SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia objętym niniejszym zapytaniem jest **dostawa kompletu elementów i podzespołów niezbędnych do wydzielenia z istniejącej teleinformatycznej infrastruktury sieciowej, infrastruktury Systemu Monitoringu Wizyjnego (CCTV) wraz z ich montażem i integracją z BMS (Building Monitoring System) i SMS (Security Monitoring System) w obiekcie przy ul. Poligonowej 3 w Warszawie.**

W związku z koniecznością wydzielenia z istniejącej teleinformatycznej infrastruktury sieciowej, infrastruktury Systemu Monitoringu Wizyjnego (CCTV), Zamawiający planuje dostawę kompletu elementów i podzespołów niezbędnych do wydzielenia systemu CCTV wraz z ich montażem i integracją z systemem zarządzania siecią ExtremeNetworks XMC oraz oprogramowaniem zarządzającym Axxon PSIM zintegrowanym z SMS (Security Monitoring System) w następującym zakresie:

a. dostawa przełączników agregacyjnych (switchy) marki Extreme Networks o symbolu 5520-48SE lub równoważnych;
b. wydzielenie z istniejącej teleinformatycznej infrastruktury sieciowej budynku, infrastruktury Systemu Monitoringu Wizyjnego (CCTV);
c. zintegrowanie wydzielonego systemu CCTV z systemem zarządzania siecią Extreme Networks XMC;
d. zintegrowanie systemu CCTV z istniejącym oprogramowaniem zarządzającym Axxon PSIM zintegrowanym z SMS (Security Monitoring System);
e. zintegrowanie systemu CCTV z istniejącym systemem kontroli dostępu Noder.

W celu wykonania powyższego Wykonawca zobowiązany byłby do wykonania następujących działań:

a. dostawy 2 szt. przełączników agregacyjnych (switchy) marki Extreme Networks o symbolu 5520-48SE lub równoważnych;
b. dostawy i montażu 132 szt. modułów 1Gb SFP+ MMF SR (33 x 2 x 2) i tyle samo patchcordów MMF 1m lub 2m do podłączenia switchy z kamerami i serwerami NVR do switchy agregujących;
c. dostawy i montażu 4 szt. modułów 1Gb SFP+ SMF LR i tyle samo patchcordów SMF 1m lub 2m do podłączenia między dwoma switchami agregującymi;
d. dostawy i wdrożenia niezbędnego oprogramowania (licencji Axxon) do integracji przełączników z Axxon PSIM dla prawidłowej pracy systemu;
e. dostawy i montażu niezbędnego okablowania;
f. przełożenia istniejących przełączników Stackowych w wolne miejsce w szafach RACK;
g. wykonania integracji wydzielonego systemu CCTV z istniejącym oprogramowaniem zarządzającym Axxon PSIM;
h. wykonania rekonfiguracji sieci LAN;
i. sporządzenia dokumentacji powykonawczej wydzielonego systemu CCTV.

Szczegółowy opis dotyczący przełączników agregacyjnych:

Przełączniki agregacyjne muszą spełniać niżej wymienione wymagania:

Wymagania ogólne.

1. Przełącznik wyposażony w 48 portów SFP.
2. Porty SFP muszą pozwalać na pracę z prędkością 100Mb/s lub 1Gb/s w zależności od zainstalowanego modułu.
3. Przełącznik być wyposażony w min. 4 porty SFP+ 10Gb/s. Jednocześnie musi być możliwe modernizacja tych portów do portów SFP28 10/25 Gb/s.
4. Przełącznik musi mieć możliwość wsparcia szyfracji MACsec 128/256-bit na min. 48 portach. Jeżeli obsługa MACsec wymaga dostarczenia dodatkowej licencji, to jej dostarczenie nie jest wymagane.
5. Wszystkie porty muszą być aktywne.
6. Wysokość urządzenia 1U, montaż w standardowej szafie Rack 19”.
7. Przełącznik musi posiadać zainstalowane dwa zasilacze 230V, które umożliwiają uzyskanie redundancji zasilania. Niedopuszczalna jest instalacja zasilaczy zewnętrznych.

8. Wymagana jest możliwość wymiany zasilacza w czasie działania przełącznika bez wpływu na jego pracę (ang. Hot-Swap).
9. Przełącznik musi zapewniać pobór powietrza z przodu i wyrzut powietrza z tyłu przełącznika oraz posiadać redundantne wentylatory z możliwością ich wymiany w czasie działania przełącznika bez wpływu na jego pracę (ang. Hot-Swap).
10. Przełącznik musi posiadać dedykowane porty (niezależne od wyspecyfikowanych powyżej) do łączenia przełączników w stos z wydajnością min. 160 Gb/s.
11. Porty dedykowane do łączenia przełączników w stos muszą mieć możliwość pracy jako standardowy port 40Gb/s, 4x10Gb/s lub 4x25Gb/s.
12. Możliwość łączenia do 8 przełączników w stos.
13. Nieblokująca architektura o wydajności przełączania min. 690 Gb/s.
14. Szybkość przełączania min. 510 Milionów pakietów na sekundę.
15. Temperatura pracy przełącznika w zakresie min. 0^{o} do 50^{o} C.
16. Tablica MAC adresów min. 40 tys.
17. Pamięć operacyjna: min. 2 GB pamięci DRAM.
18. Pamięć flash: min. 2 GB pamięci Flash.
19. Obsługa sieci wirtualnych IEEE 802.1Q – min. 4059.
20. Obsługa funkcjonalności Private VLAN - blokowanie ruchu pomiędzy klientami z umożliwieniem łączności do wspólnych zasobów sieci.
21. Wsparcie dla ramek Jumbo Frames (min. 9216 bajtów).
22. Obsługa Quality of Service:
    a. Rozpoznawanie i realizacja priorytetów ustawionych w ramach IEEE 802.1p;
    b. Rozpoznawanie i realizacja priorytetów ustawionych w ramach DiffServ;
    c. 8 kolejek priorytetów na każdym porcie wyjściowym;
    d. Obsługa kolejek Strict Priority;
    e. Obsługa kolejek Weighted Round Robin;
    f. Obsługa WRED (Weighted Random Early Detection).
23. Obsługa Link Layer Discovery Protocol LLDP IEEE 802.1AB.
24. Obsługa LLDP Media Endpoint Discovery (LLDP-MED).
25. Obsługa CDPv2 z obsługą Voice VLAN.
26. Przełącznik wyposażony w modularny system operacyjny z ochroną pamięci, procesów oraz zasobów procesora.
27. Możliwość instalacji min. dwóch wersji oprogramowania – firmware.
28. Możliwość przechowywania min. 10 wersji konfiguracji w plikach tekstowych w pamięci Flash.
29. Możliwość monitorowania zajętości CPU oraz pamięci.
30. Lokalna i zdalna możliwość monitoringu pakietów (Local and Remote Mirroring).
31. Obsługa Wirtualnych Routerów - możliwość uruchomienia oddzielnych procesów protokołu dynamicznego routingu z oddzielnymi tablicami. Możliwość użycia tych samych podsieci w różnych wirtualnych routerach.
32. Wbudowany dodatkowy port Gigabit Ethernet do zarządzania poza pasmem - out of band management.
33. Dedykowany port konsoli szeregowej RJ45.
34. Wbudowany port USB pozwalający na łatwe przenoszenie konfiguracji oraz oprogramowania przełącznika.

Obsługa Routingu IPv4.

1. Sprzętowa obsługa IPv4 forwarding.
2. Pojemność tabeli routingu min. 15 000 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego IPv4:
    a. RIP v1/v2;
    b. OSPFv2 – możliwość rozszerzenia przez licencje, licencja nie jest wymagana;
    c. BGPv4 – możliwość rozszerzenia przez licencje, licencja nie jest wymagana;
    d. IS-IS – możliwość rozszerzenia przez licencje, licencja nie jest wymagana.
5. Policy Based Routing dla IPv4.
6. Obsługa DHCP/BootP Relay dla IPv4 z możliwością wysłania zapytań jednocześnie do min. 4 serwerów.

Obsługa Routingu IPv6.

1. Sprzętowa obsługa IPv6 forwarding.
2. Pojemność tabeli routingu min. 7500 wpisów.
3. Routing statyczny.
4. Obsługa routingu dynamicznego dla IPv6:
    a. RIPng;
    b. OSPF v3 – możliwość rozszerzenia przez licencje, licencja nie jest wymagana;
    c. BGPv4 – możliwość rozszerzenia przez licencje, licencja nie jest wymagana;
    d. IS-IS – możliwość rozszerzenia przez licencje, licencja nie jest wymagana.
5. Obsługa 6to4 (RFC 3056).
6. Obsługa MLDv1 (Multicast Listener Discovery version 1).
7. Obsłgua MLDv2 (Multicast Listener Discovery version 2).
8. Policy Based Routing dla IPv6.
9. Opcja IPv6 Router Advertisement dla DNS – RFC 6106.

Obsługa Multicastów.

1. Statyczne przyłączanie do grupy multicast.
2. Filtrowanie IGMP.
3. Obsługa PIM-SM – możliwość rozszerzenia przez licencje.
4. Obsługa PIM-DM – możliwość rozszerzenia przez licencje.
5. Obsługa PIM-SSM – możliwość rozszerzenia przez licencje.
6. Obsługa Multicast VLAN Registration – MVR.
7. Obsługa IGMP v1 – RFC 1112.
8. Obsługa IGMP v2 – RFC 2236.
9. Obsługa IGMP v3 – RFC 3376.
10. Obsługa IGMP v1/v2/v3 snooping .
11. Możliwość konfiguracji statycznych tras dla Routingu Multicastów.

Bezpieczeństwo.

1. Obsługa logowania do sieci Network Login:
    a. IEEE 802.1x based Network Login;
    b. MAC based Network Login;
    c. Web-based Network Login.
2. Obsługa wielu klientów Network Login na jednym porcie (Multiple supplicants).
3. Obsługa logowania do sieci z wykorzystaniem IEEE 802.1x oraz MAC authentication na portach pracujących w trybie Link Aggregation.
4. Przydział sieci VLAN, ACL/QoS podczas logowania do sieci IEEE 802.1x, MAC authentication.
5. Obsługa Guest VLAN dla IEEE 802.1x.
6. Możliwość przekierowania na Captive Portal podczas logowania do sieci .
7. Obsługa wymuszenia autoryzacji w celu zmiany autoryzacji (VLAN, ACL, QoS) bez konieczności wyłączania i włączania portu – CoA RFC 5176.
8. Obsługa TACACS+ (RFC 1492).
9. Obsługa RADIUS Authentication (RFC 2138).
10. Obsługa RADIUS Accounting (RFC 2139).
11. RADIUS per-command Authentication.
12. 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.
13. Możliwość wyłączenia MAC learning.
14. 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.
15. Dwukierunkowe (ingress oraz egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4:
    a. Adres MAC źródłowy i docelowy plus maska;

b. Adres IP źródłowy i docelowy plus maska dla IPv4 oraz IPv6;
c. Protokół - np. UDP, TCP, ICMP, IGMP, OSPF, PIM, IPv6 itd.;
d. Numery portów źródłowych i docelowych TCP, UDP;
e. Zakresy portów źródłowych i docelowych TCP, UDP;
f. Identyfikator sieci VLAN – VLAN ID;
g. Quality of Service IEEE 802.1p oraz DiffServ;
h. Flagi TCP;
i. Obsługa fragmentów.

16. Dwukierunkowe listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszania wydajności przełącznika.
17. W ramach ALC możliwość konfiguracji min. 9000 reguł na wejściu i 1000 reguł na wyjściu.
18. Możliwość zliczania pakietów lub bajtów trafiających do konkretnej ACL i w przypadku przekroczenia skonfigurowanych wartości podejmowania akcji np. blokowanie ruchu, przekierowanie do kolejki o niższym priorytecie, wysłanie trapu SNMP, wysłanie informacji do serwera Syslog lub wykonanie komend CLI.
19. Obsługa bezpiecznego transferu plików SCP/SFTP.
20. Obsługa DHCP Option 82.
21. Obsługa IP Security – Trusted DHCP Server.
22. Obsługa IP Security – DHCP Snooping and Guard.
23. Obsługa IP Security - Gratuitous ARP Protection.
24. Obsługa IP Security – DHCP Secured ARP/ARP Validation.
25. Obsługa IP Security – IP Source guard.
26. Ograniczanie przepustowości (rate limiting) na portach wyjściowych oraz ruchu wybranego poprzez ACL.
27. Obsługa wykrywania periodycznego zaniku linku (Port-Flap). Musi istnieć możliwość zdefiniowania liczby zaniku linku w czasie określonego czasu oraz reakcji polegającej na wyłączeniu portu na stałe lub na wskazany czas. Zdarzenie musi być raportowane poprzez Trap SNMP i/lub Syslog.

Bezpieczeństwo sieciowe.

1. Obsługa redundancji routingu VRRP.
2. Obsługa STP (Spinning Tree Protocol) IEEE 802.1D.
3. Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w.
4. Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s.
5. Obsługa PVST+ lub kompatybilna.
6. Obsługa ERPS / G.8032.
7. Obsługa Link Aggregation IEEE 802.3ad wraz z LACP; możliwość utworzenia 128 grup portów oraz tworzenia grup składających się z 32 portów.
8. Obsługa MLAG - połączenie link aggregation IEEE 802.3ad do dwóch niezależnych przełączników.
9. Obsługa LACP w ramach MLAG.

Zarządzanie.

1. Obsługa synchronizacji czasu SNTP lub NTP.
2. Zarządzanie przez SNMP v1/v2/v3.
3. Zarządzanie przez przeglądarkę WWW – protokół http i https.
4. Możliwość zarządzania przez protokół XML.
5. Telnet Serwer/Klient dla IPv4 / IPv6.
6. SSH2 Serwer/Klient dla IPv4 / IPv6.
7. Ping dla IPv4 / IPv6.
8. Traceroute dla IPv4 / IPv6.
9. Obsługa SYSLOG z możliwością definiowania wielu serwerów.
10. Sprzętowa obsługa sFlow.
11. Obsługa RMON oraz RMON2 (RFC 2021).

Inne.

1. Współpraca z systemem kontroli dostępu posiadanym przez Zamawiającego.
2. Wbudowany DHCP Serwer i klient z możliwością definicji opcji (np. opcje 43, 60, 78 itp.).
3. Wsparcie standardu IEEE 802.1Qcj – Automatic Attachment to Provider Backbone Bridging.

4. Obsługa skryptów CLI.
5. Obsługa funkcji TCL/Tk w skryptach CLI.
6. Obsługa skryptów Python.
7. Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych).
8. Możliwość uruchamiania skryptów:
    a. Ręcznie;
    b. O określonym czasie lub co wskazany okres czasu;
    c. Na podstawie wpisów w logu systemowym.