ZAŁĄCZNIK NR 2.13 do zapytania ofertowego

Stanowisko badawcze nr 13:

Stanowisko sieci WLAN

Elementy Składowe	Sztuk
Kontroler	2
AP (sterowany przez kontroler)	6
Instant AP (independent AP)	3
Stół laboratoryjny	1
Fotel biurowy	1

Szczegółowe minimalne wymagania dotyczące elementów składowych stanowiska.

1. Kontroler - 2 sztuki

Kontroler sieci bezprzewodowej

- Specyfikacja fizycznego kontrolera sieci bezprzewodowej:
- Dwurdzeniowy procesor o częstotliwości pracy min. 500 Mhz
- Pamięć Flash min. 512 MB
- Port Mini PCI Express do obsługi kart 3G WAN
- Możliwość obsługi do 144 jednocześnie podpiętych punktów dostępowych
  - Budżet mocy PoE dla punktów dostępowych min. 90 W.
  - Porty 1 x 10/100/1000BASE-T / SFP oraz 5 x 10/100/1000BASE-T PoE
  - Wbudowana zapora ogniowa zarówno dla sieci przewodowej i bezprzewodowej z funkcjonalnością Role Based Firewall
  - Wbudowany mechanizm Wireless Intrusion Protection System (WIPS)
    - Wykrywanie Rouge AP
    - Kategoryzacja urządzeń
  - Obsługa IPSec VPN gateway
  - Obsługa AAA radius Server oraz zabezpieczonego dostępu gościnnego za pośrednictwem Captive Portal.
  - Uwierzytelnianie w oparciu o adresy MAC
  - Wsparcie dla standardu 802.11w Secure Management Frames
  - Obsługa polityk:
    - Polityki AAA - 24

- Polityki Captive Portal - 32
- Obsługa min. 1000 ACL
- Obsługa min. 30 instancji VRRP
- Obsługa 256 Switched Virtual IP Interfaces (SVIs)
- Realizacja min. 255 dynamicznych tuneli L2TPv3
  Realizacja min. 63 statycznych tuneli L2TPv3
- Ilość wpisów tras IPv4 /IPv6 13312
- Ilość tuneli VPN IPsec 256
- Ilość wpisów IPv4 do zapory 50000
- Ilość wpisów IPv6 do zapory 50000
- Wsparcie dla Network Access Control oraz mechanizmów analizy anomalii w ruchu sieciowym Deep Packet Inspection

Pakiet licencyjny wspierający obsługę wykazanych w opisie AP.

Oprogramowanie zarządzające:

1. Aplikacja musi pracować w architekturze klient serwer, czyli główna część oprogramowania pracuje na serwerze, a klienci mogą dołączyć się do serwera z dowolnego komputera pracującego w sieci i mającego dostęp do serwera
    a. Serwer aplikacji zarządzającej musi mieć możliwość pracy w środowisku Linux, Windows oraz jako aplikacja dedykowana dla systemu wirtualizacyjnego np. VMWare, Citrix, HyperV,
    b. Aplikacja musi wspierać klientów pracujących z wykorzystaniem systemu Linux, Windows oraz MAC OS.
2. Aplikacja musi zarządzać siecią przewodową i bezprzewodową
3. Aplikacja zarządzająca musi obsługiwać minimum 25 urządzeń (adresów IP)
4. Aplikacja zarządzająca musi pozwalać na zarządzanie siecią dla minimum 25 jednoczesnych użytkowników (administratorów).
5. Aplikacja zarządzająca musi pozwalać na uruchomienie zapasowego systemu zarządzającego oraz systemu zarządzania do laboratorium testowego. Dostawca zobowiązany jest dostarczyć dodatkowe licencje na oprogramowanie jeśli jest to wymagane przez producenta systemu zarządzającego
6. Aplikacja zarządzająca musi mieć możliwość definiowania wielopoziomowych dostępów do aplikacji zarządzającej wraz z definicją praw dla poszczególnych użytkowników
7. Aplikacja zarządzająca musi mieć możliwość integracji autoryzacji użytkowników za pomocą LDAP i/lub Radius.
8. Wszystkie dane aplikacji zarządzającej muszą być przechowywane w bazie danych SQL zintegrowanej z aplikacją działającą na serwerze.
9. Aplikacja zarządzająca musi pracować w oparciu o protokół SNMPv1, SNMPv2, SNMPv3, SNMPv3 AES
10. Aplikacja musi pozwalać na tworzenie profili SNMP dla grup urządzeń tak, aby za każdym razem przy konfiguracji nowego urządzenia nie było konieczności konfiguracji wszystkich parametrów, a konieczny był tylko wybór profilu.
11. Aplikacja musi mieć możliwość przyjmowania trapów SNMP oraz przekierowywania ich do innych systemów
12. Aplikacja musi posiadać wbudowaną przeglądarkę SNMP MIB
13. Aplikacja musi posiadać możliwość kompilowania SNMP MIB innych producentów

14. Aplikacja musi zapewniać możliwość zarządzania urządzeń poprzez SNMP MIB-I oraz SNMP MIB-II
15. Aplikacja musi zapewniać możliwość wskazania dowolnych SNMP MIB OID i prezentację ich w postaci tabelarycznej dla danych urządzeń sieciowych.
16. Aplikacja musi posiadać możliwość automatycznej reakcji na przychodzące trapy SNMP lub informacje z Syslog poprzez wysłanie email'a, wysłanie trapu SNMP, wpisu do Syslog'a lub uruchomienie skryptu.
17. Aplikacja musi posiadać wbudowany Syslog serwer
18. Aplikacja musi posiadać wbudowany BootP serwer
19. Aplikacja musi wspierać protokół IPv4 oraz IPv6
20. Aplikacja musi umożliwiać automatyczną realizację backupów swojej własnej konfiguracji pozwalających na szybkie odtworzenie aplikacji w przypadku awarii serwera.
21. Aplikacja musi zapewniać automatyczne i ręczne wykrywanie i rozpoznawanie urządzeń sieciowych, wraz z automatycznym ich grupowaniem według typu, lokalizacji i kontaktu do administratora
22. Aplikacja musi pozwalać na tworzenie przez administratora grup urządzeń oraz portów na urządzeniach.
23. Aplikacja musi zapewniać możliwość wizualizacji sieci z uwzględnieniem
    a. połączeń pomiędzy poszczególnymi urządzeniami z zaznaczeniem ich przepustowości
    b. stanu protokołu Spanning Tree oraz Multiple Spanning Tree wraz z opisem węzłów oraz roli portów
    c. konfiguracji sieci VLAN
    d. konfiguracji protokołu routingu OSPF
24. Aplikacja musi zapewniać możliwość bezpośredniego połączenia do wskazanego na mapie urządzenia za pomocą minimum telnet, ssh oraz http/https
25. Aplikacja musi zapewniać możliwość inwentaryzacji urządzeń w sieci zawierającej następujące dane:
    a. adres IP urządzenia
    b. adresu MAC urządzenia
    c. nazwy urządzenia
    d. wersji oprogramowania
    e. wersji bootrom
    f. lokalizacji urządzenia
    g. danych kontaktowych administratora
    h. numeru seryjnego
26. Aplikacja musi zapewniać centralne zarządzanie konfiguracjami urządzeń sieciowych. Wymagane jest:
    a. możliwość automatycznej periodycznej realizacji backup'u konfiguracji urządzeń o wskazanym czasie
    b. możliwość odtworzenia wskazanej konfiguracji urządzenia
    c. możliwość porównywania różnic we wskazanych tekstowych plikach konfiguracyjnych
    d. możliwość obsługi urządzeń sieciowych różnych producentów
27. Aplikacja musi zapewniać możliwość aktualizacji oprogramowania na urządzeniach sieciowych. Wymagana jest możliwość zaplanowania aktualizacji oraz restartu urządzeń we wskazanym dniu i wskazanym czasie

28. Aplikacja musi przechowywać historię zmian konfiguracji oraz oprogramowania na urządzeniach
29. Aplikacja musi zapewniać możliwość stworzenia raportu wykorzystywanych portów urządzeń sieciowych.
30. Aplikacja musi zapewniać możliwość definiowania polityk dostępu dla użytkowników przewodowych i bezprzewodowych jednocześnie z uwzględnieniem biznesowego podziału użytkowników np. Administracja, Finanse, Goście, Zarząd itp.
31. Tworzona polityka musi zawierać możliwość:
    a. blokowania lub zezwalania ruchu na podstawie
        i. źródłowy i docelowy adres MAC
        ii. źródłowy i docelowy adres IP
        iii. źródłowy i docelowy adres IP podsieci
        iv. źródłowy i docelowy port TCP/UDP
        v. źródłowy i docelowy zakres portów TCP/UDP
        vi. typ protokołu
        vii. pole IP TOS
    b. przydziału parametrów QoS
        i. priorytety
        ii. ograniczenia przepustowości
    c. przydziału użytkownika do wskazanej sieci VLAN
    d. przekierowania ruchu do zewnętrznego systemu analizującego pakiety
32. Aplikacja musi mieć możliwość wdrażania polityk bezpieczeństwa w całej sieci, dla urządzeń przewodowych i bezprzewodowych za pomocą jednego kliknięcia.
33. Aplikacja musi pozwalać na łatwą modyfikację i ponowne wdrożenie na wszystkich urządzeniach przewodowych i bezprzewodowych
34. Aplikacja zarządzająca musi posiadać wbudowany portal www dostępny dla administratora oraz działu wsparcia użytkowników. Portal musi umożliwiać:
    a. szybką lokalizację użytkownika w sieci na podstawie adresu MAC, adresu IP, nazwy użytkownika lub komputera w sieci przewodowej i bezprzewodowej bez konieczności korzystania z różnych aplikacji zarządzających. Aplikacja po zlokalizowaniu użytkownika musi wskazać, gdzie użytkownika jest dołączony w sieci z podaniem minimum urządzenia sieciowego (przełącznik lub bezprzewodowy punkt dostępowy).
    b. wyświetlenie listy obsługiwanych urządzeń sieciowych zawierającej adres MAC, adres IP, nazwę urządzenia, typu urządzenia, lokalizację, kontakt administracyjny, numer seryjny, wersję firmware oraz bootrom oraz status urządzenia (dostępne/niedostępne).
    c. wyświetlenie alarmów, trapów SNMP, wpisów syslog itp.
    d. generowanie raportów
35. Aplikacja zarządzająca musi zapewniać zarządzenia siecią bezprzewodową.
    a. Musi być zapewniona podsumowująca zawierająca informacje o liczbie kontrolerów oraz punktów dostępowych i ich stanie (działa / nie działa).
    b. Musi być zapewnione podsumowanie zawierające informacje o liczbie klientów z podziałem na wykorzystywane technologie bezprzewodowe: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz), IEEE 802.11n (5 GHz), IEEE 802.11ac
    c. Musi być zapewniona widzialność parametrów wszystkich kontrolerów bezprzewodowych zawierających następujące informacje:

i. adres IP kontrolera
ii. liczba obsługiwanych klientów
iii. szczytowe wartości zajmowanego pasma
iv. wersja oprogramowania

d. Musi być zapewniona widzialność parametrów wszystkich punktów dostępowych zawierających następujące informacje:
   i. adres IP punktu dostępowego
   ii. MAC adres punktu dostępowego
   iii. wersja oprogramowania
   iv. typ punktu dostępowego
   v. kanały pracy poszczególnych interfejsów radiowych
   vi. szczytowe wartości zajmowanego pasma na interfejsie Ethernet oraz interfejsach radiowych
e. Musi być zapewniona widzialność parametrów wszystkich klientów bezprzewodowych dołączonych do sieci bezprzewodowej zawierających następujące informacje:
   i. adres IP klienta
   ii. MAC adres klienta
   iii. nazwa użytkownika
   iv. nazwa punktu dostępowego, do którego dołączony jest użytkownik
   v. BSSID, do którego dołączony jest użytkownik
   vi. SSID, do którego dołączony jest użytkownik
f. Musi być zapewniona możliwość tworzenia map budynku i umieszczenia na nich punktów dostępowych. Mapy muszą zapewniać następujące funkcjonalności:
   i. zaznaczanie obszarów pokrycia siecią bezprzewodową wraz z informacją na temat dostępnej przepustowości (Data Rate).
   ii. zaznaczenie kanałów pracy urządzeń
   iii. lokalizacja klienta na mapie na podstawie triangulacji siły sygnału z punktów dostępowych

36. Aplikacja zarządzająca musi być zintegrowana z systemem zapewniającym widoczność zautoryzowanych klientów w sieci z zapewnieniem widzialności następujących informacji:
   a. adresu MAC
   b. adresu IP
   c. nazwy komputera
   d. typu klienta oraz systemu operacyjnego – możliwość wykrywania urządzeń na podstawie DHCP fingerprintingu np. Windows / Windows 7, iPhone / IOS itp.
   e. nazwa urządzenia, do którego dołączony jest klient – to może być nazwa bezprzewodowego punktu dostępowego lub nazwa przełącznika.
   f. adres IP urządzenia, do którego dołączony jest klient.
   g. identyfikacja portu, do którego dołączony jest klient – identyfikacja portu urządzenia bezprzewodowego (np. urządzenie może mieć dwa radia: jedno na 2.4 GHz, a drugie na 5 GHz) lub portu przełącznika sieciowego.
   h. typ autentykacji użytkownika np. autentykacja MAC, autentykacja IEEE 802.1x, kerberos snooping itp.

i. nazwa przydzielonej polityki bezpieczeństwa.

37. System zapewniający widoczność zautoryzowanych klientów w sieci musi zapewniać przechowywanie historii zautoryzowanych klientów oraz aktualnego statusu klienta zawierającej zmiany wspomnianych wcześniej parametrów, czyli np. zmiana portu na przełączniku lub zmiana punktu dostępowego, zmiana adresu IP, zmiana polityki bezpieczeństwa itp.
38. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość ponownej autentykacji użytkownika na żądanie – np. w celu przeniesienia użytkownika do innej polityki bezpieczeństwa
39. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość szybkiego przeniesienia klienta do grupy użytkowników. Grupa użytkowników może być powiązana z inną polityką bezpieczeństwa lub może to być np. grupa użytkowników, którzy mają zabroniony dostęp do sieci – grupa Black List
40. System zapewniający widoczność zautoryzowanych klientów musi zapewniać możliwość rejestracji urządzeń poprzez portal www. Rejestracji mogą podlegać np. urządzenia gości lub urządzenia, które nie mają możliwości przeprowadzenia autentykacji w sieci.
41. System zapewniający widoczność zautoryzowanych klientów musi posiadać informacje podsumowujące zawierające:
    a. liczbę urządzeń z podziałem na urządzenia klientów zautoryzowanych, klientów z problemami autoryzacyjnymi itp.
    b. liczbę urządzeń z podziałem typu autoryzacji np.: MAC, 802.1x itp.
    c. liczbę urządzeń z podziałem na typy systemów operacyjnych np.: Windows, Linux, IOS, Android
    d. liczbę urządzeń z przydziałem poszczególnych polityk bezpieczeństwa
    e. liczbę urządzeń z podziałem na obszary np. budynek 1, budynek 2 itp.
42. System zapewniający widoczność zautoryzowanych klientów, jeśli jest licencjonowany na liczbę użytkowników musi zapewniać obsługę min. 6000 urządzeń klienckich (adresów IP). Jeśli system jest licencjonowany na liczbę urządzeń autoryzujących to musi zapewniać obsługę min. 250 punktów dostępowych oraz min. 25 przełączników sieciowych
43. System zarządzania musi posiadać możliwość integracji z systemem pozwalającym na analizę ruchu w sieci do warstwy 7.
44. System zarządzania musi posiadać wbudowane API pozwalające na komunikację z systemami zewnętrznymi innych producentów.
45. System zarządzania musi być objęty 3 letnim wsparciem serwisowym producenta. Producent musi oferować dostępność wsparcia technicznego drogą elektroniczną oraz telefoniczną w trybie 24x7.

2. AP (sterowany przez kontroler) – 6 sztuk

- Punkt dostępowy z dwoma wbudowanymi, niezależnymi od siebie, modułami radiowymi dla komunikacji IEEE 802.11a/b/g/n/ac
- Obsługa 802.11ac
- Dwu zakresowe moduły radiowe; 2x2:2 MIMO

- Obsługa trybu MU MIMO
- Zysk z anten min. 4dBi - pasmo 2.4 GHz; 6 dBi - pasmo 5GHz
- Obsługa 16 SSID oraz minimum 250 użytkowników
- Punkt dostępowy musi wspierać standard Bluetooth Low Enegry (BLE) w wersji 4.2 zgodny z IEEE 802.15.4
- Punkt dostępowy zasilany poprzez POE zgodnie ze standardem IEEE 802.11af
- Port 10/100/1000BaseT Ethernet z automatycznym wykrywaniem parametrów transmisji
- Punkt dostępowy musi oferować obsługę następujących mechanizmów warstwy L2 i L3:
  - Routing warstwy L3, 802.1q, DynDNS, DHCP serwer/klient, klient BOOTP, PPPoE oraz LLDP
- Punkt dostępowy musi obsługiwać następujące mechanizmy bezpieczeństwa:
  - Firewall typu stateful, filtrowanie IP, NAT, 802.1x, 802.11i, WPA2, WPA, metoda wykrywania fałszywych urządzeń: 24x7 dwuzakresowy sensor WIPS, wbudowany IDS oraz bezpieczny dostęp gości (hotspot) wraz z portalem rejestracyjnym (captive portal), IPSec, wudowany Radius Server
- Obsługa następujących mechanizmów QoS:
  - Quality of Service (QoS) WMM, WMM-UAPSD, 802.1p, Diffserv i TOS
- Obsługa mechanizmu Smart Load Balancing polegającą na: Równomiernym dystrybuowaniu klientów na punkty dostępowe i pasma częstotliwości.
- Wsparcie dla Network Access Control oraz mechanizmów analizy anomalii w ruchu sieciowym Deep Packet Inspection
- Zintegrowana funkcjonalność widoczności i kontroli aplikacji (Layer 7) bezpośrednio na punkcie dostępowym bez zewnętrznego kontrolera
- Temperatura pracy urządzenia od 0° C do 40° C
- Interfejs konsoli RJ45
- Współdzielenie modułów radiowych oraz skanowanie poza kanałem transmisji umożliwiające pełnienia dwóch funkcji – punktu dostępowego i sensora
- 802.11r Fast Roaming: szybki roaming
- Mechanizm typu Smart Rf pozwalający urządzeniom na automatyczne i inteligentne dostosowanie się do zmian w środowisku radiowym w celu eliminacji niespodziewanych luk w zasięgu. Wykrywanie zakłóceń pochodzące od urządzeń Wi-Fi i pozostałych (np. uszkodzone anteny, sąsiednie punkty dostępu) oraz automatycznie dostosowanie w razie potrzeby, kanału i mocy sygnału.
- Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym (bez kontrolera) lub w trybie „lekkiego AP" pod kontrolą kontrolera bezprzewodowego
- Punkt dostępowy musi mieć możliwość pracy jako wirtualny kontroler (musi obsługiwać w tym trybie minimum 64 punkty dostępowe)

3. Instant AP (independent AP) – 3 sztuki

- Punkt dostępowy z dwoma wbudowanymi, niezależnymi od siebie, modułami radiowymi dla komunikacji IEEE 802.11a/b/g/n/ac
- Obsługa 802.11ac
- Dwu zakresowe moduły radiowe; 2x2:2 MIMO
- Obsługa trybu MU MIMO

- Zysk z anten min. 4dBi - pasmo 2.4 GHz; 6 dBi - pasmo 5GHz
- Obsługa 16 SSID oraz minimum 250 użytkowników
- Punkt dostępowy musi wspierać standard Bluetooth Low Enegry (BLE) w wersji 4.2 zgodny z IEEE 802.15.4
- Punkt dostępowy zasilany poprzez POE zgodnie ze standardem IEEE 802.11af
- Port 10/100/1000BaseT Ethernet z automatycznym wykrywaniem parametrów transmisji
- Punkt dostępowy musi oferować obsługę następujących mechanizmów warstwy L2 i L3:
  - Routing warstwy L3, 802.1q, DynDNS, DHCP serwer/klient, klient BOOTP, PPPoE oraz LLDP
- Punkt dostępowy musi obsługiwać następujące mechanizmy bezpieczeństwa:
  - Firewall typu stateful, filtrowanie IP, NAT, 802.1x, 802.11i, WPA2, WPA, metoda wykrywania fałszywych urządzeń: 24x7 dwuzakresowy sensor WIPS, wbudowany IDS oraz bezpieczny dostęp gości (hotspot) wraz z portalem rejestracyjnym (captive portal), IPSec, wudowany Radius Server
- Obsługa następujących mechanizmów QoS:
  - Quality of Service (QoS) WMM, WMM-UAPSD, 802.1p, Diffserv i TOS
- Obsługa mechanizmu Smart Load Balancing polegającą na: Równomiernym dystrybuowaniu klientów na punkty dostępowe i pasma częstotliwości.
- Wsparcie dla Network Access Control oraz mechanizmów analizy anomalii w ruchu sieciowym Deep Packet Inspection
- Zintegrowana funkcjonalność widoczności i kontroli aplikacji (Layer 7) bezpośrednio na punkcie dostępowym bez zewnętrznego kontrolera
- Temperatura pracy urządzenia od 0° C do 40° C
- Interfejs konsoli RJ45
- Współdzielenie modułów radiowych oraz skanowanie poza kanałem transmisji umożliwiające pełnienia dwóch funkcji – punktu dostępowego i sensora
- 802.11r Fast Roaming
- Mechanizm typu Smart Rf pozwalający urządzeniom na automatyczne i inteligentne dostosowanie się do zmian w środowisku radiowym w celu eliminacji niespodziewanych luk w zasięgu. Wykrywanie zakłóceń pochodzące od urządzeń Wi-Fi i pozostałych (np. uszkodzone anteny, sąsiednie punkty dostępu) oraz automatycznie dostosowanie w razie potrzeby, kanału i mocy sygnału.
- Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym (bez kontrolera) lub w trybie „lekkiego AP" pod kontrolą kontrolera bezprzewodowego
- Punkt dostępowy musi mieć możliwość pracy jako wirtualny kontroler (musi obsługiwać w tym trybie minimum 64 punkty dostępowe

4. Stół laboratoryjny – 1 sztuka

Stół laboratoryjny o wymiarach: 1000mm x 3000mm.
Blat : płyta wiórowa lub MDF laminowana obustronnie o grubości minimum 25mm. Dostępna paleta kolorów powinna posiadać co najmniej 6 różnych kolorów do wyboru. Stolik powinien posiadać minimum 6 metalowych nóg. Kolor nóg zostanie wybrany na etapie dostawy. Dostępna paleta kolorów powinna posiadać co najmniej 3 różne kolory do wyboru. Nogi

stołu powinny być malowane proszkowo. Wysokość stolika min 76 cm. Nośność stołu powinna wynosić co najmniej 150kg.

5. Fotel biurowy – 1 sztuka

Krzesło obrotowe na pięcioramiennej podstawie z mechanizmem umożliwiającym regulację wysokości siedziska (za pomocą podnośnika pneumatycznego lub gazowego), kąta odchylenia oparcia oraz blokadę wysokości oparcia, powinno posiadać ergonomiczne mechanizmy i kształt. Krzesło powinno być wyposażone w regulowane podłokietniki, samohamowne kółka do powierzchni twardych, blokadę oparcia w minimum czterech pozycjach. Siedzisko i oparcie powinny być wykonane z wysokiej jakości siatki. Nośność: minimum 130kg. Dostępna paleta kolorów powinna posiadać co najmniej 10 różnych kolorów do wyboru.
Do oferty należy dołączyć aktualny atest wytrzymałościowy.
Wymiary:
Min. zakres regulacji wysokości powierzchni do siedzenia (mm): od 430 mm do 530 mm
głębokość siedziska – minimum 490mm
szerokość siedziska – minimum 470mm
średnica podstawy – 690mm