Access Point ACL Filter Configuration Example

Document ID: 68097

Contents

Introduction

This document explains how to configure access control list (ACL)–based filters on Cisco Aironet Access Points (APs) with use of the command–line interface (CLI).

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- The configuration of a wireless connection with use of an Aironet AP and an Aironet 802.11 a/b/g Client Adapter
- ACLs

Components Used

The information in this document is based on these software and hardware versions:

- Aironet 1200 Series AP that runs Cisco IOS® Software Release 12.3(7)JA1
- Aironet 802.11a/b/g Client Adapter
- Aironet Desktop Utility (ADU) Software Release 2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

You can use filters on APs to perform these tasks:

- Restrict access to the wireless LAN (WLAN) network
- Provide an additional layer of wireless security

You can use different types of filters to filter traffic based on:

- Specific protocols
- MAC address of the client device
- IP address of the client device

You can also enable filters to restrict traffic from users on the wired LAN. IP address and MAC address filters allow or disallow the forwarding of unicast and multicast packets that are sent to or from specific IP or MAC addresses.

Protocol−based filters provide a more granular way to restrict access to specific protocols through the Ethernet and radio interfaces of the AP. You can use either of these methods to configure the filters on the APs:

- Web GUI
- CLI

This document explains how to use ACLs to configure filters through the CLI. For information on how to configure filters through the GUI, refer to Configuring Filters.

You can use the CLI to configure these types of ACL−based filters on the AP:

- Filters that use standard ACLs
- Filters that use extended ACLs
- Filters that use MAC address ACLs

Note: The number of allowed entries on an ACL is limited by the CPU of the AP. If there is a large number of entries to add to an ACL, for instance when filtering a list of MAC addresses for the clients, use a switch in the network that can perform the task.

Configure

In this section, you are presented with the information to configure the features described in this document.

Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

All the configurations in this document assume that a wireless connection is already established. This document focuses only on how to use the CLI in order to configure filters. If you do not have a basic wireless connection, refer to Basic Wireless LAN Connection Configuration Example.

Filters Using Standard Access Lists

You can use standard ACLs to allow or disallow the entry of client devices into the WLAN network based on the IP address of the client. Standard ACLs compare the source address of the IP packets to the addresses that are configured in the ACL in order to control traffic. This type of ACL can be referred to as a source IP

address−based ACL.

The command syntax format of a standard ACL is **access−list** *access−list−number* **{permit | deny} {host** *ip−address | source−ip source−wildcard |* **any}**.

In Cisco IOS® Software Release 12.3(7)JA, the ACL number can be any number from 1 to 99. Standard ACLs can also use the extended range of 1300 to 1999. These additional numbers are expanded IP ACLs.

When a standard ACL is configured to deny access to a client, the client still associates to the AP. However, there is no data communication between the AP and the client.

This example shows a standard ACL that is configured to filter the client IP address 10.0.0.2 from the wireless interface (radio0 interface). The IP address of the AP is 10.0.0.1.

After this is done, the client with IP address 10.0.0.2 cannot send or receive data through the WLAN network even though the client is associated to the AP.

Complete these steps in order to create a standard ACL through the CLI:

1. Log in to the AP through the CLI.

   Use the console port or use Telnet in order to access the ACL through the Ethernet interface or the wireless interface.
2. Enter global configuration mode on the AP:

   ```
   AP#configure terminal
   ```
3. Issue these commands in order to create the standard ACL:

   ```
   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. Issue these commands in order to apply this ACL to the radio interface:

   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in

   !--- Apply the standard ACL to the radio interface 0.
   ```

You can also create a standard named ACL (NACL). The NACL uses a name instead of a number to define the ACL.

```
AP#configure terminal
AP<config>#ip access-list standard name

AP<config>#permit | deny {host ip-address | source-ip [source-wildcard] | any} log
```

Issue these commands in order to use standard NACLs to deny the host 10.0.0.2 access to the WLAN network:

```
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.
```

Filters Using Extended Access Lists

Extended ACLs compare the source and destination addresses of the IP packets to the addresses that are configured in the ACL in order to control traffic. Extended ACLs also provide a means to filter traffic based on specific protocols. This provides a more granular control for the implementation of filters on a WLAN network.

Extended ACLs allow a client to access some resources on the network while the client cannot access the other resources. For example, you can implement a filter that allows DHCP and Telnet traffic to the client while it restricts all other traffic.

This is the command syntax of extended ACLs:

Note: This command is wrapped to four lines because of spatial considerations.

```
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]
```

In Cisco IOS Software Release 12.3(7)JA, extended ACLs can use numbers in the range of 100 to 199. Extended ACLs can also use numbers in the range of 2000 to 2699. This is the expanded range for extended ACLs.

Note: The **log** keyword at the end of the individual ACL entries shows:

- ACL number and name
- Whether the packet was permitted or denied
- Port−specific information

Extended ACLs can also use names instead of numbers. This is the syntax to create extended NACLs:

```
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]
```

This configuration example uses extended NACLs. The requirement is that the extended NACL must allow Telnet access to the clients. You must restrict all other protocols on the WLAN network. Also, the clients use DHCP in order to get the IP address. You must create an extended ACL that:

- Allows DHCP and Telnet traffic
- Denies all other traffic types

Once this extended ACL is applied to the radio interface, the clients associate with the AP and get an IP address from the DHCP server. The clients are also able to use Telnet. All other traffic types are denied.

Complete these steps in order to create an extended ACL on the AP:

1. Log in to the AP through the CLI.

   Use the console port or Telnet in order to access the ACL through the Ethernet interface or the wireless interface.
2. Enter global configuration mode on the AP:

   ```
   AP#configure terminal
   ```
3. Issue these commands in order to create the extended ACL:

   ```
   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. Issue these commands in order to apply the ACL to the radio interface:

   ```
   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.
   ```

Filters Using MAC–Based ACLs

You can use MAC address–based filters in order to filter client devices based on the hard coded MAC address. When a client is denied access through a MAC–based filter, the client cannot associate with the AP.

MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses.

This is the command syntax to create a MAC address–based ACL on the AP:

Note: This command has been wrapped to two lines because of spatial considerations.

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

In Cisco IOS Software Release 12.3(7)JA, MAC address ACLs can use numbers in the range of 700 to 799 as the ACL number. They can also use numbers in the expanded range of 1100 to 1199.

This example illustrates how to configure a MAC–based filter through the CLI, in order to filter the client with a MAC address of **0040.96a5.b5d4**:

1. Log in to the AP through the CLI.

   Use the console port or Telnet in order to access the ACL through the Ethernet interface or the wireless interface.
2. Enter global configuration mode on the AP CLI:

   ```
   AP#configure terminal
   ```
3. Create a MAC address ACL 700.

   This ACL does not allow the client 0040.96a5.b5d4 to associate with the AP.

   ```
   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. Issue this command in order to apply this MAC–based ACL to the radio interface:

   ```
   dot11 association mac-list 700


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

After you configure this filter on the AP, the client with this MAC address, which was previously associated to the AP, is disassociated. The AP console sends this message:

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

Filters Using Time–Based ACLs

Time–based ACLs are ACLs that can be enabled or disabled for a specific period of time. This capability provides robustness and the flexibility to define access control policies that either permit or deny certain kinds of traffic.

This example illustrates how to configure a time–based ACL through the CLI, where Telnet connection is permitted from the inside to the outside network on weekdays during business hours:

Note: A time−based ACL can be defined either on the Fast Ethernet port or on the Radio port of the Aironet AP, based on your requirements. It is never applied on the Bridge Group Virtual Interface (BVI).

1. Log in to the AP through the CLI.

   Use the console port or Telnet in order to access the ACL through the Ethernet interface or the wireless interface.
2. Enter global configuration mode on the AP CLI:

   ```
   AP#configure terminal
   ```
3. Create a Time Range. To do this, issue this command in global configuration mode:

   ```
   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. Create an 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 tim

   !--- This ACL permits Telnet traffic to and from
   !--- the network for the specified time-range Test.
   ```

   This ACL permits a Telnet session to the AP on weekdays.
5. Issue this command in order to apply this time−based ACL to the Ethernet interface:

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

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

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Use this section to troubleshoot your configuration.

Complete these steps in order to remove an ACL from an interface:

1. Go into interface configuration mode.
2. Enter **no** in front of the **ip access−group** command, as this example shows:

   ```
   interface interface

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

You can also use the **show access−list** *name | number* command in order to troubleshoot your configuration. The **show ip access−list** command provides a packet count that shows which ACL entry is being hit.

Avoid the use of both the CLI and the web−browser interfaces to configure the wireless device. If you configure the wireless device with the CLI, the web−browser interface can display an inaccurate interpretation of the configuration. However, the inaccuracy does not necessarily mean that the wireless device is misconfigured. For example, if you configure ACLs with the CLI, the web−browser interface can display this message:
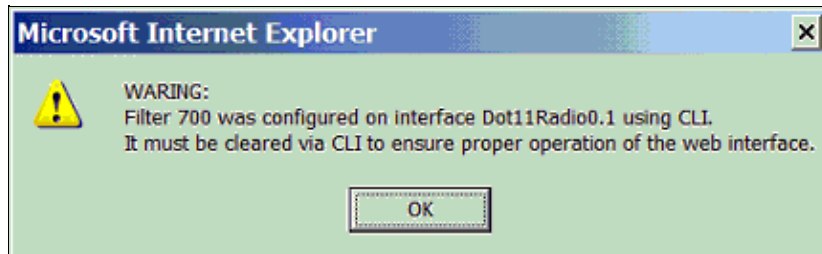
If you see this message, use the CLI in order to delete the ACLs and use the web−browser interface to reconfigure them.

Related Information

- **Configuring Filters**
- **Wireless Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jul 17, 2006   Document ID: 68097