Web verificatie voor gasten configureren op autonome APs

Inhoud

Inleiding

Dit document beschrijft hoe u de toegang van uw workflow kunt configureren op basis van autonome access points (APs) met behulp van de interne webpagina die in het AP zelf is ingesloten.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben van deze onderwerpen voordat u deze configuratie probeert:

- Hoe te om autonome APs voor basiswerking te configureren
- Hoe u de lokale RADIUS-server op autonome AP's kunt configureren
- Hoe web authenticatie als een Layer 3 veiligheidsmaatregel werkt

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- AIR-CAP 3502I-E-K9 waarmee Cisco IOS-afbeelding 15.2(4)JA1 wordt uitgevoerd

- Intel Centrino Advanced-N 6200 AGN draadloze adapter (driver versie 13.4.0.9)
- Microsoft Windows 7-applicatie

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Web Authentication is een Layer 3 (L3) security functie die de autonome AP's in staat stelt om IP-verkeer te blokkeren (behalve DHCP- en Domain Name Server (DNS)-gerelateerde pakketten) totdat de gast een geldige gebruikersnaam en wachtwoord oplevert in het webportaal waarop de client wordt hergericht wanneer een browser wordt geopend.

Met web authenticatie moet een aparte gebruikersnaam en wachtwoord worden gedefinieerd voor elke gast. De gast is bevonden met de gebruikersnaam en het wachtwoord door de lokale RADIUS-server of een externe RADIUS-server.

Deze optie is geïntroduceerd in Cisco IOS release 15.2(4)JA1.

AP-configuratie

> **Opmerking:** Dit document gaat ervan uit dat Bridge Virtual Interface (BVI) 1 op de AP een IP-adres heeft van 192.168.10.2/24 en dat de DHCP-pool intern op AP is gedefinieerd voor IP-adressen 192.168.10.10 tot 192.168.10.254 IP-adressen 192.168.10.1 t/m 192.168.10.10 zijn uitgesloten).

Voltooi deze stappen om AP voor gasttoegang te vormen:

1. Voeg een nieuwe Identifier (SSID) toe, noem het **Gast en** stel het voor web authenticatie in:

```
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. Maak een authenticatieregel, waar u het protocol voor proxy-verificatie moet specificeren en noem het **web_auth**:

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

3. Pas de SSID (**Guest**) en de authenticatieregel (**web_auth**) op de radio interface toe. In dit voorbeeld wordt 802.11b/g-radio gebruikt:

```
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. Defineert de methodelijst die specificeert waar de gebruikersreferenties voor authentiek zijn verklaard. Koppel de naam van de methodelijst met de authenticatieregel **web_auth** en noem het **web_list**:

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

5. Voltooi deze stappen om verificatie, autorisatie en accounting (AAA) te configureren op de AP- en lokale RADIUS-server en de methodelijst te koppelen aan de lokale RADIUS-server op het AP:

   AAA inschakelen:

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

   Configuratie van de lokale RADIUS-server:

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

ap(config-radsrv)#nas 192.168.10.2 key cisco

ap(config-radsrv)#exit
```

   Maak de gastrekeningen, en specificeer hun leven (in minuten). Maak één gebruikersaccount met een gebruikersnaam en wachtwoord van **gebruiker1** en stel de levenswaarde in op 60 minuten:

```
ap(config)#dot11 guest

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

ap(config-guest-mode)#exit

ap(config)#
```

U kunt andere gebruikers met hetzelfde proces maken.

Opmerking: U moet de **lokale** server inschakelen om een gastaccount aan te maken. Defineert AP als een RADIUS-server:

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

Koppel de website-authenticatielijst met de lokale server:

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

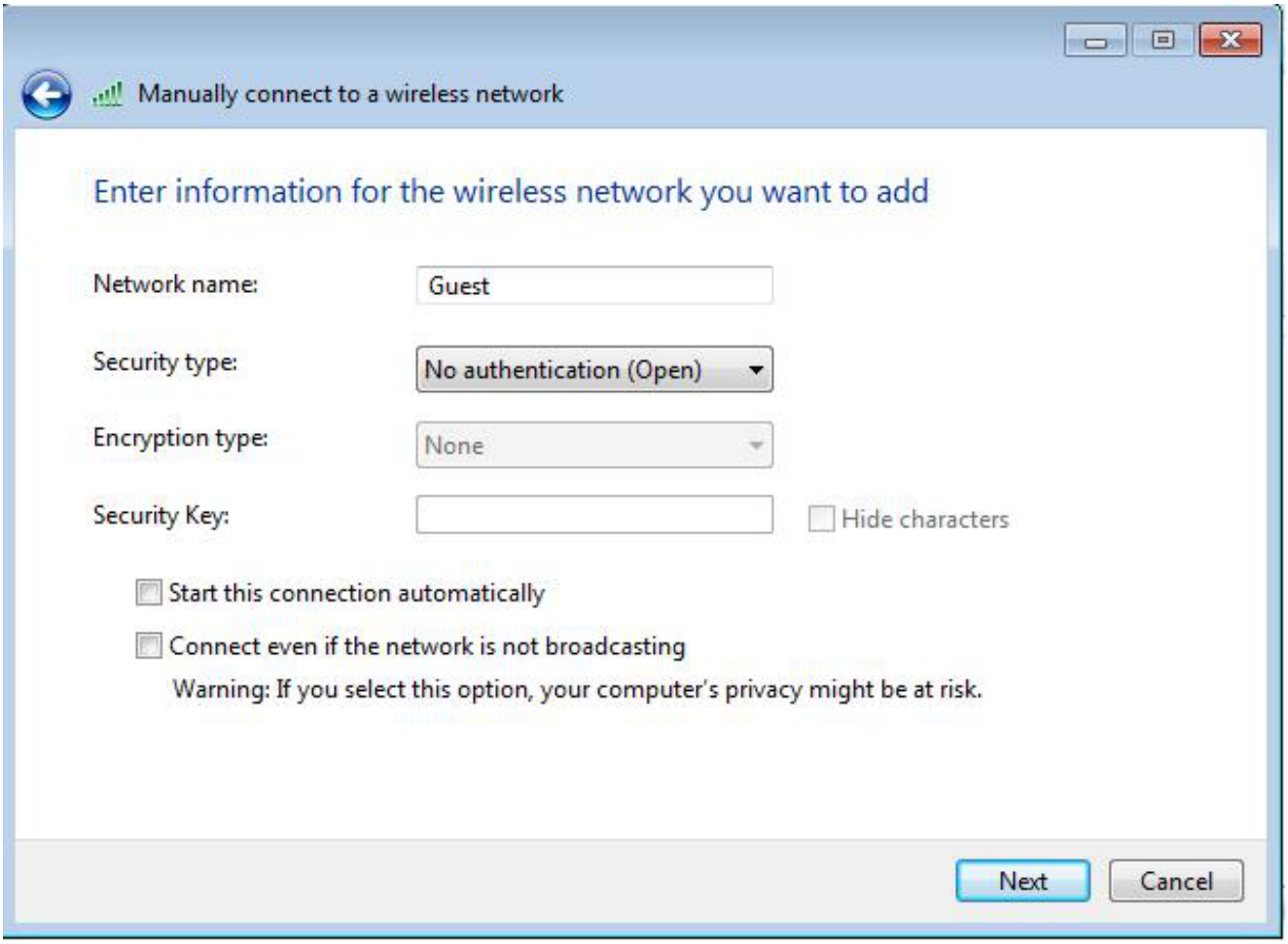
Opmerking: U kunt een externe straal server gebruiken om de gastgebruikersrekeningen te ontvangen. Om dit te doen, moet u de opdracht van de **Straal server-host** aanwijzen naar de externe server in plaats van het AP IP-adres.

De draadloze client configureren

Volg deze stappen om de draadloze client te configureren:

1. Om het draadloze netwerk op uw vensters te configureren hebt u een applicatie nodig met de naam **Guest** bij SSID, navigeer dan naar **Netwerk en Internet > Draadloze netwerken beheren** en klik op **Add**.

2. Selecteer **handmatig verbinding maken met een draadloos netwerk** en voer de gewenste informatie in, zoals in deze afbeelding:



3. Klik op **Volgende**.

Verifiëren

Nadat de configuratie is voltooid, kan de client normaal verbinding maken met SSID en u ziet dit in de AP-console:

```
%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
```

De client heeft een dynamisch IP-adres van 192.168.10.11. Wanneer u echter probeert het IP-adres van de client te pingelen, mislukt dit omdat de client niet volledig geauthentificeerd is:

```
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)
```

Als de client een browser opent en probeert om **http://1.2.3.4** te bereiken, bijvoorbeeld, wordt de client opnieuw gericht naar de interne loginpagina:

Username:

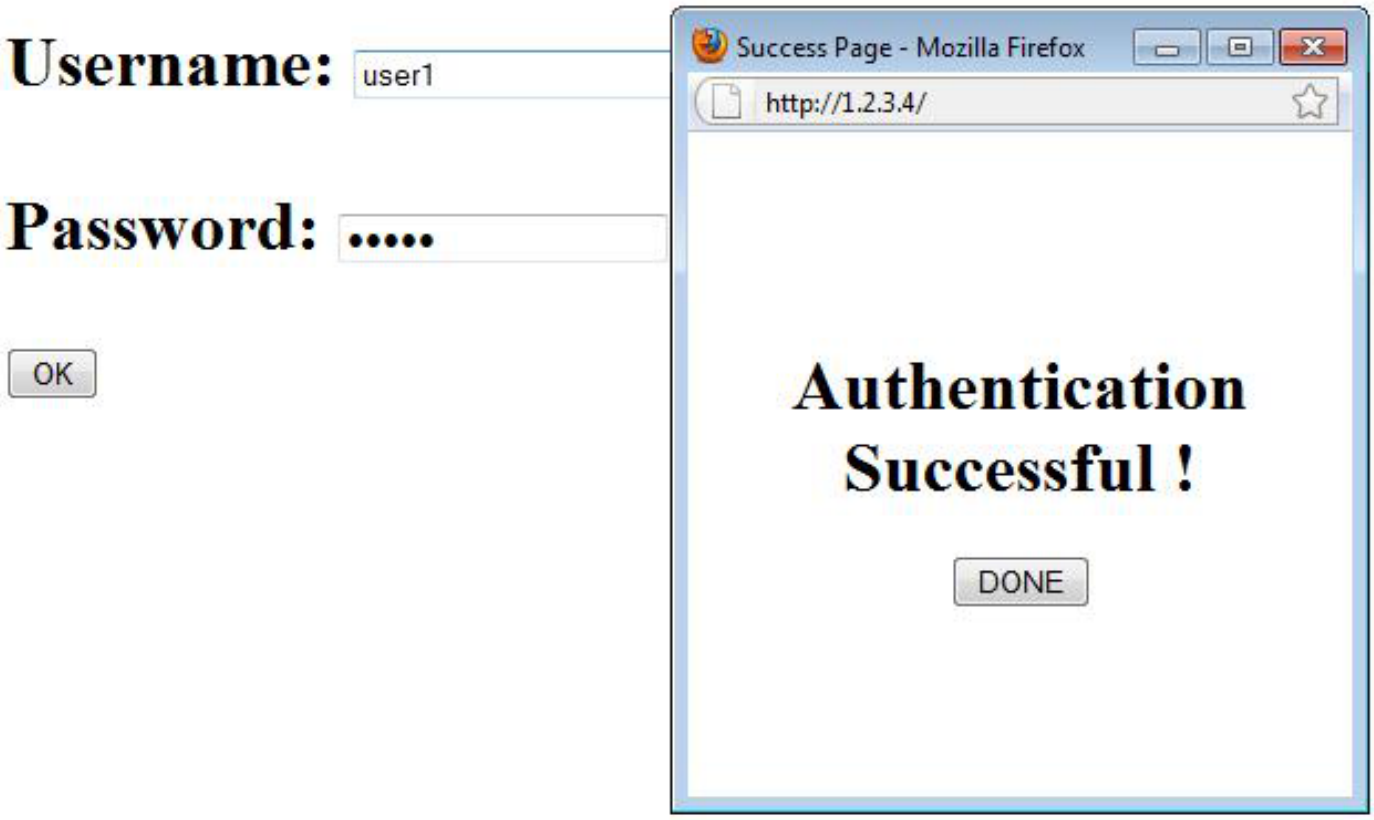
Password:

OK

> **Opmerking:** Deze test wordt voltooid met een rechtstreeks ingevoerde willekeurig IP-adres (de URL is **1.2.3.4**) zonder dat er een URL moet worden vertaald via de DNS, omdat de DNS-code niet in de test is gebruikt. In normale scenario's, gaat de gebruiker de homepage URL in, en het DNS verkeer wordt toegestaan tot de client het HTTP GET bericht naar het opgeloste adres verstuurt, dat door AP wordt onderschept. AP spaart het website adres, en richt de client naar de inlogpagina die intern opgeslagen is.

Nadat de client is omgeleid naar de logpagina, worden de gebruikersreferenties ingevoerd en geverifieerd via de lokale RADIUS-server, zoals beschreven in de AP-configuratie. Na succesvolle authenticatie wordt het verkeer dat van en naar de cliënt komt volledig toegestaan.

Dit is het bericht dat naar de gebruiker wordt verzonden na succesvolle authenticatie:



Na succesvolle authenticatie kunt u de client-IP-informatie bekijken:

```
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
```

Pings aan de cliënt na succesvolle authenticatie moet correct werken:

```
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
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

> **Opmerking:** Roaming tussen AP's tijdens web authenticatie geeft geen vlotte ervaring op, omdat de klanten moeten inloggen bij elke nieuwe AP waarmee ze verbonden zijn.

Aanpassing

Overeenkomstig met IOS op routers of switches kunt u uw pagina met een aangepast bestand aanpassen. het is echter niet mogelijk om een nieuwe webpagina op te zetten .

Gebruik deze opdrachten om de poortbestanden aan te passen:

- ip-toegangsproxy http-pagina-bestand
- ip-toegangsproxy http-pagina-bestand
- ip-toegangsproxy-bestand
- ip-toegangsproxy-bestand voor defectpagina