接入点ACL过滤器配置示例

Contents

Introduction

本文说明如何使用命令行界面 (CLI) 在 Cisco Aironet 接入点 (AP) 上配置基于访问控制表 (ACL) 的过滤器。

Prerequisites

Requirements

Cisco建议您有这些题目基础知识：

- 无线连接的配置与使用的Aironet AP和Aironet 802.11 a/b/g客户端适配器
- ACL

Components Used

本文档中的信息基于以下软件和硬件版本：

- Aironet 1200运行Cisco IOS软件版本12.3(7)JA1的系列AP
- Aironet 802.11a/b/g 客户端适配器
- Aironet Desktop软件(ADU)软件版本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.

背景信息

您能使用在APs的过滤器执行这些任务：

- 限制对无线局域网(WLAN)网络的访问
- 提供无线安全一个另外的层

您能使用不同种类的过滤器到基于的过滤流量：

- 特定协议
- 客户端设备的MAC地址
- 客户端设备的IP地址

您能也限制数据流的enable (event)过滤器从有线LAN的用户。被发送到/从特定IP或MAC地址的IP地址和MAC地址过滤器允许或禁止单播和组播信息包转发。

基于协议的过滤器提供一个更加粒状的方式通过AP的以太网和无线接口限制对特定协议的访问。您能使用这些方法之一配置在APs的过滤器：

- Web GUI
- CLI

本文解释如何使用ACL通过CLI配置过滤器。关于如何通过GUI配置过滤器的信息，请参见配置过滤器。

您能使用CLI配置基于ACL的过滤器的这些类型在AP的：

- 使用标准ACL的过滤器
- 使用扩展ACL的过滤器
- 使用MAC地址ACL的过滤器

Note: 允许的条目的数量在ACL的由AP的CPU限制。如果有添加的很大数量的条目到ACL，例如，当过滤客户端的时MAC地址列表，请使用一台交换机在可执行任务的网络。

Configure

本部分提供有关如何配置本文档所述功能的信息。

有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

在本文的所有配置假设，无线连接已经被建立。本文仅着重如何使用CLI为了配置过滤器。如果没有基本的无线连接，请参见基本的无线局域网连接配置示例。

过滤器使用标准访问列表

您能使用标准ACL允许或禁止客户端设备条目到根据客户端的IP地址的WLAN网络。标准ACL与在

ACL为了控制数据流被配置的地址比较IP信息包的源地址。此种ACL可以指来源基于IP地址的ACL。

标准ACL的命令语法格式是**访问列表***access-list-number* **{许可证|拒绝} {主机***IP地址*|*来源IP source-wildcard*|**其中任一}**。

在Cisco IOS软件版本12.3(7)JA中， ACL编号可以是任何编码从1到99。标准ACL能也使用1300到1999年的扩充域。这些附加的编号是扩充IP ACL。

当配置标准ACL拒绝对客户端时的访问，客户端仍然联合对AP。然而，没有数据通信的在AP和客户端之间。

配置过滤从无线接口的此示例显示一标准ACL (radio0接口)的客户端IP地址10.0.0.2。AP的IP地址是10.0.0.1。

在这执行后，有IP地址10.0.0.2的客户端不能通过WLAN网络发送或接受数据，即使客户端被关联对AP。

完成这些步骤为了通过CLI创建标准ACL ：

1. 登陆对AP通过CLI。请使用控制台端口或请使用Telnet为了通过以太网接口或无线接口访问ACL。
2. 输入在AP的全局配置模式：
   ```
   AP#configure terminal
   ```
3. 发出这些命令为了创建标准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. 发出这些命令为了适用此ACL于无线接口：
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in
   !--- Apply the standard ACL to the radio interface 0.
   ```

您能也创建名为ACL的标准(NACL)。NACL使用一个名字而不是编号定义ACL。

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

发出这些命令为了使用标准的NACLs拒绝对WLAN网络的主机10.0.0.2访问：

```
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.
```

过滤器使用延长的访问列表

扩展ACL与在ACL为了控制数据流被配置的地址比较IP信息包的源地址和目的地址。扩展ACL也提供方法给根据特定协议的过滤流量。这为过滤器的实施提供一个更加粒状的控制在WLAN网络。

而客户端不能访问其他资源，扩展ACL允许客户端访问在网络的一些资源。例如，您能实现允许DHCP和Telnet数据流给客户端的过滤器，当限制其他数据流时。

这是扩展ACL命令句法：

Note: 此命令包裹对四条线路由于空间的考虑。

```
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]
```

在Cisco IOS Software Release 12.3(7)JA，扩展ACL能使用编号在100到199范围内。扩展ACL能也使用编号在2000年到2699范围内。这是扩展ACL的扩展范围。

Note: 日志关键字在各自的ACL条目结束时显示：

- ACL编号和名字
- 信息包是否允许或被丢弃了
- 端口特定的信息

扩展ACL能也使用名字而不是编号。这是创建延长的NACLs的语法：

```
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]
```

此配置示例使用延长的NACLs。需求是延长的NACL必须允许对客户端的Telnet访问。您必须限制关于WLAN网络的其他协议。并且，客户端使用DHCP为了获得IP地址。您必须创建扩展ACL那：

- 允许DHCP和Telnet数据流
- 拒绝其他话务类型

一旦此扩展ACL适用于无线接口，客户端与AP产生关联并且从DHCP服务器获得IP地址。客户端也能使用Telnet。其他话务类型被拒绝。

完成这些步骤为了创建在AP的扩展ACL ：

1. 登陆对AP通过CLI。请使用控制台端口或远程登录为了通过以太网接口或无线接口访问ACL。
2. 输入在AP的全局配置模式：
   ```
   AP#configure terminal
   ```
3. 发出这些命令为了创建扩展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. 发出这些命令为了适用ACL于无线接口：

```
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.
```

过滤器使用基于MAC的ACL

您能使用MAC基于地址的过滤器为了过滤根据硬编码MAC地址的客户端设备。当客户端是拒绝访问通过一台基于MAC的过滤器时，客户端不能与AP产生关联。MAC地址过滤器允许或禁止单播和组播信息包转发发送从或被寄到特定MAC地址。

这是创建在AP的MAC基于地址的ACL的命令句法：

Note: 此命令包裹对两条线路由于空间的考虑。

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

在Cisco IOS Software Release 12.3(7)JA， MAC地址ACL能使用编号在700到799范围内作为ACL编号。他们在扩展范围能也使用编号1100到1199。

此示例说明如何通过CLI配置一台基于MAC的过滤器，为了过滤有**0040.96a5.b5d4** MAC地址的客户端：

1. AP的洛金通过CLI。请使用控制台端口或远程登录为了通过以太网接口或无线接口访问ACL。
2. 输入在AP CLI的全局配置模式：

```
AP#configure terminal
```

3. 创建MAC地址ACL 700。此ACL不允许客户端0040.96a5.b5d4与AP产生关联。

```
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. 发出此命令为了适用此基于MAC的ACL于无线接口：

```
dot11 association mac-list 700

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

在您配置在AP后的此过滤器，有此MAC地址的客户端，以前被关联对AP，被分离。AP控制台传送此信息：

```
dot11 association mac-list 700

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

过滤器使用基于时间的ACL

基于时间的ACL是可以是启用或禁用的在一段特定时期的ACL。此功能提供抗错性和灵活性定义请允许或拒绝某些种类数据流的访问控制策略。

此示例说明如何通过CLI配置基于时间的ACL，在工作时间， Telnet连接从里面允许到工作日的外部网络：

Note: 基于时间的ACL可以被定义在快速以太网端口或在Aironet AP的无线端口，根据您的需求。它在网桥组虚拟接口(BVI)从未适用。

1. AP的洛金通过CLI。请使用控制台端口或远程登录为了通过以太网接口或无线接口访问ACL。
2. 输入在AP CLI的全局配置模式：
   ```
   AP#configure terminal
   ```
3. 创建时间范围。要执行此，请发出此in命令全局配置模式：
   ```
   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. 创建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.
   ```
   此ACL允许远程登录会话对工作日的AP。
5. 发出此命令为了适用此基于时间的ACL于以太网接口：

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

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

Verify

当前没有可用于此配置的验证过程。

Troubleshoot

使用本部分可排除配置故障。

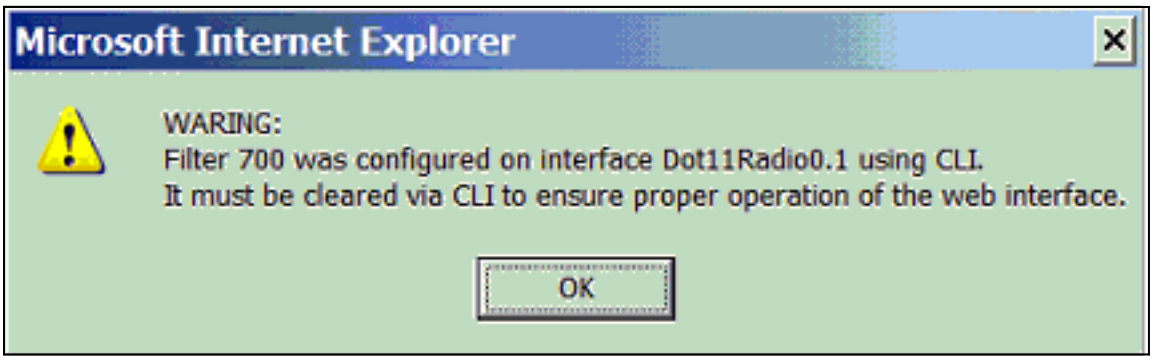
完成这些步骤为了从接口去除ACL ：

1. 进入Interface Configuration模式。
2. 进入**不在ip access-group命令前面**，此示例显示：

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

您能也使用**show access-list*名字*|*number*命令**为了排除您的配置故障。**show ip access-list命令**提供显示的信息包计数哪ACL条目被击中。

避免使用CLI和Web浏览器接口配置无线设备。如果用CLI配置无线设备， Web浏览器接口能显示配置的一个不正确的解释。然而，不精确性不一定意味着无线设备是不正确的配置的。例如，如果用CLI配置ACL， Web浏览器接口能显示此消息：



如果看到此消息，请使用CLI为了删除ACL和使用Web浏览器接口重新配置他们。

Related Information

- 配置过滤器
- 无线支持页
- Technical Support & Documentation - Cisco Systems