CISCO Academy

Pakiet Tracer - Konfiguracja WPA2 Enterprise WLAN na WLC

Tabela adresowania

Urządzenie	Interface	Adres IP
R1	G0/0/0.5	192.168.5.1/24
	G0/0/0.200	192.168.200.1/24
	G0/0/1	172.31.1.1/24
SW1	VLAN 200	192.168.200.100/24
LAP-1	G0	DHCP
WLC-1	Management	192.168.200.254/24
Serwer RADIUS/SNMP	karta sieciowa	172.31.1.254/24
Admin PC	karta sieciowa	192.168.200.200/24

Cele

W tym ćwiczeniu zostanie skonfigurowana nowa sieć WLAN na kontrolerze bezprzewodowej sieci LAN (WLC), w tym interfejs VLAN, z którego będzie korzystać. Skonfigurujesz sieć WLAN do używania serwera RADIUS i WPA2-Enterprise do uwierzytelniania użytkowników. Skonfigurujesz również WLC do korzystania z serwera SNMP.

- Skonfiguruj nowy interfejs VLAN w sieci WLC.
- Skonfiguruj nową sieć WLAN w sieci WLC.
- Skonfiguruj nowy zakres na wewnętrznym serwerze DHCP WLC.
- Skonfiguruj WLC z ustawieniami SNMP.
- Skonfiguruj WLC, aby używał serwera RADIUS w celu uwierzytelniania użytkowników sieci WLAN.
- Zabezpieczyć WLAN z WPA2-Enterprise.
- Podłącz hosty do nowego WLC.

Wprowadzenie

Już skonfigurowano i przetestowano WLC z istniejącą siecią WLAN. Skonfigurowano WPA2-PSK dla tej sieci WLAN, ponieważ miał być używany w mniejszej firmie. Zostałeś poproszony o skonfigurowanie i przetestowanie topologii WLC, która będzie używana w większym przedsiębiorstwie. Wiesz, że WPA2-PSK nie skaluje się dobrze i nie jest odpowiedni do użycia w sieci korporacyjnej. Ta nowa topologia użyje serwera usługi RADIUS i WPA2-Enterprise do uwierzytelniania użytkowników sieci WLAN. Umożliwia to administrowanie kontami użytkowników z centralnej lokalizacji i zapewnia większe bezpieczeństwo i przejrzystość, ponieważ każde konto ma własną nazwę użytkownika i hasło. Ponadto aktywność użytkownika jest rejestrowana na serwerze.

W tym laboratorium utworzysz nowy interfejs VLAN, użyjesz tego interfejsu do utworzenia nowej sieci WLAN i zabezpieczysz tę sieć WLAN za pomocą WPA2-Enterprise. Skonfigurujesz również WLC do używania

korporacyjnego serwera RADIUS do uwierzytelniania użytkowników. Ponadto konfiguracja WLC będzie korzystała z serwera SNMP.

Instrukcje

Część 1: Tworzenie nowej sieci WLAN

Krok 1: Utwórz nowy interfejs VLAN.

Każda sieć WLAN wymaga wirtualnego interfejsu w sieci WLC. Interfejsy te są znane jako interfejsy dynamiczne. Interfejs wirtualny ma przypisany identyfikator sieci VLAN, a ruch korzystający z interfejsu zostanie znakowany jako ruch VLAN. Dlatego połączenia między AP, WLC i routerem są realizowane portami trunk. Aby ruch z wielu sieci WLAN był przesyłany przez sieć, ruch w sieciach WLAN VLAN musi być trankingowy.

- a. Otwórz okno Web Browser z zakładki Desktop Admin PC. Połącz się z adresem IP WLC przez HTTPS.
- b. Zaloguj się, podając nazwę użytkownika admin i hasło Cisco123.
- c. Kliknij menu **Controller**, a następnie kliknij **Interfaces** z menu po lewej stronie. Zobaczysz domyślny interfejs wirtualny i interfejs zarządzania, do którego jesteś podłączony.
- d. Kliknij przycisk **New** w prawym górnym rogu strony. Może być konieczne przewijanie strony w prawo, aby go zobaczyć.
- e. Wprowadź nazwę nowego interfejsu. Nazwiemy to WLAN-5. Skonfiguruj identyfikator sieci VLAN jako 5. Jest to sieć VLAN, która będzie przenosić ruch dla sieci WLAN, którą tworzymy później. Kliknij Apply. Prowadzi to do ekranu konfiguracji interfejsu VLAN.
- f. Najpierw skonfiguruj interfejs, aby użył fizycznego portu numer **1**. Wiele interfejsów VLAN może korzystać z tego samego portu fizycznego, ponieważ interfejsy fizyczne są jak dedykowane porty trunk.
- g. Zaadresuj interfejs w następujący sposób:

Adres IP: 192.168.5.254

Maska: 255.255.255.0

Brama: 192.168.5.1

Główny serwer DHCP: 192.168.5.1

Ruch użytkownika w sieci WLAN korzystającej z tego interfejsu VLAN będzie odbywał się w sieci 192.168.5.0/24. Domyślną bramą jest adres interfejsu na routerze R-1. Na routerze skonfigurowano pulę DHCP. Adres, który konfigurujemy tutaj dla DHCP informuje WLC, aby przesyłał wszystkie żądania DHCP, które odbiera od hostów w sieci WLAN do serwera DHCP na routerze.

h. Pamiętaj, aby kliknąć Apply, aby wprowadzić zmiany i kliknąć przycisk OK, aby odpowiedzieć na komunikat ostrzegawczy. Kliknij przycisk Save Configuration, aby konfiguracja była dostępna po ponownym uruchomieniu usługi WLC.

Krok 2: Skonfiguruj usługę WLC do korzystania z serwera usługi RADIUS.

WPA2-Enterprise używa zewnętrznego serwera RADIUS do uwierzytelniania użytkowników sieci WLAN. Na serwerze usługi RADIUS można skonfigurować indywidualne konta użytkowników z unikatowymi nazwami użytkownika i hasłami. Zanim usługa WLC będzie mogła korzystać z usług serwera usługi RADIUS, WLC musi być skonfigurowana z adresem serwera.

- a. Kliknij menu Security w WLC.
- b. Kliknij przycisk New i wprowadź adres IP serwera usługi RADIUS w polu Adres IP serwera.

 c. Serwer usługi RADIUS uwierzytelnia WLC, zanim umożliwi WLC dostęp do informacji o koncie użytkownika, które znajdują się na serwerze. Wymaga to wspólnej wartości tajnej. Użyj Cisco123. Potwierdź współdzielony klucz i kliknij Apply.

Uwaga: Nie jest to dobra praktyka, aby ponownie używać haseł. To ćwiczenie wykorzystuje ponownie hasła tylko po to, aby ułatwić wykonywanie czynności i przeglądanie.

Krok 3: Utwórz nową sieć WLAN.

Utwórz nową sieć WLAN. Użyj nowo utworzonego interfejsu VLAN dla nowej sieci WLAN.

- a. Kliknij wpis **WLANs** na pasku menu. Zlokalizuj pole rozwijane w prawym górnym rogu ekranu WLAN. Będzie to napisane " **Create New**". Kliknij przycisk **Go**, aby utworzyć nową sieć WLAN.
- b. Wprowadź Profile Name dla nowej sieci WLAN. Użyj nazwy profilu Floor 2 Employees. Przypisz identyfikator SSID SSID-5 do sieci WLAN. Zmień identyfikator na 5. Hosty będą musiały użyć tego identyfikatora SSID, aby dołączyć do sieci. Po zakończeniu kliknij przycisk Apply, aby zaakceptować ustawienia.

Uwaga: Identyfikator jest dowolną wartością, która jest używana jako etykieta dla sieci WLAN. W tym przypadku skonfigurowaliśmy go jako 5, aby był zgodny z VLAN dla sieci WLAN. To może być dowolna dostępna wartość.

- c. Kliknij Apply, aby ustawienia weszły w życie.
- d. Po utworzeniu sieci WLAN można skonfigurować własności sieci. Kliknij przycisk **Enabled**, aby sieć WLAN działała. Częstym błędem jest przypadkowe pominięcie tego kroku.
- e. Wybierz interfejs VLAN, który będzie używany dla nowej sieci WLAN. WLC użyje tego interfejsu dla ruchu użytkownika w sieci. Kliknij pole rozwijane dla Interface/Interface Group (G). Wybierz interfejs, który stworzyliśmy w kroku 1.
- f. Idź do zakładki Advanced. Przewiń do sekcji FlexConnect interfejsu.
- g. Kliknij, aby włączyć FlexConnect Local Switching i FlexConnect Local Auth.
- h. Kliknij przycisk **Apply**, aby włączyć nową sieć WLAN. Jeśli zapomnisz to zrobić, WLAN nie będzie działać.

Krok 4: Skonfiguruj zabezpieczenia WLAN.

Zamiast WPA2-PSK, będziemy skonfigurować nową sieć WLAN do korzystania WPA2-Enterprise.

- a. Kliknij identyfikator sieci WLAN nowo utworzonej sieci WLAN, aby kontynuować jego konfigurację, jeśli to konieczne.
- b. Kliknij na zakładkę Security. Na karcie Warstwa 2 wybierz WPA+WPA2 z rozwijanego pola.
- c. W obszarze Parametry WPA+WPA2 włącz WPA2 Policy. Kliknij pozycję 802.1X w obszarze Zarządzanie kluczami uwierzytelniania. To informuje WLC, aby używał protokołu 802.1X do zewnętrznego uwierzytelniania użytkowników.
- d. Kliknij kartę **AAA Servers**. Otwórz menu rozwijane obok pozycji Server 1 w kolumnie Authentication Servers i wybierz serwer, który skonfigurowaliśmy w kroku 2.
- e. Kliknij przycisk **Apply**, aby wykonać tę konfigurację. Skonfigurowałeś teraz WLC do używania serwera RADIUS do uwierzytelniania użytkowników, którzy próbują połączyć się z siecią WLAN.

Część 2: Konfiguracja zakresu DHCP i SNMP

Krok 1: Skonfiguruj zakres DHCP.

WLC oferuje własny wewnętrzny serwer DHCP. Firma Cisco zaleca, aby serwer DHCP WLAN nie był używany do usług DHCP o dużej objętości, takich jak te wymagane przez większe sieci WLAN użytkowników.

Jednak w mniejszych sieciach serwer DHCP może być używany do dostarczania adresów IP do LAP podłączonych do sieci przewodowej zarządzania. W tym kroku będziemy skonfigurować zakres DHCP na WLC i używać go do adresowania LAP-1.

- a. Powinien być podłączony do GUI WLC z Admin PC.
- b. Kliknij menu Controller, a następnie kliknij polecenie Interfaces.

Jakie interfejsy są obecne?

c. Kliknij interfejs management. Zapisz tutaj informacje adresowe.

Adres IP.

Maska sieci:

Brama:

Główny serwer DHCP:

- d. Chcemy, aby WLC używał własnego serwera DHCP do adresowania urządzeń w bezprzewodowej sieci zarządzania, takich jak lekkie punkty dostępowe. Z tego powodu wprowadź adres IP interfejsu zarządzania WLC jako podstawowy adres serwera DHCP. Kliknij Apply. Kliknij przycisk OK, aby potwierdzić wszystkie wyświetlane komunikaty ostrzegawcze.
- e. W menu po lewej stronie rozwiń sekcję Internal DHCP Server. Kliknij DHCP Scope.
- f. Aby utworzyć zakres DHCP, kliknij przycisk New....
- g. Nazwij zakres Wired Management. Ten zakres DHCP zostanie skonfigurowany w taki sposób, aby udostępniał adresy do sieci infrastruktury przewodowej łączącej komputery administratora, WLC-1 i LAP-1.
- h. Kliknij przycisk Apply, aby utworzyć nowy zakres DHCP.
- i. Kliknij nowy zakres w tabeli DHCP Scope, aby skonfigurować informacje adresowe dla zakresu. Wprowadź następujące informacje

Adres początkowy puli: 192.168.200.240

Adres końcowy puli: 192.168.200.249

Status: Enabled

Podaj wartości dla Network, Netmask i Default Routers na podstawie informacji zebranych w kroku 1c.

j. Kliknij przycisk Apply, aby aktywować konfigurację. Kliknij przycisk Save Configuration w prawym górnym rogu interfejsu WLC, aby zapisać pracę tak, aby była ona dostępna po ponownym uruchomieniu WLC.

Wewnętrzny serwer DHCP dostarczy teraz adres do LAP-1 po krótkim opóźnieniu. Gdy LAP-1 ma swój adres IP, zostanie utworzony tunel CAPWAP, a LAP-1 będzie mógł zapewnić dostęp do sieci WLAN Floor 2 Employees (SSID-5). Jeśli przesuniesz kursor myszy nad LAP-1 w topologii, powinieneś zobaczyć jego adres IP, stan tunelu CAPWAP i sieć WLAN, do której zapewnia dostęp LAP-1.

Krok 2: Skonfiguruj SNMP

a. Kliknij menu Management w interfejsie graficznym WLC i rozwiń wpis SNMP w menu po lewej stronie.

- b. Kliknij Trap Receivers, a następnie New...
- c. Wprowadź community string jako WLAN_SNMP i adres IP serwera 172.31.1.254.
- d. Kliknij przycisk Apply, aby zakończyć konfigurację.

Część 3: Łączenie hostów z siecią

Krok 1: Skonfiguruj hosta, aby połączyć się z siecią przedsiębiorstwa.

W aplikacji klienta Packet Tracer PC Wireless musisz skonfigurować profil WLAN, aby podłączyć się do WPA2-Enterprise WLAN.

- a. Kliknij pozycję Wireless Host i otwórz aplikację PC Wireless.
- b. Kliknij kartę **Profile**, a następnie kliknij przycisk **New**, aby utworzyć nowy profil. Nazwij profil **WLC NET**.
- c. Zaznacz nazwę sieci bezprzewodowej dla utworzonej wcześniej sieci WLAN i kliknij opcję **Advanced Setup**.
- d. Sprawdź, czy identyfikator SSID bezprzewodowej sieci LAN jest obecny, a następnie kliknij przycisk Next. Host bezprzewodowy powinien zobaczyć SSID-5. Jeśli tak nie jest, przesunąć kursor myszy na LAP-1, aby sprawdzić, czy komunikuje się z WLC. Okno popup powinno wskazywać, że LAP-1 jest świadomy SSID-5. Jeśli tak nie jest, sprawdź konfigurację WLC. Można również ręcznie wprowadzić identyfikator SSID.
- e. Sprawdź, czy wybrano ustawienie sieci DHCP i kliknij przycisk Next.
- f. W polu rozwijanym Security wybierz WPA2-Enterprise. Kliknij przycisk Next.
- g. Wpisz login user1 i hasło User1Pass i kliknij Next.
- h. Zweryfikuj ustawienia profilu i kliknij przycisk Save.
- i. Wybierz profil WLC NET i kliknij przycisk Connect to Network. Po krótkim opóźnieniu powinieneś zobaczyć bezprzewodowe połączenie hosta z LAP-1. Możesz kliknąć przycisk Fast Forward Time, aby przyspieszyć proces, jeśli wydaje się, że trwa to zbyt długo.
- j. Upewnij się, że host sieci bezprzewodowej ma połączenie z siecią WLAN. Host sieci bezprzewodowej powinien otrzymać adres IP z serwera DHCP skonfigurowanego dla hostów na R1. Adres będzie w sieci 192.168.5.0/24. Możesz kliknąć przycisk Packet Tracer Fast Forward Time, aby przyspieszyć proces.

Krok 2: Przeprowadź test połączeń.

- a. Zamknij aplikację PC Wireless.
- b. Otwórz wiersz polecenia i potwierdź, że laptop Wireless Host uzyskał adres IP z sieci WLAN.

W jakiej sieci powinien znajdować się adres? Wyjaśnij.

c. Wykonaj ping bramy domyślnej, SW1 i serwera usługi RADIUS. Sukces oznacza pełną łączność w ramach tej topologii.

Pytania do przemyślenia

1. Serwer usługi RADIUS używa podwójnego mechanizmu uwierzytelniania. Jakie dwie rzeczy są uwierzytelniane przez serwer usługi RADIUS? Dlaczego uważasz, że jest to konieczne?

2. Jakie są zalety WPA2-Enterprise nad WPA2-PSK?