Configurazione dell'autenticazione Web per guest in access point autonomi

Sommario

Introduzione

In questo documento viene descritto come configurare l'accesso guest ai punti di accesso autonomi con l'utilizzo della pagina Web interna incorporata nell'access point stesso.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti prima di provare la configurazione:

- Come configurare i punti di accesso autonomi per le operazioni di base
- Come configurare il server RADIUS locale su access point autonomi
- Funzionamento dell'autenticazione Web come misura di sicurezza di livello 3

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AIR-CAP3502I-E-K9 con immagine Cisco IOS® 15.2(4)JA1

- Scheda wireless Intel Centrino Advanced-N 6200 AGN (driver versione 13.4.0.9)
- Utilità supplicant di Microsoft Windows 7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'autenticazione Web è una funzione di sicurezza di layer 3 (L3) che consente ai punti di accesso autonomi di bloccare il traffico IP (ad eccezione dei pacchetti correlati a DHCP e DNS (Domain Name Server)) finché il guest non fornisce un nome utente e una password validi nel portale Web a cui il client viene reindirizzato quando viene aperto un browser.

Con l'autenticazione Web, è necessario definire un nome utente e una password distinti per ogni guest. Il guest viene autenticato con il nome utente e la password dal server RADIUS locale o da un server RADIUS esterno.

Questa funzione è stata introdotta in Cisco IOS versione 15.2(4)JA1.

Configurazione AP

> **Nota:** In questo documento si presume che il protocollo BVI (Bridge Virtual Interface) 1 sull'access point abbia un indirizzo IP di 192.168.10.2 /24 e che il pool DHCP sia definito internamente sull'access point per gli indirizzi IP da 192.168.10.10 a 192.168.10.254 (gli indirizzi IP da 192.168.10.1 a 192.168.10.10 sono esclusi).

Completare questa procedura per configurare l'access point per l'accesso guest:

1. Aggiungere un nuovo SSID (Service Set Identifier), denominarlo **Guest** e configurarlo per l'autenticazione Web:

```
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. Creare una regola di autenticazione, in cui è necessario specificare il protocollo di autenticazione proxy e denominarlo **web_auth**:

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

3. Applicare il SSID (**Guest**) e la regola di autenticazione (**web_auth**) all'interfaccia radio. Nell'esempio viene usata la radio 802.11b/g:

```
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. Definire l'elenco dei metodi che specifica dove vengono autenticate le credenziali utente. Collegare il nome dell'elenco di metodi alla regola di autenticazione **web_auth** e denominarlo **elenco_Web**:

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

5. Completare la procedura seguente per configurare Authentication, Authorization, and Accounting (AAA) sul punto di accesso e sul server RADIUS locale e collegare l'elenco dei metodi al server RADIUS locale sul punto di accesso:

   Abilitare AAA:

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

   Configurare il server RADIUS locale:

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

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   Creare gli account Guest e specificarne la durata (in minuti). Creare un account utente con nome utente e password **user1** e impostare il valore della durata su 60 minuti:

```
ap(config)#dot11 guest

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

ap(config-guest-mode)#exit

ap(config)#
```

È possibile creare altri utenti con lo stesso processo.

Nota: Per creare account guest, è necessario abilitare **il server RADIUS locale**.
Definire l'access point come server RADIUS:

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

Collegare l'elenco di autenticazione Web al server locale:

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

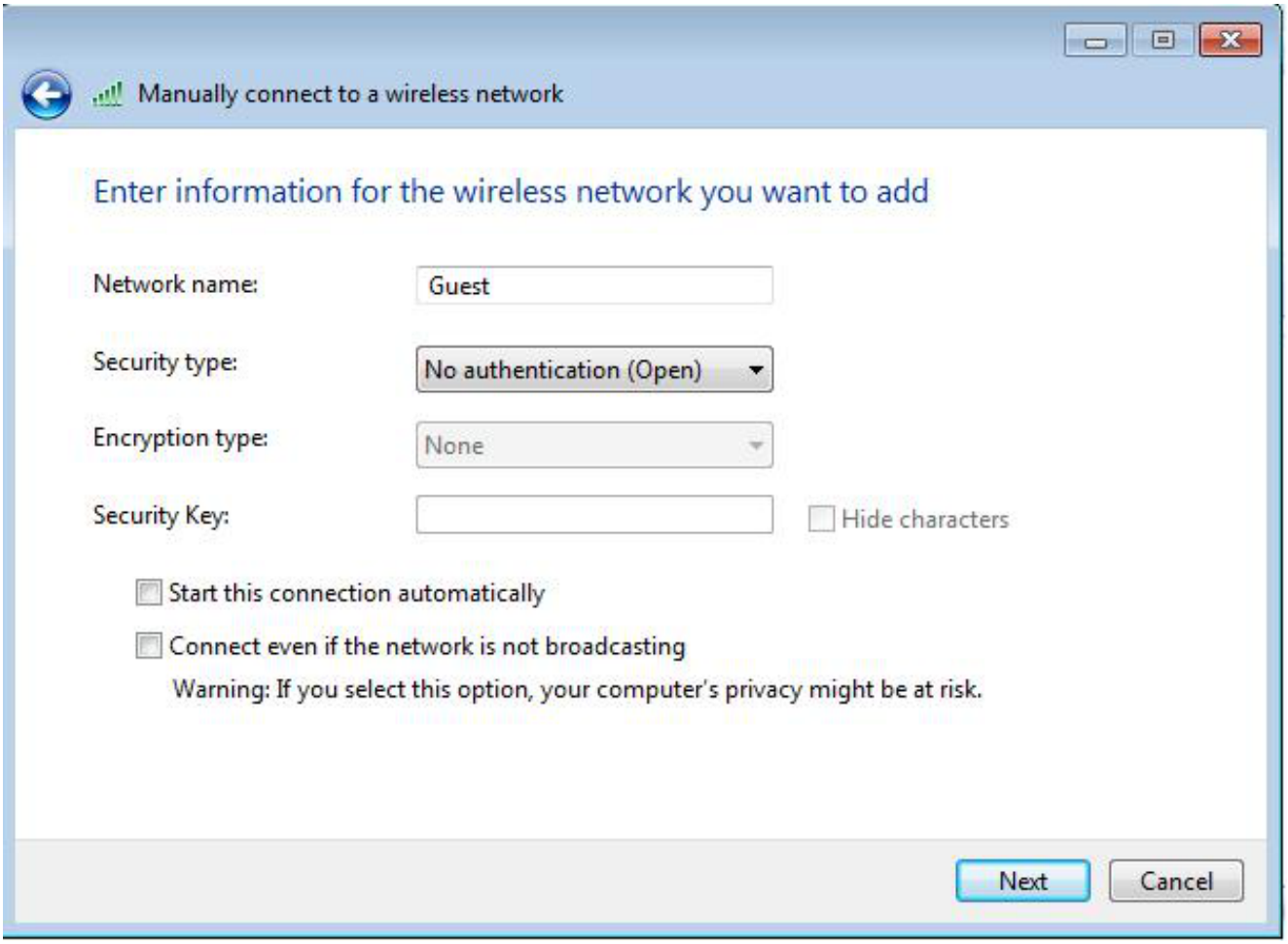
Nota: È possibile utilizzare un server RADIUS esterno per ospitare gli account utente guest. A tal fine, configurare il comando **radius-server host** in modo che punti al server esterno anziché all'indirizzo IP dell'access point.

Configurazione del client wireless

Per configurare il client wireless, completare la procedura seguente:

1. Per configurare la rete wireless sull'utility di Windows supplicant con il SSID denominato **Guest**, selezionare **Rete e Internet > Gestisci reti wireless**, quindi fare clic su **Aggiungi**.

2. Selezionare **Connetti manualmente a una rete wireless** e immettere le informazioni necessarie, come mostrato nell'immagine:



3. Fare clic su **Next** (Avanti).

Verifica

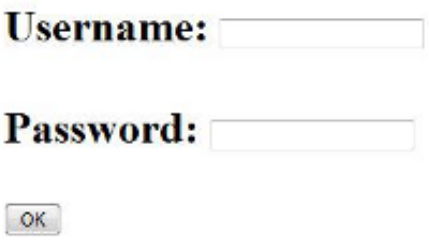
Al termine della configurazione, il client può connettersi al SSID normalmente e ciò si verifica sulla console AP:

```
%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
```

L'indirizzo IP dinamico del client è 192.168.10.11. Tuttavia, il tentativo di eseguire il ping dell'indirizzo IP del client ha esito negativo perché il client non è completamente autenticato:

```
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)
```

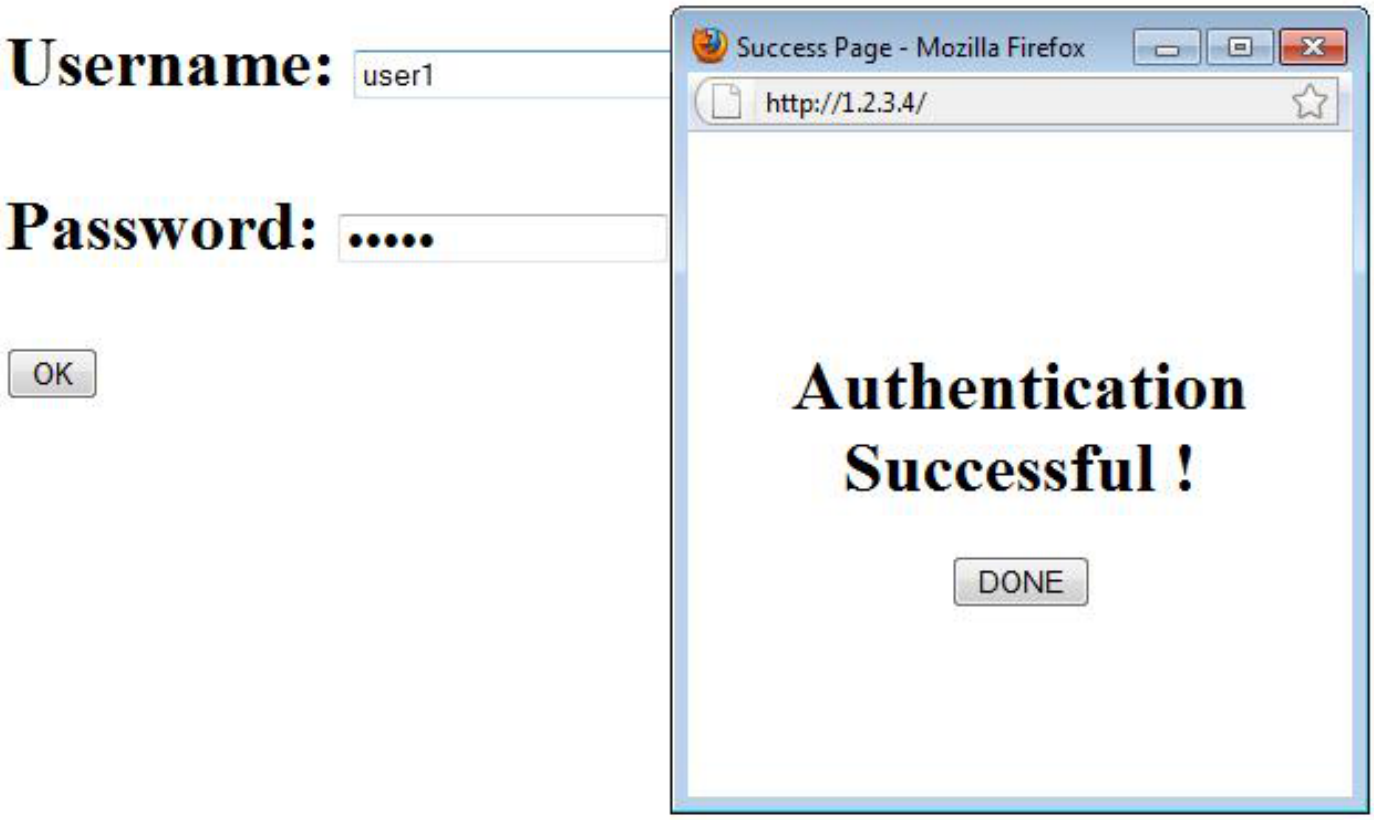
Se il client apre un browser e tenta di raggiungere **http://1.2.3.4** ad esempio, il client viene reindirizzato alla pagina di accesso interna:



> **Nota:** Questo test viene completato con un indirizzo IP casuale immesso direttamente (qui l'URL immesso è **1.2.3.4**) senza la necessità di tradurre un URL tramite il DNS, perché il DNS non è stato utilizzato nel test. In scenari normali, l'utente immette l'URL della home page e il traffico DNS è consentito fino a quando il client non invia il messaggio HTTP GET all'indirizzo risolto, intercettato dall'access point. L'access point falsifica l'indirizzo del sito Web e reindirizza il client alla pagina di accesso memorizzata internamente.

Una volta reindirizzato il client alla pagina di accesso, le credenziali utente vengono immesse e verificate rispetto al server RADIUS locale, in base alla configurazione dell'access point. Dopo l'autenticazione, il traffico proveniente dal client e diretto al client è completamente consentito.

Di seguito è riportato il messaggio inviato all'utente dopo l'autenticazione:



Una volta completata l'autenticazione, è possibile visualizzare le informazioni sull'IP del client:

```
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
```

I ping al client dopo il completamento dell'autenticazione dovrebbero funzionare correttamente:

```
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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

> **Nota:** Il roaming tra punti di accesso durante l'autenticazione Web non garantisce un'esperienza ottimale, in quanto i client devono accedere a ogni nuovo punto di accesso a cui si connettono.

Personalizzazione

Analogamente agli IOS sui router o sugli switch, è possibile personalizzare la pagina con un file personalizzato; tuttavia, non è possibile reindirizzare a una pagina web esterna.

Utilizzare questi comandi per personalizzare i file del portale:

- file della pagina di login http del proxy di ammissione ip
- file di paging http scaduto proxy di ammissione ip
- file della pagina http proxy di ammissione ip
- file di paging http proxy di ammissione ip