Opis przedmiotu zamówienia -

Opis funkcjonalny

Zawartość

1 Wstęp

W dokumencie tym zostały opisane elementy i wymagania:

- elementy, jakie wchodzą w skład sieci internetowej
- sposób konfiguracji urządzeń
- sposób integracji z istniejącymi systemami na Uniwersytecie Rzeszowskim

Celem opracowania jest zaprojektowanie remontu sieci LAN, Wi-Fi spełniającej oczekiwania inwestora.

Głównymi celami Zamawiającego są:

- remont sieci istniejącej – kablowej z umożliwieniem z korzystania z sieci Wi-Fi przeznaczonej dla mieszkańców akademików URZ, będącymi studentami uczelni
    - sieć Wi-Fi musi być oparta o kontroler umożliwiającym zarządzenie całością infrastruktury Wi-Fi oraz AP-tami
- remont sieci istniejącej – kablowej z umożliwieniem z korzystania z sieci Wi-Fi przeznaczonej dla mieszkańców akademików URZ niebędących studentami URZ
- wymiana istniejących przełączników na nowe, obsługujące istniejącą sieć LAN oraz umożliwiających podłączenia AP-tów po portach PoE+
- wymiana istniejącego urządzenia dostępowego do sieci Internet(systemu bezpieczeństwa) umożliwiającego jednocześnie identyfikację użytkowników korzystających z sieci oraz umożliwiającego logowanie sesji/ruchu użytkowników
- modernizacja dostępu do sieci internetowej poprzez montaż AP wraz z doprowadzeniem okablowania w celu połączenia urządzeń do sieci LAN
- integracja z obecnie wykorzystywanym Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej oraz istniejącą siecią Wi-Fi „eduroam”
- konfiguracja sieci LAN umożliwiająca
    - blokowanie mac adresów na portach dostępowych
    - blokowanie obcych serwerów DHCP
    - blokowanie statycznych adresów IP na portach przełączników(użytkownicy mają otrzymywać adresy IP z uczelnianego serwera DHCP)

W celu realizacji projektu należy zdemontować wymieniane urządzenia pozostawiając je inwestorowi oraz dostarczyć niżej wymiennie urządzenia w podziale na poszczególne kategorie.

2 Remont instalacji sieci.

W ramach realizacji projektu należy wykonać następujące prace.

1. Demontaż istniejących urządzeń aktywnych
2. Instalacja nowych urządzeń aktywnych
3. Ułożenie i montaż kanałów kablowych, montaż instalacji elektrycznej oraz montaż gniazd sieciowych niezbędnych dla potrzeb instalacji AP-tów
4. Przebicia przez ściany/stropy dla potrzeb instalacji sieci internetowej oraz wykonanie drobnych prac malarskich po wykonaniu robót budowlanych,
5. Wykonanie instalacji światłowodowej pomiędzy punktami dystrybucyjnymi wraz z pomiarami:
    a. światłowód wielomodowy 12-włóknowy z PD_2 do PD_0
    b. światłowód wielomodowy 12-włóknowy z PD_2 do PD_4
6. Montaż AP-tów w wyznaczonych przez Zamawiającego miejscach

Podczas wykonywania instalacji kablowych należy dostarczyć przełącznice światłowodowe w punktach dystrybucyjnych, organizery kabli, panele krosowe, kasetę zapasu kabla światłowodowego oraz wszystkie inne niezbędne elementy potrzebne do prawidłowego wykonania instalacji.

3 Dostawa urządzeń

W ramach projektu należy dostarczyć następujące urządzenia aktywne.

Zamawiający wymaga aby oferowane przełączniki pochodziły z legalnego kanału dystrybucyjnego określonego przez producenta. Zamawiający zastrzega sobie możliwość wystosowania po dostawie sprzętu zapytania do producenta z prośbą o weryfikację numerów seryjnych w celu potwierdzenia zgodności z powyższymi wymogami i zastrzega sobie prawo odstąpienia od podpisania protokołu odbioru sprzętu w przypadku nie spełnienia powyższych zapisów.

3.1 Przełączniki do punktu dystrybucyjnego PD_0

Do punktu PD_0 należy dostarczyć przełącznik sieciowy o parametrach jak poniżej, dokonać jego instalacji i konfiguracji zgodnie z wymogami opisanymi w poniższych punktach.

Przełącznik sieciowy 24 portowy o parametrach nie gorszych niż – **ilość 1:**

1. Minimum 24 porty 10BASE-T/100BASE-TX/1000BASE-T wspierające standard 802.3at (PoE+)
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).

Przełącznik wyposażony w min. wkładkę SFP+ 10GbBaseSR.

3. Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 95 Mp/s
5. Tablica adresów MAC o wielkości minimum 16000 pozycji
6. Bufor pakietów nie mniejszy niż 1,5MB
9. Budżet mocy dla PoE minimum 370W
10. Obsługa ramek Jumbo
11. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+), nie mniej niż 210 portów 100/1000BaseX i ich kombinacji.
12. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
13. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
14. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP
15. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng
16. Policy Based Routing
17. Wsparcie dla Bidirectional Forwarding Detection (BFD)
18. Minimum 32 interfejsy IP VLAN
19. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
20. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
21. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
22. Obsługa IEEE 802.1ad QinQ i Selective QinQ
23. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
24. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
25. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)
26. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
27. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
28. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
29. Obsługa standardu 802.1p – min. 8 kolejek na porcie

30. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p

31. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP

32. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s

33. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring

34. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

• Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x

• Możliwość uwierzytelniania wielu użytkowników na jednym porcie

• Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS

• Przypisanie profilu QoS dla użytkownika lub grupy użytkowników

35. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED

36. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC

37. TACACS+ i RADIUS Network Login

38. RADIUS Accounting

39. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS

40. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https

41. Syslog

42. Obsługa NETCONF

43. Obsługa sFlow

44. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3

45. Obsługa NTP i SNTP

46. Obsługa protokołów 802.3ah oraz 802.1ag

47. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter

48. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).

49. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

50. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien 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 nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

51. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego
52. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol
53. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych
54. Minimalny zakres pracy od -5°C do 45°C
55. Wysokość w szafie 19" – 1U, głębokość nie większa niż 30 cm
56. Maksymalny pobór mocy (z pełnym obciążeniem PoE) nie większy niż 500W
57. Przełącznik - gwarancja co najmniej 60 miesięcy, obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Dodatkowo wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji
58. Pozostałe elementy min. 12 miesięcy.

3.2 Przełączniki do punktu dystrybucyjnego PD_2

Do punktu PD_2 należy dostarczyć przełączniki sieciowe o parametrach jak poniżej, dokonać ich instalacji i konfiguracji zgodnie z wymogami opisanymi w poniższych punktach:

a) Przełącznik sieciowy 48 portowy o parametrach nie gorszych niż – **ilość 1:**

1. Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T wspierających standard 802.3at (PoE+)
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Przełącznik wyposażony w kabel DAC QSFP+ o długości co najmniej 0,6 metra.
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 130,9 Mp/s
5. Tablica adresów MAC o wielkości minimum 16000 pozycji
6. Bufor pakietów nie mniejszy niż 3MB
9. Budżet mocy dla PoE minimum 370W
10. Obsługa ramek Jumbo

11. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+), nie mniej niż 210 portów 100/1000BaseX i ich kombinacji.
12. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
13. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
14. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP
15. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng
16. Policy Based Routing
17. Wsparcie dla Bidirectional Forwarding Detection (BFD)
18. Minimum 32 interfejsy IP VLAN
19. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
20. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
21. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
22. Obsługa IEEE 802.1ad QinQ i Selective QinQ
23. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
24. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
25. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)
26. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
27. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
28. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
29. Obsługa standardu 802.1p – min. 8 kolejek na porcie
30. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p
31. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
32. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
33. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
34. Obsługa funkcji logowania do sieci („Network Login”) zgodna ze standardem IEEE 802.1x:

• Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x

• Możliwość uwierzytelniania wielu użytkowników na jednym porcie

• Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS

• Przypisanie profilu QoS dla użytkownika lub grupy użytkowników

35. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED

36. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC

37. TACACS+ i RADIUS Network Login

38. RADIUS Accounting

39. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS

40. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https

41. Syslog

42. Obsługa NETCONF

43. Obsługa sFlow

44. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3

45. Obsługa NTP i SNTP

46. Obsługa protokołów 802.3ah oraz 802.1ag

47. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter

48. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).

49. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

50. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien 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 nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

51. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego

52. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol

53. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych

54. Minimalny zakres pracy od -5°C do 45°C

55. Wysokość w szafie 19" – 1U, głębokość nie większa niż 40 cm

56. Maksymalny pobór mocy (z pełnym obciążeniem PoE) nie większy niż 500W

57. Przełącznik - gwarancja co najmniej 60 miesięcy, obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Dodatkowo wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji.

58. Pozostałe elementy min. 12 miesięcy.

b) Przełącznik sieciowy 48 portowy o parametrach nie gorszych niż – **ilość 2:**

1. Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T

2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).

Każdy przełącznik wyposażony w min. kabel DAC QSFP+ o długości co najmniej 0,6 metra.

Każdy przełącznik wyposażony min. w wkładkę SFP+ 10GbBaseSR.

3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)

4. Wydajność: minimum 130,9 Mp/s

5. Tablica adresów MAC o wielkości minimum 16000 pozycji

6. Bufor pakietów nie mniejszy niż 3MB

9. Obsługa ramek Jumbo

10. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+), nie mniej niż 210 portów 100/1000BaseX i ich kombinacji.

11. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))

12. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie

13. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP

14. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng

15. Policy Based Routing

16. Wsparcie dla Bidirectional Forwarding Detection (BFD)

17. Minimum 32 interfejsy IP VLAN
18. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
19. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
20. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
21. Obsługa IEEE 802.1ad QinQ i Selective QinQ
22. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
23. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom
24. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)
25. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
26. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia
27. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)
28. Obsługa standardu 802.1p – min. 8 kolejek na porcie
29. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p
30. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP
31. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s
32. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
33. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

• Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x
• Możliwość uwierzytelniania wielu użytkowników na jednym porcie
• Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS
• Przypisanie profilu QoS dla użytkownika lub grupy użytkowników

34. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
35. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
36. TACACS+ i RADIUS Network Login
37. RADIUS Accounting
38. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
39. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
40. Syslog
41. Obsługa NETCONF

42. Obsługa sFlow

43. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3

44. Obsługa NTP i SNTP

45. Obsługa protokołów 802.3ah oraz 802.1ag

46. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter

47. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).

48. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

49. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien 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 nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

50. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego

51. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol

52. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych

53. Minimalny zakres pracy od -5°C do 45°C

54. Wysokość w szafie 19” – 1U, głębokość nie większa niż 30 cm

55. Maksymalny pobór mocy nie większy niż 50W

57. Przełącznik - gwarancja co najmniej 60 miesięcy, obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Dodatkowo wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji.

58. Pozostałe elementy min. 12 miesięcy.

3.3 Przełączniki do punktu dystrybucyjnego PD_4

Do punktu PD_4 należy dostarczyć przełączniki sieciowe o parametrach jak poniżej, dokonać ich instalacji i konfiguracji zgodnie z wymogami opisanymi w poniższych punktach.

a) Przełącznik sieciowy 24 portowy o parametrach nie gorszych niż – **ilość 1:**

1. Minimum 24 porty 10BASE-T/100BASE-TX/1000BASE-T wspierające standard 802.3at (PoE+)
2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP).

Przełącznik wyposażony w min. kabel DAC QSFP+ o długości co najmniej 0,6 metra.

Przełącznik wyposażony w min. wkładkę SFP+ 10GbBaseSR.

3. Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 95 Mp/s
5. Tablica adresów MAC o wielkości minimum 16000 pozycji
6. Bufor pakietów nie mniejszy niż 1,5MB
9. Budżet mocy dla PoE minimum 370W
10. Obsługa ramek Jumbo
11. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+), nie mniej niż 210 portów 100/1000BaseX i ich kombinacji.
12. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))
13. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie
14. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP
15. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng
16. Policy Based Routing
17. Wsparcie dla Bidirectional Forwarding Detection (BFD)
18. Minimum 32 interfejsy IP VLAN
19. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
20. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol
21. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN
22. Obsługa IEEE 802.1ad QinQ i Selective QinQ
23. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree

24. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom

25. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)

26. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI

27. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia

28. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)

29. Obsługa standardu 802.1p – min. 8 kolejek na porcie

30. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p

31. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP

32. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s

33. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring

34. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:

• Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x

• Możliwość uwierzytelniania wielu użytkowników na jednym porcie

• Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS

• Przypisanie profilu QoS dla użytkownika lub grupy użytkowników

35. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED

36. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC

37. TACACS+ i RADIUS Network Login

38. RADIUS Accounting

39. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS

40. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https

41. Syslog

42. Obsługa NETCONF

43. Obsługa sFlow

44. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3

45. Obsługa NTP i SNTP

46. Obsługa protokołów 802.3ah oraz 802.1ag

47. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter

48. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).

49. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).

50. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien 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 nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.

51. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego

52. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol

53. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych

54. Minimalny zakres pracy od -5°C do 45°C

55. Wysokość w szafie 19” – 1U, głębokość nie większa niż 30 cm

56. Maksymalny pobór mocy (z pełnym obciążeniem PoE) nie większy niż 500W

57. Przełącznik - gwarancja co najmniej 60 miesięcy, obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Dodatkowo wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji.

58. Pozostałe elementy min. 12 miesięcy.

b) Przełącznik sieciowy 48 portowy o parametrach nie gorszych niż – **ilość 3:**

1. Minimum 48 portów 10BASE-T/100BASE-TX/1000BASE-T

2. Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP). Każdy przełącznik wyposażony w min. kabel DAC QSFP+ o długości co najmniej 0,6 metra.

3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)

4. Wydajność: minimum 130,9 Mp/s

5. Tablica adresów MAC o wielkości minimum 16000 pozycji

6. Bufor pakietów nie mniejszy niż 3MB

9. Obsługa ramek Jumbo

10. Funkcja łączenia urządzeń w stosy z wykorzystaniem portów 10Gb/s i agregowanych portów 10Gb/s. Urządzenia połączone w stos widziane jako jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Wymagane jest by urządzania tworzące stos mogły posiadać łącznie nie mniej niż 390 portów 100/1000BaseT (z obsługą i bez obsługi standardu PoE+), nie mniej niż 210 portów 100/1000BaseX i ich kombinacji.

11. Topologia stosu musi zapewniać redundancję (połączenia typu pierścień lub mesh, nie dopuszcza się topologii typu łańcuch (daisy-chain))

12. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie

13. Routing IPv4 – minimum: statyczny (minimum 512 tras), RIP

14. Routing IPv6 – minimum: statyczny (minimum 256 tras), RIPng

15. Policy Based Routing

16. Wsparcie dla Bidirectional Forwarding Detection (BFD)

17. Minimum 32 interfejsy IP VLAN

18. Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping

19. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol

20. Obsługa sieci IEEE 802.1Q VLAN – minimum 4094 sieci VLAN

21. Obsługa IEEE 802.1ad QinQ i Selective QinQ

22. Funkcja Root Guard umożliwiająca ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree

23. BPDU Guard – funkcja umożliwiająca wyłączenie portów Fast Start w momencie odebrania na tym porcie ramek BDPU w celu przeciwdziałania pętlom

24. Wsparcie dla funcji DHCP server, DHCP Relay, DHCP client oraz DHCP Snooping (wszystkie dla IPv4 i IPv6)

25. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI

26. Listy ACL muszą być obsługiwane sprzętowo, bez pogarszania wydajności urządzenia

27. Możliwość realizacji tzw. czasowych list ACL (list reguł dostępu, działających w określonych odcinkach czasu)

28. Obsługa standardu 802.1p – min. 8 kolejek na porcie

29. Możliwość zmiany wartości pola DSCP i wartości priorytetu 802.1p

30. Możliwość wyboru sposobu obsługi kolejek – Strict Priority (SP); Weighted Round Robin (WRR); WRR + SP

31. Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczania pasma dla ruchu określonego listą ACL z dokładnością do 64 kb/s

32. Funkcja mirroringu portów lokalnego i zdalnego: 1 to 1 Port mirroring, Many to 1 port mirroring
33. Obsługa funkcji logowania do sieci („Network Login") zgodna ze standardem IEEE 802.1x:
• Możliwość przydziału stacji do wskazanej sieci wirtualnej podczas logowania IEEE 802.1x
• Możliwość uwierzytelniania wielu użytkowników na jednym porcie
• Możliwość obsługi wielu domen, z których każda może być przypisana do własnego serwera RADIUS
• Przypisanie profilu QoS dla użytkownika lub grupy użytkowników
34. LLDP - IEEE 802.1AB Link Layer Discovery Protocol oraz LLDP-MED
35. Możliwość stworzenia lokalnej bazy użytkowników dla autoryzacji IEEE 802.1x oraz MAC
36. TACACS+ i RADIUS Network Login
37. RADIUS Accounting
38. Możliwość centralnego uwierzytelniania administratorów na serwerze RADIUS
39. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https
40. Syslog
41. Obsługa NETCONF
42. Obsługa sFlow
43. Obsługa protokołu OpenFlow w wersji, co najmniej, 1.3
44. Obsługa NTP i SNTP
45. Obsługa protokołów 802.3ah oraz 802.1ag
46. Przełącznik musi posiadać mechanizm zdefiniowania i generowania testowych próbek ruchu sieciowego. Musi umożliwiać gromadzenie i podgląd statystyk z ich wykonania, obejmujących takie parametry jak RTT, Packet Loss, Jitter
47. Przechowywanie wielu wersji oprogramowania na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch wersji oprogramowania).
48. Przechowywanie wielu plików konfiguracyjnych na przełączniku (liczba wersji ograniczona jedynie dostępną pamięcią stałą, nie dopuszcza się rozwiązań pozwalających na przechowywanie jedynie dwóch konfiguracji).
49. Funkcja wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej. Plik konfiguracyjny urządzenia powinien 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 nowa konfiguracją. Zmiany aktywnej konfiguracji muszą być widoczne natychmiast - nie dopuszcza się częściowych restartów urządzenia po dokonaniu zmian.
50. Wsparcie dla Private VLAN (protected port / private port / isolated port, private edge port, isolated VLAN) lub równoważnego

51. Wsparcie dla mechanizmu typu DLDP - Device Link Detection Protocol

52. Ochrona przed sztormami pakietowymi (broadcast, multicast, unicast), z możliwością definiowania wartości progowych

53. Minimalny zakres pracy od -5°C do 45°C

54. Wysokość w szafie 19" – 1U, głębokość nie większa niż 30 cm

55. Maksymalny pobór mocy nie większy niż 50W

57. Przełącznik - gwarancja co najmniej 60 miesięcy, obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Dodatkowo wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji.

58. Pozostałe elementy min. 12 miesięcy.

3.4 Moduły do przełączników

Należy dostarczyć moduły SFP lub SFP+ działających na światłowodzie jednomodowym na jednym włóknie kompatybilne z kupowanymi przełącznikami oraz do przełącznika istniejącego HP 7500. Moduły te należy wykorzystać do zestawienia połączenia pomiędzy lokalizacjami: Akademiki – Centrala URZ.

Odległość pomiędzy lokalizacjami to około 20km. Zestawienie połączenia jest w zakresie Wykonawcy. Należy również dokonać rekonfiguracji istniejących przełączników rdzeniowych i firewalli na UR (CheckPoint) w celu zapewnienia prawidłowego działania nowo tworzonych sieci, tak aby z nowo definiowanych sieci zapewniły dostęp do udostępnianych zasobów centralnych (serwerów i systemów).

3.6 Firewall z systemem zbierania logów

W punkcie dystrybucyjnym PD_2 należy zamontować dostarczony Firewall o parametrach nie gorszych niż – **ilość 1:**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania administratorów do poszczególnych instancji systemu.

System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dyski:

1. System realizujący funkcję Firewall musi dysponować minimum 18 portami Gigabit Ethernet RJ-45, 4 gniazdami SFP 1 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.

3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 2 mln. jednoczesnych połączeń oraz 130 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 3,5 Gbps.
4. Wydajność szyfrowania VPN IPSec dla pakietów 512 B, przy zastosowaniu algorytmu AES256 – SHA256: nie mniej niż 7 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu HTTP - minimum 6 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1,1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL (TLS v1.2 z algorytmem AES128-SHA256) dla ruchu http – minimum 800 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Analiza ruchu szyfrowanego protokołem SSL oraz SSH.
10. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
11. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.

Polityki, Firewall

1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

- Translację jeden do jeden oraz jeden do wielu
- Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:

- Wsparcie dla IKE v1 oraz v2.
- Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM)
- Obsługa protokołu Diffiego-Hellman grup 19 i 20
- Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
- Tworzenie połączeń typu Site-to-site oraz Client-to-Site.
- Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
- Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
- Obsługa mechanizmów: IPSec NAT Traversal, DPD, XAuth
- Mechanizm „Split tunneling" dla połączeń Client-to-Site

2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:

- Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
- Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.

3. Dla modułów: IPSec VPN oraz SSL VPN – producent musi dostarczać klienta VPN współpracującego z oferowanym rozwiązaniem. Klient VPN musi umożliwiać weryfikację stanu bezpieczeństwa stacji zdalnej.

4. Rozwiązanie powinno zapewniać funkcjonalność VTEP (VXLAN Tunnel End Point)

Routing i obsługa łączy WAN

1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:

- Routingu statycznego
- Policy Based Routingu
- Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

2. System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Kontrola Antywirusowa

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń.

Ochrona przed atakami

1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
5. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2800 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P, Botnet.

5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware, phishing, spam, Dynamic DNS, proxy avoidance.

3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.

4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.

5. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.

6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:

- Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
- Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.

3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.

3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.

4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.

5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.

6. System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, zbieranie pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

Logowanie:

1. System musi mieć możliwość logowania do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikaty:

- ICSA lub EAL4 dla funkcji Firewall
- ICSA lub NSS Labs dla funkcji IPS
- ICSA dla funkcji: SSL VPN, IPSec VPN

5. Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu musi zostać zapewniony dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

6. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć (przed podpisaniem umowy) dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

7. Oferent winien przedłożyć (przed podpisaniem umowy) oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań podwójnego zastosowania.

Wraz z firewall-em należy dostarczyć system do zbierania i archiwizacji logów o parametrach nie gorszych niż – **ilość 1:**

System centralnego logowania, raportowania i korelacji logów.

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0, Microsoft Hyper-V 2008 R2/2012/2012 R2, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM.

Interfejsy, Dyski:

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 1 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 2 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:

a. Listę najczęściej wykrywanych ataków.

b. Listę najbardziej aktywnych użytkowników.

c. Listę najczęściej wykorzystywanych aplikacji.

d. Listę najczęściej odwiedzanych stron www.

e. Listę krajów , do których realizowana jest komunikacja.

f. Listę najczęściej wykorzystywanych polityk Firewall.

g. Informacje o realizowanych połączeniach IPSec.

4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów z do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów, co najmniej po typie logów (traffic, zdarzeń ataków, wykrycia malware'u, odwiedzanych stron, wykrytych aplikacji sieciowych).

5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: HTML, PDF, CSV.

2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.

3. Funkcję definiowania własnych raportów.

4. Możliwość spolszczenia raportów.

5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja Logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.

2. Konfigurację powiadomień poprzez: e-mail, SNMP v1/v2c/v3 w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.

3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii eventów:

- Malware.
- Kontroli aplikacji.
- Email.
- IPS.
- Traffic.
- Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

a. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać definiowanie wielu administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Gwarancja oraz wsparcie

3. Gwarancja: System musi być objęty serwisem gwarancyjnym przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu musi być zapewniony dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

4. W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca winien przedłożyć (przed podpisaniem umowy) dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

5. Oferent winien przedłożyć (przed podpisaniem umowy) oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań podwójnego zastosowania.

3.7 AP-ty do sieci bezprzewodowej

Pod potrzeby budowy sieci WiFi należy dostarczyć AP-ty o parametrach nie gorszych niż – **sztuk 15:**

Urządzenie musi być tzw. cienkim punktem dostępowym zarządzanym z poziomu kontrolera sieci bezprzewodowej. Obudowa urządzenia musi być wykonana z tworzywa sztucznego i umożliwiać montaż na

suficie wewnątrz budynku. Musi być wyposażone w dwa niezależne moduły radiowe pracujące w pasmach i obsługiwać następujące standardy:

1. 2.4 GHz lub 5 GHz b/g/n
2. 5 GHz a/n/ac

Urządzenie musi pozwalać na jednoczesne rozgłaszanie co najmniej 14 SSID

Liczba interfejsów Ethernet – min. 1 w standardzie 10/100/1000 Base-TX

Urządzenie powinno być zasilane poprzez interfejs ETH w standardzie 802.3af lub zewnętrzny zasilacz

Interfejs radiowy urządzenia powinien wspierać następujące funkcje:

1. MIMO – 2x2
2. Maksymalna przepustowość interfejsu dla poszczególnych pasm:

a) 2.4GHz – 300 Mbps

b) 5 GHz – 867 Mbps

3. Wymagana moc nadawania min. 20 dBm
4. Wsparcie dla 802.11n 20/40Mhz HT
5. Wsparcie dla kanału 80 MHz dla 802.11ac
6. Anteny – 4 wbudowane o zysku min. 3dBi dla pasma 2.4GHz, 6dBi dla pasma 5GHz

Gwarancja: Urządzenia muszą być objęte serwisem gwarancyjnym przez okres min. 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W przypadku awarii urządzenia należy w ciągu 24 godzin podstawić urządzenie zastępcze o tych samych funkcjonalnościach. W ramach tego serwisu musi być zapewniony również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5.

3.8 Serwer pod VMWARE ESXi

Należy dostarczyć serwer po wirtualizacje VMWARE ESXi o parametrach nie gorszych niż – **ilość 1:**

Obudowa:

-Typu Tower;

-Obudowa umożliwia konwersję do rack jedynie poprzez dodanie elementów fabrycznych producenta serwera (np. szyny rack czy tzw. „conversion-kit”;

-Wysokość serwera po konwersji do rack - 4U;

-Obudowa posiada fabryczne zabezpieczenie klatek z dyskami oraz napędami przed nieautoryzowanym dostępem (zamek);

Płyta główna:

-Wyprodukowana i zaprojektowana przez producenta serwera;

-4 złącza PCI Express w tym 2 złącza PCI Express 3.0 x8 (prędkość i typ złącza);
-Możliwość konwersji jednego ze złącz do złącza PCI 32bit
-Płyta posiada możliwość integracji dedykowanej, wewnętrznej pamięci flash przeznaczonej dla wirtualizatora (niezależne od dysków twardych);
-Możliwość zintegrowania układu TPM z płyta główna;

Procesor:

-Zainstalowany procesor min. 4-rdzeniowy w architekturze x86 osiągający w oferowanym serwerze w testach wydajności SPECint_rate_base2006 min. 199 pkt;

Pamięć RAM:

-Zainstalowane min. 32 GB pamięci RAM DDR4 2400Mhz w kościach o pojemności 16 GB
-Wsparcie dla technologii zabezpieczania pamięci ECC;
-Minimum 4 gniazda pamięci RAM, obsługa minimum 64GB pamięci RAM;

Kontrolery dyskowe, I/O:

-Zainstalowany wbudowany kontroler RAID 0,1,10;

Dyski twarde:

-Zainstalowane min. 2 dyski SATA o pojemności 1TB każdy,7.2K RPM 3,5”, dyski Hotplug;
-Obudowa posiada min. 4 wnęki dla dysków twardych Hotplug 3,5”;
-Obudowa umożliwia rozbudowę serwera do obsługi min. 12 dysków twardych Hotplug 3,5 cala

Kontrolery LAN:

-min. 2x 1Gb/s LAN, ze wsparciem iSCSI i iSCSI boot, RJ-45;

Porty:

-zintegrowana karta graficzna ze złączem VGA;

-min. 9x USB, w tym min. 5 złącz w standardzie USB 3.0 (2 na panelu przednim i 2 na panelu tylnym, min. 1 złącze wewnętrzne);
-min. 1x RS-232;

Zasilanie:

-Redundantne zasilacze hotplug o sprawności 94% (tzw. klasa Platinum) o mocy max. 450W;

Zarządzanie:

-Wbudowane diody informacyjne informujące o stanie serwera – sygnalizacja (poprawna praca/usterka) dla komponentów jak: procesor, wentylatory, dyski twarde, temperatura wewnątrz obudowy, pamięci, zasilaczy; sygnalizacja pracy (zasilania), sygnalizacja identyfikacji (włączana zdalnie)
-Zintegrowany z płytą główną serwera kontroler sprzętowy zdalnego zarządzania zgodny z IPMI 2.0 o funkcjonalnościach:

- Niezależny od systemu operacyjnego, sprzętowy kontroler umożliwiający pełne zarządzanie, zdalny restart serwera;
- Dedykowana karta LAN min. 1 Gb/s RJ-45 do komunikacji wyłącznie z kontrolerem zdalnego zarządzania z możliwością przeniesienia tej komunikacji na inną kartę sieciową współdzieloną z systemem operacyjnym;
- Dostęp poprzez przeglądarkę Web (także SSL, SSH)
- Zarządzanie mocą i jej zużyciem oraz monitoring zużycia energii
- Zarządzanie alarmami (zdarzenia poprzez SNMP)
- Możliwość przejęcia konsoli tekstowej
- Przekierowanie konsoli graficznej na poziomie sprzętowym oraz możliwość montowania zdalnych napędów i ich obrazów na poziomie sprzętowym (cyfrowy KVM)
- Oprogramowanie zarządzające i diagnostyczne wyprodukowane przez producenta serwera umożliwiające konfigurację kontrolera RAID, instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (m.in. temperatura, dyski, zasilacze, płyta główna, procesory, pamięć operacyjna itd.).

Gwarancja:

- min. 12 miesięcy gwarancji on-site z gwarantowanym czasem naprawy najpóźniej w następnym dniu roboczym od zgłoszenia usterki.

-Dostępność części zamiennych przez min. 5 lat od momentu zakupu serwera;

-Bezpłatna dostępność poprawek i aktualizacji BIOS/Firmware/sterowników dożywotnio dla oferowanego serwera;

-Wsparcie ogólnopolskiej, telefonicznej infolinii technicznej serwera, ogólnopolski numer o zredukowanej odpłatności 0 801) w czasie obowiązywania gwarancji na sprzęt i umożliwiająca po podaniu numeru seryjnego urządzenia weryfikację: konfiguracji sprzętowej serwera, w tym model i typ dysków twardych, procesora, ilość fabrycznie zainstalowanej pamięci operacyjnej, czasu obowiązywania i typ udzielonej gwarancji;

-Możliwość aktualizacji i pobrania sterowników do oferowanego modelu serwera w najnowszych certyfikowanych wersjach bezpośrednio z sieci Internet za pośrednictwem strony www, nie później niż w tym samym dniu od udostępnienia ich przez producenta urządzania;

Dokumentacja, inne:

-Elementy, z których zbudowany jest serwer są produktami producenta tych serwerów lub są przez niego certyfikowane oraz całe są objęte gwarancją producenta, o podanym powyżej poziomie SLA.

4 Konfiguracja urządzeń i sieci w Akademiku OLIMP

W ramach projektu należy wykonać konfigurację wszystkich nowych urządzeń aktywnych oraz już posiadanych przez Zamawiającego zgodnie z poniższymi wymogami.

4.1 Konfiguracja sieci LAN

Przełączniki w poszczególnych punktach dystrybucyjnych należy zamontować w szafach i połączyć w stos. Stos powinien być odporny na awarię pojedynczego linku oraz zapewniać minimalną prędkość działania 10Gbps.

Połączenia pomiędzy punktem dystrybucyjnym PD_2, a punktami PD_0 i PD_4 należy wykonać w technologii 10Gbps po linkach światłowodowych realizowanych w ramach projektu.

W sieci LAN należy stworzyć następujące VLAN-y:

- LAN MGMT – przeznaczony do celów administracyjnych urządzeniami aktywnymi
    - Dostęp do tego VLAN-u należy maksymalnie ograniczyć
        - Z sieci użytkowników dostęp do tego VLAN-u ma być całkowicie zabroniony
- LAN Użytkownicy w ramach projektu należy stworzyć trzy sieci pod użytkowników, każda z sieci będzie działała w obrębie jednego z punktów dystrybucyjnych:
    - LAN_Users_PD_0
    - LAN_Users_PD_2
    - LAN_Users_PD_4
- LAN_WiFi_Eduroam – sieć ta przeznaczona jest na potrzeby sieci bezprzewodowej „eduroam:
    - Ruch z sieci bezprzewodowej eduroam ma wpadać bezpośrednio z AP-ta do vlanu stworzonego na przełączniku
- Routing pomiędzy sieciami LAN_Users i LAN_WiFi_Eduroam ma odbywać się na przełączniku(stosie przełączników) PD_2. Ruch pomiędzy sieciami ma być zezwolony i nieograniczony.

Z aktualnie wykorzystywanych przełączników należy przenieść wskazane przez Zamawiającego vlan-y i wykonać przełączenie istniejących gniazdek na nowe urządzenia. Przeniesione sieci pracownicze mają być odseparowane od nowo tworzonych sieci. Do połączenia z siecią URZ(Centrala) należy wykorzystać jedno włókno dostępne pomiędzy lokalizacjami. Połącznie to należy zestawić na dostarczanych modułach 1Gbps działających na jednym włóknie.

W celu zabezpieczenia sieci LAN należy uruchomić następujące funkcjonalności na przełącznikach sieciowych:

- Blokować obce serwery DHCP uruchomione na portach dostępowych przez użytkowników końcowych

- Ograniczyć ruch broadcastowy na portach użytkowników końcowych do 3000pps, w przypadku przekroczenia progu ruch taki należy blokować lub wyłączyć port
- Ograniczyć ruch mac adresów na portach przełączników
- Uruchomić zabezpieczenie przez występowaniem pętli w sieci
- Ograniczyć możliwość wpisywania statycznych adresów IP na urządzeniach końcowych – wszyscy użytkownicy sieci LAN/WiFi muszą korzystać z serwera DHCP uruchamianego w ramach projektu
- Ograniczyć dostęp do urządzeń do adresów administracyjnych

Wszystkie ustalenia odnoście nazewnictwa, adresacji należy uzgodnić z Zamawiającym przez przystąpieniem do prac konfiguracyjnych.

4.2 Konfiguracja sieci WiFi

W ramach projektu należy uruchomić następujące sieci WiFi

- Sieć WiFi „eduroam" – jest to obecnie wykorzystywana sieć na URZ, której działanie należy rozszerzyć na akademik OLIMP zgodnie z wymogami jakie obowiązują przy konfiguracji tej sieci
    - Do celów autoryzacji użytkowników należy uruchomić dodatkowy serwer Radius na URZ oraz wykorzystać już jeden istniejący
    - Ruch użytkowników tej sieci WiFi na być bridge-owany z portem przełącznika na którym podpięty jest Access-Point
- Sieć WiFi „AK_OLIMP" – sieć WiFi oparta na autoryzacji użytkowników WPA2_ENT
    - autoryzacja użytkowników na serwerze Radius lokalnym instalowanym w ramach tego projektu

Wszystkie AP-ty należy zamontować w wyznaczonych przez Zamawiającego miejscach. Do AP-tów należy doprowadzić okablowanie ETH. AP-ty należy zasilić z dostarczanych przełączników z portów PoE/PoE+.
AP-ty należy zaadresować w VLAN-ie MGMT, należy im przypisać statyczne adresy IP oraz skonfigurować bramę domyślną i serwer DNS(usługę serwera DNS należy uruchomić na porcie Firewall-a dostarczanego w ramach projektu.)
Wszystkie dostarczane AP-ty należy podłączyć pod kontroler bezprzewodowy. Z poziomu kontrolera należy wykonać konfigurację wymienionych sieci WiFi.

4.3 Instalacja i konfiguracja serwera wirtualizacyjnego

W ramach projektu należy zainstalować darmową wersję oprogramowania VMWARE ESXi . Serwer ten należy zaadresować w sieci MGMT i podłączyć go dwoma linkami do przełączników w PD_2.

Serwer ten należy przeznaczyć pod instalację maszyn wirtualnych potrzebnych w ramach tego projektu.

4.4 Konfiguracja serwera Radius

W ramach projektu należy zainstalować serwer Radius(z usługą Radius), który umożliwi:

- Uruchomienie usługi Radius wykorzystywanej do autoryzacji użytkowników w ramach sieci bezprzewodowej „AK_OLIMP"
- Tworzenie/usuwanie/zarządzanie użytkownikami wykorzystywanymi do podłączenia się do sieci bezprzewodowej przez administratorów systemu
- Wystawienie portalu użytkownikom, w celu możliwości zmiany hasła dostępowego

Wraz z systemem należy dostarczyć wszystkie niezbędne licencje do uruchomiania i prawidłowego działania systemu.

4.5 Konfiguracja serwera DHCP

W ramach projektu należy uruchomić usługę serwera DHCP. Serwer ten należy skonfigurować tak, aby obsługiwał wszystkie stworzone VLAN-y w sieci LAN oraz wszystkie stworzone sieci WiFi w ramach projektu. Do wykonawcy należy również konfiguracja wszystkich urządzeń pośrednich w celu prawidłowego przydzielania adresów IP. Wszystkie niezbędne licencje potrzebne do uruchomienia serwera dostarczy Wykonawca.

4.6 Konfiguracja Firewall-a i systemu zbierania logów

W ramach projektu należy dostarczyć zamontować i skonfigurować urządzenie Firewall oraz system zbierania logów zgodnie z poniższymi założeniami. Głównym zadaniem firewall-a jest zagwarantowanie dostępu do sieci Internet w bezpieczny sposób. Wszyscy użytkownicy chcący skorzystać z sieci Internet muszą się **autoryzować** za pomocą konta uczelnianego lub dla nie posiadających konta uczelnianego konta lokalnego wygenerowanego przez administratora systemów w akademikach OLIMP.

4.6.1 Konfiguracja firewall-a

Na firewall-u należy wyznaczyć następujące strefy:

- LAN_MGMT – przeznaczona do wydzielonej sieci zarządzającej z której i do której ruch ma być ograniczony tylko do ruchu administratorów systemu
- WAN – strefa przeznaczona do podłączenia łącza internetowego
- LAN_SW – strefa do wykonania podłączenia z przełącznikiem routującym w sieci LAN, w strefie tej mają znajdować się tylko urządzenia routujące – firewall i przełącznik

W zakresie Wykonawcy jest również wykonanie pełnej konfiguracji firewall-a tak aby osiągnąć następujące założenia:

- Dostęp z sieci użytkowników(sieci LAN oraz sieci WiFi) do Internetu na być **dozwolony tylko dla użytkowników, którzy dokonają autoryzacji** za pomocą:
    - konta uczelnianego
    - konta lokalnego utworzonego w akademiku na serwerze lokalnym Radius poprzez system obsługi gości hotelowych domu studenckiego
- Dostęp z sieci użytkowników do sieci LAN_MGMT ma być zabroniony
- Dostęp z sieci Internet do sieci za firewallem ma być zabroniony, nie licząc ruchu administracyjnego – ruch ten musi być ograniczony jedynie do protokołów uznawanych za bezpieczne
- Ruch użytkowników do sieci Internet ma być ograniczony:
    - QoS zezwalający na 10Mbps per IP
    - Limit sesji dla jednego IP – 3000
- Wykonanie publikacji serwera, serwerów jeżeli zajdzie taka potrzeba
- Wykonanie połączeń VPN Site-to-Site do firewalla w centrali URZ - w celu wymiany informacji pomiędzy systemami uczelni, a stawianymi systemami w ramach projektu

Wykonawca zobowiązany jest do konfiguracji nowo dostarczanych urządzeń oraz istniejących pod nadzorem administratorów URZ.

Dostarczany system logowania należy zintegrować z firewall-em. Logi odnośnie ruchu użytkowników należy zapisywać na urządzeniu logującym oraz archiwizować przez okres co najmniej 60 dni.
W logach systemu powinna znajdować się informacja odnoście użytkownika(autoryzacja użytkowników) jaki generuje dany ruch.

5 Rekonfiguracja urządzeń/serwerów pod potrzeby sieci „eduroam” w centrali URZ

W celu zwiększenia niezawodności, dostępności i wydajności należy dokonać rozbudowy istniejącego systemu autoryzacji użytkowników sieci LAN/WiFi o dodatkowy serwer autoryzujący.

5.1 Konfiguracja serwera Radius02

W ramach projektu należy zainstalować i skonfigurować dodatkowy serwer Radius w centrali URZ. Należy dokonać jego konfiguracji tak, aby funkcjonalnie działał jak istniejący serwer oraz umożliwiał ciągłą pracę w przypadku awarii serwera istniejącego. Zasoby na uruchomienie serwera oraz licencje zapewnia Zamawiający.

Zamawiający dostarczy również certyfikat do obu serwerów Radius jaki należy używać w procesie autoryzacji. Rekonfiguracja serwerów z nowym certyfikatem jest w zakresie Wykonawcy.

5.2 Rekonfiguracja obecnie wykorzystywanych połączeń urządzeń aktywnych do serwerów Radius

Należy dokonać zmian istniejącej konfiguracji tak, aby:

- System bezprzewodowy w budynkach uczelni autoryzował się na istniejącym serwerze, w przypadku awarii na serwerze Radius02.
- Systemy LAN/WiFi w akademikach Laura/Filon autoryzowały się na serwerze Radius02, w przypadku awarii na serwerze istniejącym Radius01
- Systemy LAN/WiFi w akademiku OLIMP autoryzowały się na serwerze Radius02, w przypadku awarii na serwerze istniejącym Radius01
- Oba serwery powinny być wykorzystywane do wymiany informacji w ramach działania sieci EDUROAM z serwerami Radius na Politechnice Rzeszowskiej – należy dokonać rozbudowy istniejącej konfiguracji o serwer Radius02

5.3 Rekonfiguracja obecnie wykorzystywanych systemów autoryzacji

Rekonfiguracja systemów elektronicznych legitymacji

W ramach realizacji przedmiotu zamówienia wymagana jest integracja nowo tworzonej struktury sieci LAN oraz sieci Wi-Fi z istniejącym Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej.

Celem, jaki należy osiągnąć jest:

- Możliwość logowania się studentom, pracownikom oraz innym użytkownikom do sieci „eduroam” konfigurowanej w ramach projektu
- Możliwość autoryzacji użytkowników sieci LAN przy wyjściu do Internetu. Każdy z użytkowników powinien podać dane do autoryzacji po pojawieniu się strony internetowej w przeglądarce.

W ramach prowadzonych prac należy wykonać konfigurację wszystkich elementów wchodzących w skład systemu oraz wszystkich urządzeń pośredniczących w komunikacji, w szczególności:

- Konfiguracja Systemu Elektronicznej Legitymacji Studenckiej (SELS),
- Konfiguracja Systemu Elektronicznej Legitymacji Doktoranta
- Konfiguracja Systemu Elektronicznej Karty Pracowniczej
- Konfiguracja kontrolera sieci Wi-Fi
- Konfiguracja firewalla

Konfiguracja połączenia z zasobami w centrali – reguły na centralnym firewall-u w celu przepuszczenia ruchu

6 Obsługa gości hotelowych domu studenckiego.

Zamawiający wymaga dostawy i wdrożenia oprogramowania wspierającego procesy obsługi gości hotelowych domu studenckiego w szczególności usystematyzowanie procesów związanych z rezerwacjami pokoi dla gości hotelowych wraz z obsługą meldowania, wydawania kluczy i generowania danych dostępowych do Internetu z wykorzystaniem oprogramowania informatycznego.

Wdrożony system musi spełniać następujące minimalne wymagania:

- System musi umożliwiać obsługę następujących procesów związanych z funkcjami hotelowymi domu studenckiego :

  - tworzenie rezerwacji
  - meldunek gości hotelowych
  - wymeldowanie gości hotelowych
  - wydanie kluczy do pokoju hotelowego
  - nadzór nad listą gości hotelowych

- System musi umożliwiać użytkownikom dostęp do następujących informacji:

  - grafik pomieszczeń
  - lista gości hotelowych
  - lista rezerwacji

- System dla grafiku pomieszczeń musi prezentować listę wszystkich dostępnych pokoi hotelowych dla całego miesiąca z graficznym oznaczeniem pokoi wolnych, zarezerwowanych i wynajętych.

-System musi umożliwiać zarządzanie pokojami hotelowymi, strukturą, dostępnością do rezerwacji z poziomu części administracyjnej systemu.

- System z poziomu grafiku dostępności pokoi musi umożliwić:

  - utworzenie rezerwacji
  - podgląd szczegółów rezerwacji
  - anulowanie rezerwacji
  - zameldowanie gościa hotelowego
  - wymeldowanie gościa hotelowego

- Formularz rezerwacji musi umożliwiać rejestrację co najmniej następujących danych gościa:

  - imię
  - nazwisko
  - data zameldowania
  - planowana data wymeldowania
  - nr pokoju
  - budynek
  - status rezerwacji np. (aktywna/anulowana/zrealizowana/zrealizowana archiwalna)

- System musi umożliwić rejestrację wielu gości na portierni jednocześnie tj. w jednym cyklu możliwe jest dodanie wielu gości do jednej osoby(pracownika)
- Formularz meldowania gościa hotelowego musi umożliwiać rejestrację co najmniej następujących danych gościa:

- imię
- nazwisko
- data zameldowania
- planowany termin wymeldowania
- nr pokoju
- nr budynku
- dane adresowe
- opis
- typ dokumentu, którym posługuje się gość
- pole opisowe ‘uwagi przy wejściu’
- pole opisowe ‘uwagi przy wyjściu’

- System musi umożliwiać podgląd listy bieżących gości hotelowych prezentując co najmniej dane:

- imię
- nazwisko
- data zameldowania
- planowana data wymeldowania
- nr pokoju hotelowego

- Lista gości domyślnie powinna prezentować aktualną listę zameldowanych gości. System musi umożliwiać wyszukiwanie gości:

- archiwalnych
- w danym okresie czasu,
- wg nazwiska gościa
- wg budynku

- Lista gości hotelowych musi w sposób graficzny identyfikować gości dla których skończyła się doba hotelowa a którzy nadal pozostają zameldowani.
- System musi współpracować z funkcjonującym systemem Portiernia domu studenckiego.
- Zamawiający dopuszcza rozbudowę funkcjonującego systemu Portiernia o funkcje hotelowe.
- System musi być otwarty na możliwą rozbudowę uwzględniającą inne budynki będące w posiadaniu Zamawiającego.
- System musi umożliwiać proces logowania operatorów za pomocą loginów i haseł.

- Operatorzy wydający klucze muszą być zalogowani do systemu w celu identyfikacji wykonawców operacji w systemie.
- System musi umożliwić obsługę nielimitowanej ilości pokoi, gości hotelowych, rezerwacji.
- System musi archiwizować dane/logi/zdarzenia.
- System musi pozwalać na eksport wyników raportów co najmniej do pliku CSV i PDF.
- System musi być zrealizowany w technologii klient - serwer.
- System musi zapewniać integrację z funkcjonującym na uczelni systemem wewnętrznej sieci internetowej.
- Podczas meldunku gościa hotelowego system musi pozwolić na założenia konta AD (login, hasło – wg zdefiniowanej maski oraz termin aktywności konta)
- System musi przypisać założone konto do wybranej grupy domenowej mającej dostęp do sieci Wi-Fi domu studenckiego
- System hotelowy musi umożliwiać wydruk danych logowania przez operatora systemu. Wydruk powinien zawierać opracowany regulamin korzystania z sieci.
- System przy ponownym meldowaniu gościa hotelowego, dla którego zostało założone wcześniej konto AD musi je aktywować na czas zameldowania gościa.
- System hotelowy musi umożliwiać ponowne wygenerowanie hasła dostępowego do sieci Wi-Fi

7. Dokumentacja powykonawcza oraz szkolenie

Wykonawca dostarczy dokumentację powykonawczą, która musi zawierać:

- Schemat sieci LAN wraz z wykorzystywanymi portami na przełącznikach oraz panelami światłowodowymi
- Tabelą opisującą wykaz portów oraz podpięte urządzenia
- Opis funkcjonalny systemu
- Wykaz zmian na istniejących systemach
- Pomiary wykonanych instalacji sieciowych
- Szkolenie całościowe z dostarczonego rozwiązania dla trzech osób.