Esempio di configurazione del filtro ACL del punto di accesso

Sommario

Introduzione

Questo documento spiega come configurare i filtri basati su ACL (Access Control List) sui Cisco Aironet Access Point (AP) con l'uso dell'interfaccia della riga di comando (CLI).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Configurazione di una connessione wireless con l'uso di un access point Aironet e di un adattatore client Aironet 802.11 a/b/g
- ACL

Componenti usati

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

- Aironet serie 1200 AP con software Cisco IOS® versione 12.3(7)JA1

- Aironet 802.11a/b/g Client Adapter
- Software Aironet Desktop Utility (ADU) versione 2.5

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.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

È possibile utilizzare i filtri degli access point per eseguire le seguenti attività:

- Limitazione dell'accesso alla rete LAN wireless (WLAN)
- Fornire un livello aggiuntivo di sicurezza wireless

Èpossibile utilizzare diversi tipi di filtri per filtrare il traffico in base a:

- Protocolli specifici
- Indirizzo MAC del dispositivo client
- Indirizzo IP del dispositivo client

Èinoltre possibile abilitare i filtri per limitare il traffico proveniente dagli utenti sulla LAN cablata. I filtri degli indirizzi IP e MAC consentono o non consentono l'inoltro di pacchetti unicast e multicast inviati a o da indirizzi IP o MAC specifici.

I filtri basati sul protocollo forniscono un modo più granulare per limitare l'accesso a protocolli specifici tramite le interfacce Ethernet e radio dell'access point. Per configurare i filtri sugli access point, è possibile utilizzare uno dei seguenti metodi:

- GUI Web
- CLI

Questo documento spiega come usare gli ACL per configurare i filtri dalla CLI. Per informazioni su come configurare i filtri tramite la GUI, consultare il documento sulla configurazione dei filtri.

Èpossibile usare la CLI per configurare questi tipi di filtri basati sugli ACL nell'access point:

- Filtri che usano ACL standard
- Filtri che usano ACL estesi
- Filtri che usano ACL di indirizzi MAC

Nota: il numero di voci consentite in un ACL è limitato dalla CPU dell'access point. Se il numero di voci da aggiungere a un ACL è elevato, ad esempio quando si filtra un elenco di indirizzi MAC per i client, usare uno switch in rete in grado di eseguire l'operazione.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità

descritte più avanti nel documento.

per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

In tutte le configurazioni di questo documento si presume che sia già stata stabilita una connessione wireless. Questo documento è incentrato solo su come usare la CLI per configurare i filtri. Se non si dispone di una connessione wireless di base, vedere Esempio di configurazione di base della connessione LAN wireless.

Filtri che utilizzano elenchi degli accessi standard

Èpossibile usare gli ACL standard per consentire o impedire l'ingresso di dispositivi client nella rete WLAN in base all'indirizzo IP del client. Gli ACL standard confrontano l'indirizzo di origine dei pacchetti IP con gli indirizzi configurati negli elenchi stessi al fine di controllare il traffico. Questo tipo di ACL può essere chiamato ACL basato sull'indirizzo IP di origine.

Il formato della sintassi del comando di un ACL standard è **access-list** ***access-list-number*** **{allow | deny} {***indirizzo-ip***-host | *source-ip source-wildcard* | qualsiasi}**.

Nel software Cisco IOS® versione 12.3(7)JA, il numero ACL può essere un numero compreso tra 1 e 99. Gli ACL standard possono usare anche l'intervallo esteso tra 1300 e 1999. Gli ACL che usano questi numeri aggiuntivi sono ACL IP espansi.

Quando un ACL standard è configurato per negare l'accesso a un client, il client continua a essere associato all'access point. Tuttavia, non vi è alcuna comunicazione di dati tra l'access point e il client.

Nell'esempio viene mostrato un ACL standard configurato per filtrare l'indirizzo IP 10.0.0.2 del client dall'interfaccia wireless (interfaccia radio0). L'indirizzo IP dell'access point è 10.0.0.1.

Al termine, il client con indirizzo IP 10.0.0.2 non può inviare o ricevere dati tramite la rete WLAN anche se è associato al punto di accesso.

Completare questi passaggi per creare un ACL standard dalla CLI:

1. Accedere all'access point dalla CLI.Usare la porta console o usare Telnet per accedere all'ACL tramite l'interfaccia Ethernet o l'interfaccia wireless.
2. Accedere alla modalità di configurazione globale sull'access point:
   ```
   AP#configure terminal
   ```
3. Per creare l'ACL standard, usare questi comandi:
   ```
   AP<config>#access-list 25 deny host 10.0.0.2
   !--- Create a standard ACL 25 to deny access to the !--- client with IP address 10.0.0.2.
   AP<config>#access-list 25 permit any
   !--- Allow all other hosts to access the network.
   ```
4. Per applicare il presente ACL all'interfaccia radio, usare questi comandi:
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in
   !--- Apply the standard ACL to the radio interface 0.
   ```

Èpossibile anche creare un ACL standard con nome (NACL). Per definire l'ACL, l'NACL usa un nome anziché un numero.

```
AP#configure terminal
AP<config>#ip access-list standard name
AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

Per negare all'host 10.0.0.2 l'accesso alla rete WLAN, usare questi comandi per usare gli NACL standard:

```
AP#configure terminal
AP<config>#ip access-list standard TEST
!--- Create a standard NACL TEST.

AP<config-std-nacl>#deny host 10.0.0.2
!--- Disallow the client with IP address 10.0.0.2 !--- access to the network. AP<config-std-
nacl>#permit any
!--- Allow all other hosts to access the network. AP<config-std-nacl>#exit
!--- Exit to global configuration mode. AP<config>#interface Dot11Radio 0
!--- Enter dot11 radio0 interface mode. AP<config-if>#ip access-group TEST in
!--- Apply the standard NACL to the radio interface.
```

Filtri che utilizzano elenchi degli accessi estesi

Gli ACL estesi confrontano gli indirizzi di origine e di destinazione dei pacchetti IP con gli indirizzi configurati negli elenchi stessi al fine di controllare il traffico. Gli ACL estesi offrono anche un metodo per filtrare il traffico in base a protocolli specifici. Ciò fornisce un controllo più granulare per l'implementazione dei filtri su una rete WLAN.

Gli ACL estesi consentono a un client di accedere ad alcune risorse della rete, ma non alle altre risorse. Ad esempio, è possibile implementare un filtro che consenta il traffico DHCP e Telnet per il client mentre limita tutto il resto del traffico.

Di seguito viene mostrata la sintassi del comando degli ACL estesi:

Nota: per problemi di spazio, questo comando va a capo su quattro righe.

```
access-list access-list-number [dynamic dynamic-name [timeout minutes]] {deny | permit} protocol
source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [log |
log-input] [time-range time-range-name]
```

Nel software Cisco IOS versione 12.3(7)JA, gli ACL estesi possono usare numeri compresi tra 100 e 199. Gli ACL estesi possono usare anche numeri compresi tra 2000 e 2699. Questo è l'intervallo esteso degli ACL estesi.

Nota: la parola chiave **log** situata alla fine di una voce dell'elenco restituisce:

- Numero e nome ACL
- Se il pacchetto è stato autorizzato o rifiutato
- Informazioni specifiche sulla porta

Anche gli ACL estesi possono usare nomi anziché numeri. Questa è la sintassi per creare gli NACL estesi:

ip access-list extended *name* **{deny | permit}** *protocol source source-wildcard* **destination** *destination-wildcard* **[precedence** *precedence***] [tos** *tos***] [log | log-input] [time-range** *time-range-name***]**

In questo esempio di configurazione vengono usati NACL estesi. Il requisito è che l'ACL esteso consenta l'accesso Telnet ai client. è necessario limitare tutti gli altri protocolli sulla rete WLAN. Inoltre, i client usano DHCP per ottenere l'indirizzo IP. È necessario creare un ACL esteso che:

- Consente il traffico DHCP e Telnet
- Nega tutti gli altri tipi di traffico

Dopo aver applicato l'ACL esteso all'interfaccia radio, i client si associano all'access point e ricevono un indirizzo IP dal server DHCP. I client possono inoltre utilizzare Telnet. Tutti gli altri tipi di traffico sono rifiutati.

Completare questi passaggi per creare un ACL esteso sull'access point:

1. Accedere all'access point dalla CLI.Per accedere all'ACL tramite l'interfaccia Ethernet o l'interfaccia wireless, usare la porta console o Telnet.
2. Accedere alla modalità di configurazione globale sull'access point:
   ```
   AP#configure terminal
   ```
3. Per creare l'ACL esteso, usare questi comandi:
   ```
   AP<config>#ip access-list extended Allow_DHCP_Telnet
   !--- Create an extended ACL Allow_DHCP_Telnet.

   AP<config-extd-nacl>#permit tcp any any eq telnet
   !--- Allow Telnet traffic. AP<config-extd-nacl>#permit udp any any eq bootpc
   !--- Allow DHCP traffic. AP<config-extd-nacl>#permit udp any any eq bootps
   !--- Allow DHCP traffic. AP<config-extd-nacl>#deny ip any any
   !--- Deny all other traffic types. AP<config-extd-nacl>#exit
   !--- Return to global configuration mode.
   ```
4. Per applicare l'ACL all'interfaccia radio, usare questi comandi:
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group Allow_DHCP_Telnet in
   !--- Apply the extended ACL Allow_DHCP_Telnet !--- to the radio0 interface.
   ```

Filtri che usano ACL basati su MAC

È possibile utilizzare filtri basati sull'indirizzo MAC per filtrare i dispositivi client in base all'indirizzo MAC hardcoded. Quando a un client viene negato l'accesso tramite un filtro basato su MAC, il client non può associarsi all'access point. I filtri degli indirizzi MAC consentono o non consentono l'inoltro di pacchetti unicast e multicast inviati o indirizzati a indirizzi MAC specifici.

Questa è la sintassi del comando per creare un ACL basato su indirizzo MAC nell'access point:

Nota: per problemi di spazio, questo comando è stato disposto su due righe.

access-list *access-list-number* **{permit | deny}** *48-bit-hardware-address 48-bit-hardware-address-mask*

Nel software Cisco IOS versione 12.3(7)JA, gli ACL con indirizzi MAC possono usare numeri compresi tra 700 e 799 come numero ACL. Possono inoltre utilizzare numeri compresi tra 1100 e 1199.

L'esempio mostra come configurare un filtro basato su MAC dalla CLI per filtrare il client con un indirizzo MAC pari a **0040.96a5.b5d4**:

1. Accedere all'access point dalla CLI.Per accedere all'ACL tramite l'interfaccia Ethernet o l'interfaccia wireless, usare la porta console o Telnet.
2. Accedere alla modalità di configurazione globale nella CLI dell'access point:
   AP#**configure terminal**

3. Creare un ACL 700 per l'indirizzo MAC.Questo ACL non consente al client 0040.96a5.b5d4 di associarsi all'access point.

   ```
   access-list 700 deny 0040.96a5.b5d4 0000.0000.0000
   !--- This ACL denies all traffic to and from !--- the client with MAC address
   0040.96a5.b5d4.
   ```
4. Per applicare questo ACL basato sull'indirizzo MAC all'interfaccia radio, usare questo comando:

   ```
   dot11 association mac-list 700

   !--- Apply the MAC-based ACL.
   ```

Dopo aver configurato il filtro sull'access point, il client con questo indirizzo MAC, precedentemente associato all'access point, viene dissociato. La console AP invia questo messaggio:

```
AccessPoint# *Mar 1 01:42:36.743: %DOT11-6-DISASSOC: Interface
 Dot11Radio0, Deauthenticating Station 0040.96a5.b5d4
```

Filtri che usano ACL con limiti di tempo

Gli ACL con limiti di tempo sono ACL che possono essere abilitati o disabilitati per un periodo di tempo specifico. Questa funzionalità garantisce solidità e flessibilità nella definizione di policy di controllo dell'accesso che consentono o negano determinati tipi di traffico.

L'esempio mostra come configurare un ACL con limiti di tempo tramite la CLI, in cui la connessione Telnet viene autorizzata dalla rete interna verso l'esterno nei giorni feriali durante l'orario di lavoro:

Nota: un ACL con limiti di tempo può essere definito sulla porta Fast Ethernet o sulla porta Radio dell'Aironet AP, in base ai requisiti dell'utente. Non viene mai applicata all'interfaccia virtuale del gruppo di bridge (BVI).

1. Accedere all'access point dalla CLI.Per accedere all'ACL tramite l'interfaccia Ethernet o l'interfaccia wireless, usare la porta console o Telnet.
2. Accedere alla modalità di configurazione globale nella CLI dell'access point:
   AP#**configure terminal**

3. Creare un intervallo di tempo. A tale scopo, eseguire questo comando in modalità di configurazione globale:
   AP<config>#**time-range Test**

```
!--- Create a time-range with name Test. AP(config-time-range)# periodic weekdays 7:00 to
19:00
!--- Allows access to users during weekdays from 7:00 to 19:00 hrs.
```

4. Creare un ACL 101:

```
AP<config># ip access-list extended 101
AP<config-ext-nacl>#permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range
Test
!--- This ACL permits Telnet traffic to and from !--- the network for the specified time-
range Test.
```

   Questo ACL consente una sessione Telnet con l'access point nei giorni feriali.

5. Per applicare questo ACL con limiti di tempo all'interfaccia Ethernet, usare questo comando:

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in

!--- Apply the time-based ACL.
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

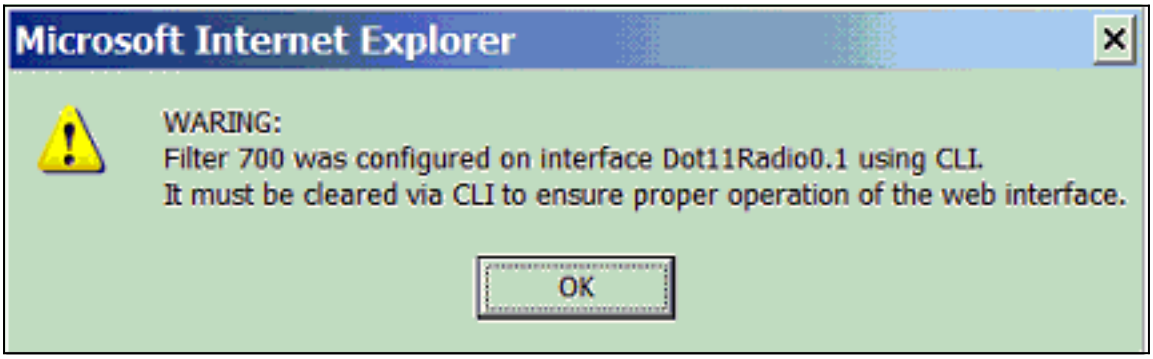
Per rimuovere un ACL da un'interfaccia, completare la procedura seguente:

1. Andare alla modalità di configurazione interfaccia.
2. Immettere **no** davanti al comando **ip access-group**, come mostrato nell'esempio:

```
interface interface
no ip access-group {access-list-name | access-list-number} {in | out}
```

Èinoltre possibile utilizzare il nome **show access-list | *number* per risolvere i problemi relativi alla configurazione.** Il comando **show ip access-list** restituisce un numero di pacchetto che mostra la voce ACL con cui è stata trovata una corrispondenza.

Evitare di usare sia la CLI che l'interfaccia del browser Web per configurare il dispositivo wireless. Se si configura il dispositivo wireless con la CLI, l'interfaccia del browser Web può visualizzare un'interpretazione errata della configurazione. Tuttavia, l'imprecisione non significa necessariamente che il dispositivo wireless non sia configurato correttamente. Ad esempio, se si configurano gli ACL con la CLI, l'interfaccia del browser Web può visualizzare questo messaggio:



Se viene visualizzato questo messaggio, usare la CLI per eliminare gli ACL e usare l'interfaccia del browser Web per riconfigurarli.

Informazioni correlate

- Configurazione dei filtri
- Pagina di supporto wireless
- Documentazione e supporto tecnico – Cisco Systems