

Zadanie 2:

Przełącznik sieciowy – „typ 2"

1) Montaż w szafie 19" rack. System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19".
2) Liczba portów optycznych minimum 1 Gbps – co najmniej 4 sztuki.
3) Liczba portów Gigabit Ethernet 1000 Base-T – co najmniej 48 z obsługą PoE+ (802.3at), z mocą dla urządzeń PoE na poziomie co najmniej 740W.
4) Wszystkie porty Ethernet (miedziane) muszą być dostępne od przodu urządzenia.
5) Urządzenie musi zapewniać przepustowość magistrali wewnętrznej (switching capacity) co najmniej 104 Gbps.
6) Musi istnieć możliwość tworzenia połączeń typu Link Aggregation, zgrupowanych na czterech fizycznych portach zgodnych z IEEE 802.3ad (LACP).
   Połączenie urządzeń typu Link Aggregation nie może zmniejszać dostępnej ilości portów Ethernet.
7) Obsługa VLAN 802.1Q i TRUNK na wszystkich portach.
8) Rozmiar tablicy adresów MAC urządzenia - co najmniej 16000.
9) Obsługa co najmniej 1024 sieci VLAN.
10) Wsparcie dla protokołów Spanning Tree: STP, RSTP, MSTP, PVST.
11) Urządzenie musi zapewniać obsługę Jumbo Frame o rozmiarze co najmniej 9198 bajtów.
12) Urządzenie musi wspierać następujące mechanizmy związane z bezpieczeństwem sieci:
    a) Obsługa mechanizmu IP DHCP SNOOPING
    b) Obsługa minimum 1500 wpisów ACL.
    c) Obsługa protokołu TACACS+, implementacja powinna umożliwiać:
       - Uwierzytelnienie (Authentication) użytkownika.
       - Autoryzację (Authorization) i księgowanie (Accounting) każdej z komend wykonywanej przez użytkownika z poziomu SSH i CLI.
       - Możliwość zdefiniowania kliku serwerów TACACS+, wraz z automatycznym przełączeniem na inny serwer, w przypadku awarii aktywnego serwera.

d) Obsługa protokołu RADIUS, implementacja powinna umożliwiać:
   - Obsługę protokołu 802.1x.
   - Obsługę uwierzytelnienia urządzeń nieposiadających wbudowanego suplikanta 802.1x, przy użyciu adresu MAC (MAB).
   - Obsługę uwierzytelnienia minimum 5 urządzeń na jednym porcie przełącznika.
   - Możliwość wyboru kolejności i priorytetu uwierzytelnienia na porcie(np. 802.1x, MAB).
   - Obsługę list kontroli dostępu (ACL) wysyłanych z serwera NAC (per użytkownik /urządzenie).
   - Obsługę dynamicznego przydzielania VLAN przez serwer NAC.
   - Mechanizm pozwalający na wysyłanie, do serwera NAC, adresu IP (uwierzytelnionego urządzenia) przydzielonego w sposób dynamiczny.
   - Mechanizm pozwalający na wysyłanie, do serwera NAC, statycznego adresu IP (uwierzytelnionego urządzenia).

e) Obsługę mechanizmu CoA w zakresie:
   - Disconnect – po wysłaniu pakietu CoA, urządzenie zostanie uwierzytelnione ponownie z nowym numerem sesji (SessionID).
   - Port-Bounce- po wysłaniu pakietu CoA, port, do którego urządzenie jest podłączone zostanie włączony i wyłączony.

f) Uwierzytelnienie klienta poprzez Centralny Portal Uwierzytelniający, poprzez przekierowanie strony www, gdzie link do przekierowania jest wysyłany z serwera NAC,

g) Obsługi mechanizmu ponownego uwierzytelnienia, co określony czas, definiowanego przez serwer NAC.

h) Obsługi uwierzytelnienia telefonu (VLAN VoIP) i urządzenia (VLAN DATA) na jednym fizycznym porcie przełącznika;

i) Obsługi komunikatów o odłączeniu uwierzytelnionego urządzenia od telefonu IP. Przełącznik powinien wysłać informację do serwera NAC o zakończonej sesji.

13) Możliwość zdefiniowania minimum 5 serwerów RADIUS, wraz z możliwością przełączenia na inny serwer, w przypadku awarii aktywnego serwera.

14) Zarządzanie:

a) CLI;
b) HTTPS;
c) SSHv2.

15) Obsługiwane protokoły:
a) ICMP;
b) SNMP;
c) SNMPv2;
d) SNMPv3;
e) NTP – Client;
f) TFTP – Client;
g) DHCP Client;
h) DHCP Relay.

Zadanie 3:

Przełącznik sieciowy – „typ 3"

1) Montaż w szafie 19" rack. System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19".
2) Liczba portów optycznych minimum 1 Gbps – co najmniej 4 sztuki.
3) Liczba portów Gigabit Ethernet 1000 Base-T – co najmniej 24.
4) Wszystkie porty Ethernet (miedziane) muszą być dostępne od przodu urządzenia.
5) Urządzenie musi zapewniać przepustowość magistrali wewnętrznej (switching capacity) co najmniej 56 Gb/s
6) Musi istnieć możliwość tworzenia połączeń typu Link Aggregation zgrupowanych na czterech fizycznych portach zgodnych z IEEE 802.3ad (LACP).
   Połączenie urządzeń typu Link Aggregation nie może zmniejszać dostępnej ilości portów Ethernet.

7) Obsługa VLAN 802.1Q i TRUNK na wszystkich portach
8) Rozmiar tablicy adresów MAC urządzenia - co najmniej 16000.
9) Obsługa co najmniej 1024 sieci VLAN.
10) Wsparcie dla protokołów Spanning Tree: STP, RSTP, MSTP, PVST.
11) Urządzenie musi zapewniać obsługę Jumbo Frame o rozmiarze co najmniej 9198 bajtów.
12) Urządzenie musi wspierać następujące mechanizmy związane z bezpieczeństwem sieci:
    1. Obsługa mechanizmu IP DHCP SNOOPING.
    2. Obsługa minimum 1500 wpisów ACL.
    3. Obsługa protokołu TACACS+, implementacja powinna umożliwiać:
        - Uwierzytelnienie (Authentication) użytkownika,
        - Autoryzację (Authorization) i księgowanie (Accounting) każdej z komend wykonywanej przez użytkownika z poziomu SSH i CLI.
        - Możliwość zdefiniowania kliku serwerów TACACS+, wraz z automatycznym przełączeniem na inny serwer, w przypadku awarii aktywnego serwera.
    4. Obsługa protokołu RADIUS, implementacja powinna umożliwiać:
        - Obsługę protokołu 802.1x.
        - Obsługę uwierzytelnienia urządzeń nieposiadających wbudowanego suplikanta 802.1x, przy użyciu adresu MAC (MAB).
        - Obsługę uwierzytelnienia minimum 5 urządzeń na jednym porcie przełącznika.
        - Możliwość wyboru kolejności i priorytetu uwierzytelnienia na porcie(np. 802.1x, MAB)
        - Obsługę list kontroli dostępu (ACL) wysyłanych z serwera NAC (per użytkownik /urządzenie),
        - Obsługę dynamicznego przydzielania VLAN przez serwer NAC,
        - Mechanizm pozwalający na wysyłanie, do serwera NAC, adresu IP (uwierzytelnionego urządzenia) przydzielonego w sposób dynamiczny,

- Mechanizm pozwalający na wysyłanie, do serwera NAC, statycznego adresu IP (uwierzytelnionego urządzenia).

5. Obsługę mechanizmu CoA w zakresie:
   - Disconnect – po wysłaniu pakietu CoA, urządzenie zostanie uwierzytelnione ponownie z nowym numerem sesji (SessionID).
   - Port-Bounce - po wysłaniu pakietu CoA, port, do którego urządzenie jest podłączone zostanie włączony i wyłączony.

13) Możliwość zdefiniowania minimum 5 serwerów radius, wraz z możliwością przełączenia na inny serwer, w przypadku awarii aktywnego serwera.

14) Zarządzanie:
   1. CLI;
   2. HTTPS;
   3. SSHv2.

15) Obsługiwane protokoły
   1. ICMP;
   2. SNMP;
   3. SNMPv2;
   4. SNMPv3;
   5. NTP – Klient;
   6. TFTP – Klient;
   7. DHCP Client;
   8. DHCP Relay.

Zadanie 4:

Przełącznik sieciowy – „typ 4"

1) Montaż w szafie 19" rack. System musi być dostarczony ze wszystkimi komponentami do instalacji w szafie rack 19".
2) Liczba portów optycznych minimum 1 Gbps co najmniej 4 sztuki.
3) Liczba portów Gigabit Ethernet 1000 Base-T co najmniej 48 .
4) Wszystkie porty Ethernet (miedziane) muszą być dostępne od przodu urządzenia.
5) Urządzenie musi zapewniać przepustowość magistrali wewnętrznej (switching capacity) co najmniej 104 Gb/s
6) Musi istnieć możliwość tworzenia połączeń typu Link Aggregation zgrupowanych na czterech fizycznych portach zgodnych z IEEE 802.3ad (LACP).
   Połączenie urządzeń typu Link Aggregation nie może zmniejszać dostępnej ilości portów Ethernet.
7) Obsługa VLAN 802.1Q i trunk na wszystkich portach
8) Rozmiar tablicy adresów MAC urządzenia - co najmniej 16000.
9) Obsługa co najmniej 1024 sieci VLAN.
10) Wsparcie dla protokołów Spanning Tree: STP, RSTP, MSTP, PVST.
11) Urządzenie musi zapewniać obsługę Jumbo Frame o rozmiarze co najmniej 9198 bajtów.
12) Urządzenie musi wspierać następujące mechanizmy związane z bezpieczeństwem sieci:
    b) Obsługa mechanizmu IP DHCP SNOOPING.
    c) Obsługa minimum 1500 wpisów ACL.
    d) Obsługa protokołu TACACS+, implementacja powinna umożliwiać:
        - Uwierzytelnienie (Authentication) użytkownika,
        - Autoryzację (Authorization) i księgowanie (Accounting) każdej z komend wykonywanej przez użytkownika z poziomu SSH i CLI.
        - Możliwość zdefiniowania kliku serwerów TACACS+, wraz z automatycznym przełączeniem na inny serwer, w przypadku awarii aktywnego serwera.
    e) Obsługa protokołu RADIUS, implementacja powinna umożliwiać:

- Obsługę protokołu 802.1x,
- Obsługę uwierzytelnienia urządzeń nieposiadających wbudowanego suplikanta 802.1x, przy użyciu adresu MAC (MAB),
- Obsługę uwierzytelnienia minimum 5 urządzeń na jednym porcie przełącznika,
- Możliwość wyboru kolejności i priorytetu uwierzytelnienia na porcie(np. 802.1x, MAB)
- Obsługę list kontroli dostępu (ACL) wysyłanych z serwera NAC (per użytkownik /urządzenie),
- Obsługę dynamicznego przydzielania VLAN przez serwer NAC,
- Mechanizm pozwalający na wysyłanie, do serwera NAC, adresu IP (uwierzytelnionego urządzenia) przydzielonego w sposób dynamiczny,
- Mechanizm pozwalający na wysyłanie, do serwera NAC, statycznego adresu IP (uwierzytelnionego urządzenia).

f) Obsługę mechanizmu CoA w zakresie:

- Disconnect – po wysłaniu pakietu CoA, urządzenie zostanie uwierzytelnione ponownie z nowym numerem sesji (SessionID).
- Port-Bounce- po wysłaniu pakietu CoA port, do którego urządzenie jest podłączone zostanie włączony i wyłączony.

13) Możliwość zdefiniowania minimum 5 serwerów radius, wraz z możliwością przełączenia na inny serwer, w przypadku awarii aktywnego serwera.

14) Zarządzanie:

a. CLI;
b. HTTPS;
c. SSHv2.

15) Obsługiwane protokoły

a. ICMP
b. SNMP
c. SNMPv2

d. SNMPv3
e. NTP – Klient
f. TFTP – Klient
g. DHCP Client
h. DHCP Relay