자동 AP에서 게스트에 대한 웹 인증 구성

목차

소개

이 문서에서는 AP 자체에 포함된 내부 웹 페이지를 사용하여 자동 액세스 포인트(AP)에서 게스트 액세스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 컨피그레이션을 시도하기 전에 이러한 주제에 대해 알고 있는 것이 좋습니다.

- 기본 작동을 위해 자동 AP를 구성하는 방법
- 자동 AP에서 로컬 RADIUS 서버를 구성하는 방법
- 레이어 3 보안 측정으로서의 웹 인증 작동 방식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 이미지 15.2(4)JA1을 실행하는 AIR-CAP3502I-E-K9
- Intel Centrino Advanced-N 6200 AGN 무선 어댑터(드라이버 버전 13.4.0.9)
- Microsoft Windows 7 신청자 유틸리티

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

웹 인증은 게스트가 브라우저를 열 때 클라이언트가 리디렉션되는 웹 포털에서 유효한 사용자 이름과 비밀번호를 제공할 때까지 자율 AP가 IP 트래픽(DHCP 및 DNS(Domain Name Server) 관련 패킷 제외)을 차단할 수 있도록 하는 L3(Layer 3) 보안 기능입니다.

웹 인증에서는 각 게스트에 대해 별도의 사용자 이름과 비밀번호를 정의해야 합니다. 게스트는 로컬 RADIUS 서버 또는 외부 RADIUS 서버에 의해 사용자 이름 및 비밀번호로 인증됩니다.

이 기능은 Cisco IOS Release 15.2(4)JA1에서 도입되었습니다.

AP 컨피그레이션

> **참고:** 이 문서에서는 AP의 BVI(Bridge Virtual Interface) 1에 IP 주소가 192.168.10.2 /24이고 DHCP 풀이 IP 주소 192.168.10.10~192.168.10.254(IP 주소 192.168.10.1~192.168.10.10은 제외)의 AP에 내부적으로 정의되어 있다고 가정합니다.

게스트 액세스를 위한 AP를 구성하려면 다음 단계를 완료합니다.

1. 새 SSID(Service Set Identifier)를 추가하고 **Guest**로 이름을 **지정하고** 웹 인증을 위해 구성합니다.

```
ap(config)#dot11 ssid Guest

ap(config-ssid)#authentication open

ap(config-ssid)#web-auth

ap(config-ssid)#guest-mode

ap(config-ssid)#exit
```

2. 인증 규칙을 생성합니다. 여기서 프록시 인증 프로토콜을 지정하고 이름을 **web_auth**로 지정해야 합니다.

```
ap(config)#ip admission name web_auth proxy http
```

3. SSID(**Guest**) 및 인증 규칙(**web_auth**)을 무선 인터페이스에 적용합니다. 이 예에서는 802.11b/g 라디오를 사용합니다.

```
ap(config)#interface dot11radio 0

ap(config-if)#ssid Guest

ap(config-if)#ip admission web_auth

ap(confi-if)#no shut

ap(config-if)#exit
```

4. 사용자 자격 증명이 인증되는 위치를 지정하는 방법 목록을 정의합니다. 메서드 목록 이름을 **web_auth** 인증 규칙과 연결하고 이름을 **web_list로 지정합니다**.

```
ap(config)#ip admission name web_auth method-list authentication web_list
```

5. AP 및 로컬 RADIUS 서버에서 AAA(Authentication, Authorization, and Accounting)를 구성하고 AP의 로컬 RADIUS 서버와 연결 하려면 다음 단계를 완료합니다.

   AAA 활성화:

```
ap(config)#aaa new-model
```

   로컬 RADIUS 서버를 구성합니다.

```
ap(config)#radius-server local

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   게스트 어카운트를 생성하고 해당 수명(분)을 지정합니다. 사용자 이름 및 비밀번호가 user1인 사용자 계정을 한 개로 만들고 수명 값을 60분으로 설정합니다.

```
ap(config)#dot11 guest

ap(config-guest-mode)#username  user1 lifetime 60 password user1

ap(config-guest-mode)#exit

ap(config)#
```

   동일한 프로세스를 사용하여 다른 사용자를 생성할 수 있습니다.

   참고: 게스트 계정을 생성하려면 **radius-server local**을 활성화해야 합니다.
   AP를 RADIUS 서버로 정의합니다.

```
ap(config)#radius-server host 192.168.10.2 auth-port 1812
 acct-port 1813 key cisco
```

웹 인증 목록을 로컬 서버와 연결합니다.

```
ap(config)#aaa authentication login web_list group radius
```

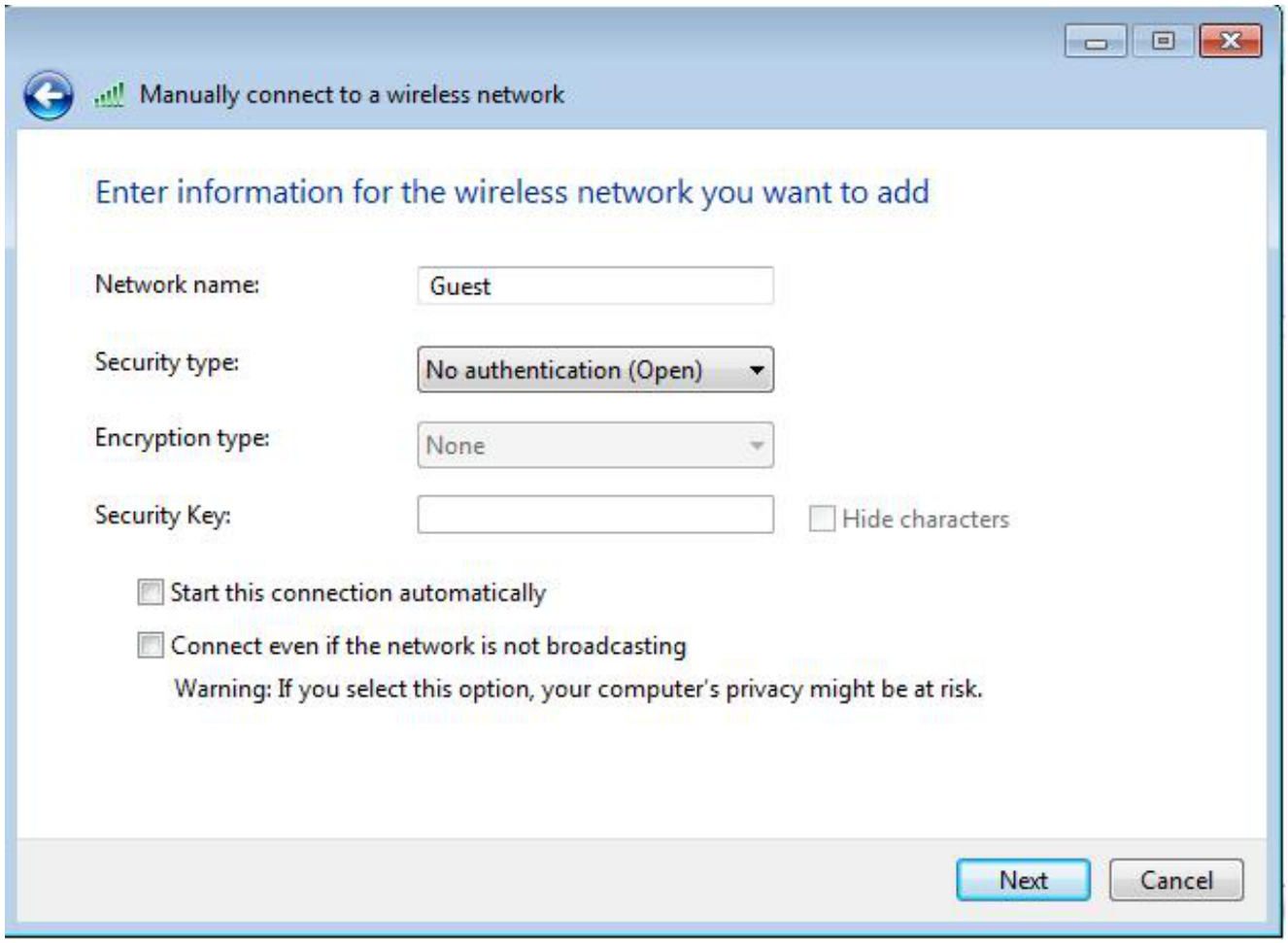
참고: 게스트 사용자 계정을 호스팅하기 위해 외부 radius 서버를 사용할 수 있습니다. 이렇게 하려면 AP IP 주소 대신 외부 서버를 가리키도록 **radius-server host** 명령을 구성합니다.

무선 클라이언트 구성

무선 클라이언트를 구성하려면 다음 단계를 완료합니다.

1. Windows 서 플리 컨 트 유틸리티에서 SSID **Guest**를 사용하여 무선 네트워크를 구성하려면 **Network and Internet(네트워크 및 인터넷) > Manage Wireless Networks(무선 네트워크 관리)로** 이동하고 **Add(추가)**를 클릭합니다.

2. **무선 네트워크에 수동으로 연결**을 선택하고 다음 이미지와 같이 필요한 정보를 입력합니다.



3. Next(**다음)를 클릭합니다**.

다음을 확인합니다.

컨피그레이션이 완료되면 클라이언트가 SSID에 정상적으로 연결할 수 있으며 AP 콘솔에 다음과 같은 내용이 표시됩니다.

```
%DOT11-6-ASSOC: Interface Dot11Radio0, Station ap 0027.10e1.9880
 Associated KEY_MGMT[NONE]

ap#show dot11 ass

802.11 Client Stations on Dot11Radio0:

SSID [Guest] :

MAC Address    IP address   IPV6 address  Device    Name  Parent  State

0027.10e1.9880  0.0.0.0     ::           ccx-client  ap   self    Assoc
```

클라이언트의 동적 IP 주소가 192.168.10.11입니다. 그러나 클라이언트의 IP 주소를 ping하려고 하면 클라이언트가 완전히 인증되지 않아 실패합니다.

```
ap#PING 192.168.10.11

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)
```

클라이언트가 브라우저를 열고 **http://1.2.3.4**에 연결하려고 시도하면 클라이언트가 내부 로그인 페이지로 리디렉션됩니다.

Username:

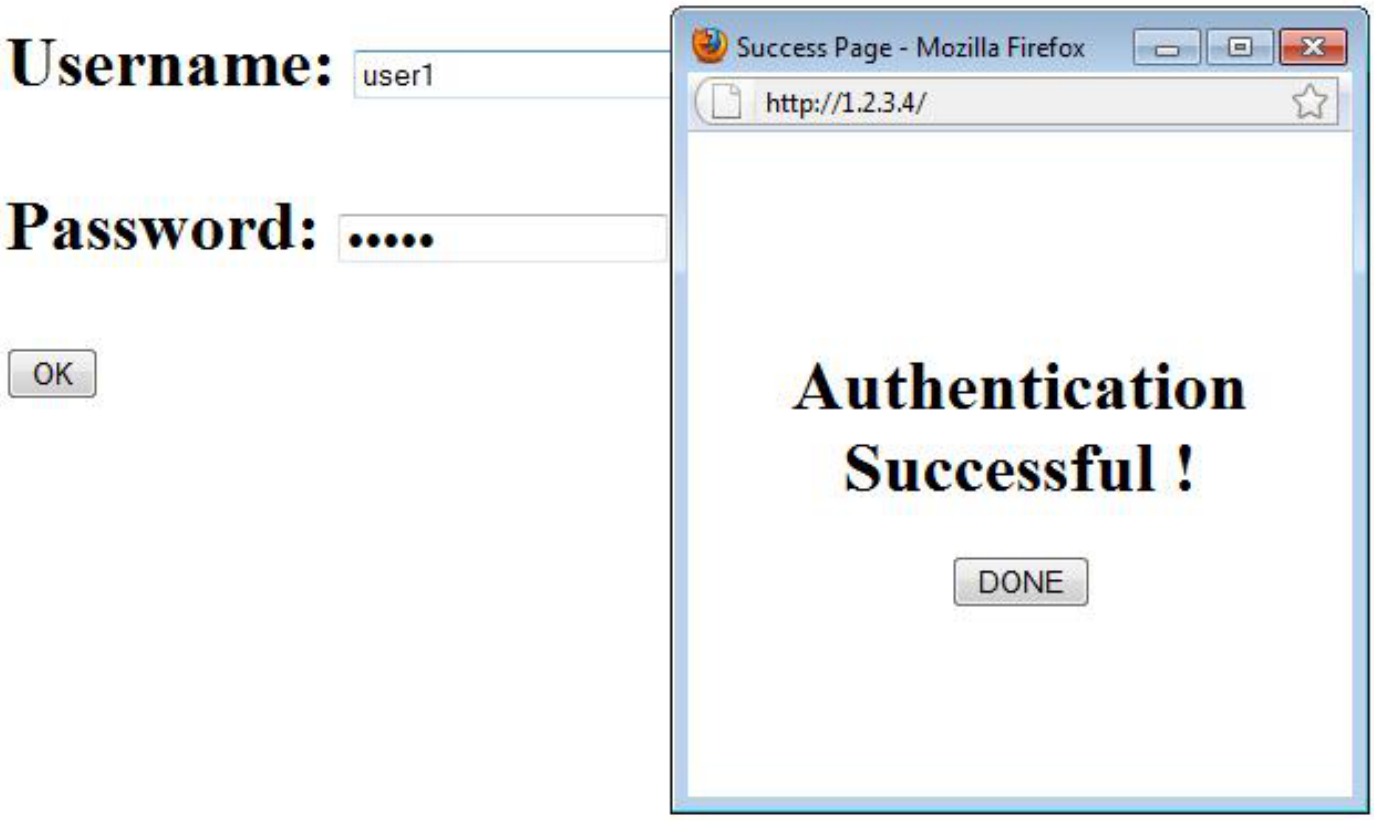
Password:

OK

> **참고:** 이 테스트는 DNS가 테스트에서 사용되지 않았기 때문에 DNS를 통해 URL을 변환할 필요 없이 직접 입력된 임의 IP 주소(입력된 URL은 **1.2.3.4**)로 완료됩니다. 일반적인 시나리오에서 사용자는 홈 페이지 URL을 입력하며, 클라이언트가 HTTP GET 메시지를 확인된 주소로 보낼 때까지 DNS 트래픽이 허용되며, 이는 AP에서 가로채입니다. AP는 웹 사이트 주소를 스푸핑하고 내부적으로 저장된 로그인 페이지로 클라이언트를 리디렉션합니다.

클라이언트가 로그인 페이지로 리디렉션되면 AP 컨피그레이션에 따라 로컬 RADIUS 서버에 대해 사용자 자격 증명이 입력되고 확인됩니다. 인증에 성공하면 클라이언트에서 들어오고 클라이언트로 이동하는 트래픽이 완전히 허용됩니다.

인증 성공 후 사용자에게 전송되는 메시지는 다음과 같습니다.



인증에 성공하면 클라이언트 IP 정보를 볼 수 있습니다.

```
ap#show dot11 ass
802.11 Client Stations on Dot11Radio0:
SSID [Guest] :
MAC Address    IP address    IPV6 address  Device   Name  Parent  State
0027.10e1.9880  192.168.10.11 ::       ccx-client  ap    self   Assoc
```

인증이 성공적으로 완료된 후 클라이언트에 ping하는 작업은 올바르게 작동해야 합니다.

```
ap#ping 192.168.10.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6 ms
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

> **참고:** 웹 인증 중에 AP 간 로밍은 원활한 환경을 제공하지 않습니다. 클라이언트는 연결되는 각 새 AP에 로그인해야 하기 때문입니다.

사용자 지정

라우터 또는 스위치의 IOS와 마찬가지로, 사용자 지정 파일을 사용하여 페이지를 사용자 지정할 수 있습니다. 그러나 외부 웹 페이지로 리디렉션할 수는 없습니다.

포털 파일을 사용자 지정하려면 다음 명령을 사용합니다.

- **ip admission proxy http 로그인 페이지 파일**
- **ip admission proxy http 만료된 페이지 파일**
- **ip admission proxy http 성공 페이지 파일**
- **ip admission proxy http 실패 페이지 파일**