接入點ACL過濾器配置示例

目錄

簡介

本檔案將說明如何使用指令行介面(CLI)在Cisco Aironet存取點(AP)上設定存取控制清單(ACL)型過濾器。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- 使用Aironet AP和Aironet 802.11 a/b/g客戶端介面卡配置無線連線
- ACL

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行Cisco IOS®軟體版本12.3(7)JA1的Aironet 1200系列AP
- Aironet 802.11a/b/g使用者端配接器
- Aironet案頭公用程式(ADU)軟體版本2.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

您可以在AP上使用過濾器執行以下任務：

- 限制對無線LAN(WLAN)網路的訪問
- 提供額外的無線安全層

您可以使用不同型別的過濾器根據以下條件過濾流量：

- 特定協定
- 客戶端裝置的MAC地址
- 客戶端裝置的IP地址

您還可以啟用過濾器以限制來自有線LAN上使用者的流量。IP地址和MAC地址過濾器允許或不允許轉發傳送到特定IP或MAC地址的單播和組播資料包。

基於協定的過濾器提供了一種更精細的方式，以限制通過AP的乙太網和無線電介面訪問特定協定。您可以使用以下任一方法在AP上配置過濾器：

- Web GUI
- CLI

本檔案將說明如何使用ACL透過CLI設定過濾器。有關如何通過GUI配置過濾器的資訊，請參閱配置過濾器。

您可以使用CLI在AP上配置以下型別的基於ACL的過濾器：

- 使用標準型ACL的過濾器
- 使用延伸型ACL的過濾器
- 使用MAC位址ACL的過濾器

注意：ACL上允許的條目數受AP的CPU的限制。如果要向ACL新增大量條目（例如過濾客戶端的MAC地址清單時），請使用網路中可以執行該任務的交換機。

設定

本節提供用於設定本文件中所述功能的資訊。

使用命令查詢工具(僅供已註冊客戶使用)可查詢有關本文檔中所用命令的更多資訊。

本文檔中的所有配置均假定已建立無線連線。本文僅著重說明如何使用CLI設定過濾器。如果您沒有基本無線連線，請參閱基本無線LAN連線組態範例。

使用標準存取清單的篩選條件

您可以使用標準ACL來允許或禁止客戶端裝置根據客戶端的IP地址進入WLAN網路。標準型ACL會將IP封包的來源位址與ACL中設定的位址進行比較，以便控制流量。此型別的ACL可稱為來源IP位址型ACL。

標準型 ACL 的命令語法格式為 **access-list access-list-number {permit | deny} {host *ip-address* | *source-ip source-wildcard* | any}**。

在Cisco IOS®軟體版本12.3(7)JA中，ACL編號可以是1到99之間的任何數字。標準型ACL也可以使用從1300到1999的擴展範圍。這些額外的數字是延伸型IP ACL。

當標準ACL配置為拒絕對客戶端的訪問時，客戶端仍然會與AP關聯。但是，AP和客戶端之間沒有資料通訊。

此範例顯示已設定為從無線介面（radio0介面）過濾使用者端IP位址10.0.0.2的標準ACL。 AP的IP地址為10.0.0.1。

完成此操作後，IP地址為10.0.0.2的客戶端無法通過WLAN網路傳送或接收資料，即使該客戶端與AP相關聯。

完成以下步驟，以便透過CLI建立標準型ACL:

1. 通過CLI登入到AP。使用主控台連線埠或使用Telnet以透過乙太網路介面或無線介面存取ACL。
2. 進入AP上的全域性配置模式：
   ```
   AP#configure terminal
   ```
3. 核發以下命令，以便建立標準型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. 發出以下命令，將此ACL套用至無線電介面：
   ```
   AP<config>#interface Dot11Radio 0
   AP<config-if>#ip access-group 25 in
   !--- Apply the standard ACL to the radio interface 0.
   ```

您還可以建立標準命名型ACL(NACL)。 NACL使用名稱而不是數字來定義ACL。

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

發出以下命令，以便使用標準NACL拒絕主機10.0.0.2訪問WLAN網路：

```
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.
```

使用延伸存取清單的篩選條件

延伸型ACL會將IP封包的來源和目的地位址與ACL中設定的位址進行比較，以便控制流量。延伸型

ACL也提供了一種根據特定通訊協定過濾流量的方法。這樣可為WLAN網路上的過濾器實作提供更精細的控制。

延伸型ACL允許使用者端存取網路上的某些資源，但使用者端無法存取其他資源。例如，您可以實施一個過濾器，允許DHCP和Telnet流量流向客戶端，同時限制所有其他流量。

以下是延伸型ACL的命令語法：

注意：出於空間考慮，此命令將換行到四行。

```
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軟體版本12.3(7)JA中，延伸型ACL可以使用100到199之間的數字。延伸型ACL也可以使用2000到2699之間的數字。這是延伸型ACL的延伸範圍。

注意：個別ACL專案結尾的**log關鍵字顯示**：

- ACL編號和名稱
- 允許還是拒絕封包
- 埠特定資訊

延伸型ACL也可以使用名稱而非數字。以下是建立延伸型NACL的語法：

```
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]
```

此組態範例使用延伸型NACL。要求是擴展NACL必須允許Telnet訪問客戶端。您必須限制WLAN網路上所有其他的協定。此外，客戶端使用DHCP來獲取IP地址。您必須建立一個具有以下特徵的擴展ACL:

- 允許DHCP和Telnet流量
- 拒絕所有其他流量型別

將此擴展ACL應用於無線電介面後，客戶端將與AP關聯並從DHCP伺服器獲取IP地址。客戶端也可以使用Telnet。拒絕所有其他流量型別。

完成以下步驟，以便在AP上建立延伸型ACL:

1. 通過CLI登入到AP。使用主控台連線埠或Telnet，透過乙太網路介面或無線介面存取ACL。
2. 進入AP上的全域性配置模式：
   ```
   AP#configure terminal
   ```
3. 核發以下命令，以便建立延伸型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. 發出以下命令，以便將ACL套用至無線電介面：

```
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.
```

使用基於MAC的ACL的過濾器

您可以使用基於MAC地址的過濾器來根據硬編碼MAC地址過濾客戶端裝置。當客戶端被拒絕通過基於MAC的過濾器訪問時，客戶端無法與AP關聯。MAC地址過濾器允許或不允許轉發從特定MAC地址傳送或發往特定MAC地址的單播和組播資料包。

以下是在AP上建立基於MAC地址的ACL的命令語法：

注意：出於空間方面的考慮，此命令已包裝為兩行。

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

在Cisco IOS軟體版本12.3(7)JA中，MAC位址ACL可以使用700到799範圍內的編號作為ACL編號。它們還可以使用從1100到1199的擴展範圍中的數字。

此範例說明如何透過CLI設定基於MAC的過濾器，以便使用MAC位址**0040.96a5.b5d4過濾使用者端**：

1. 通過CLI登入到AP。使用主控台連線埠或Telnet，透過乙太網路介面或無線介面存取ACL。
2. 在AP CLI上進入全域性配置模式：

```
AP#configure terminal
```

3. 建立MAC地址ACL 700。此ACL不允許客戶端0040.96a5.b5d4與AP關聯。

```
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. 發出此命令，以將此基於MAC的ACL應用於無線電介面：

```
dot11 association mac-list 700

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

在AP上配置此過濾器後，具有此MAC地址的客戶端（以前與AP相關聯）將取消關聯。AP控制檯傳送以下消息：

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

使用時間型ACL的過濾器

時間型ACL是可以在特定期間啟用或停用的ACL。此功能提供了健壯性和靈活性，可定義允許或拒絕特定型別流量的訪問控制策略。

以下範例說明如何透過CLI設定時間型ACL，在工作日的外部網路中允許Telnet連線：

注意：基於時間的ACL可以根據需要在Aironet AP的快速乙太網埠或無線埠上定義。它從未應用於橋接組虛擬介面(BVI)。

1. 通過CLI登入到AP。使用主控台連線埠或Telnet，透過乙太網路介面或無線介面存取ACL。
2. 在AP CLI上進入全域性配置模式：
   ```
   AP#configure terminal
   ```
3. 建立時間範圍。為此，請在全域性配置模式下發出以下命令：
   ```
   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. 建立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允許在工作日與AP進行Telnet會話。
5. 發出此命令，以將此時間型ACL套用到乙太網路介面：

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

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

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

使用本節內容，對組態進行疑難排解。

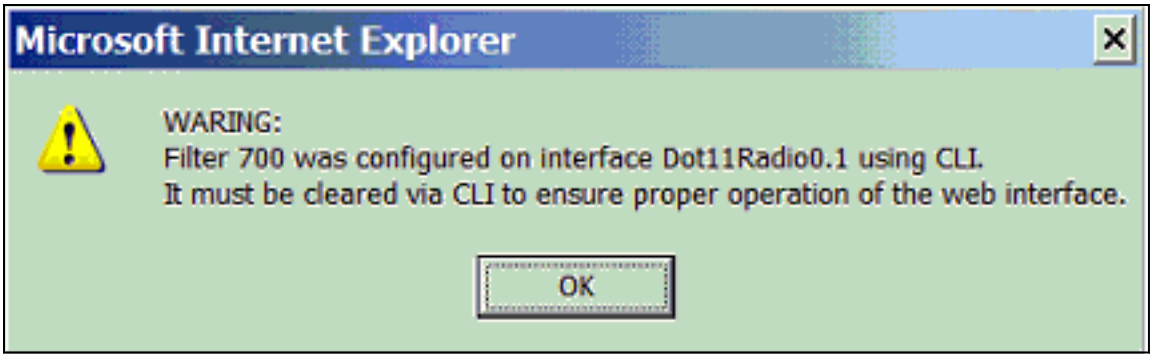
完成以下步驟即可從介面中移除ACL:

1. 進入介面配置模式。
2. 在**ip access-group**命令前輸入**no**，如以下示例所示：

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

您還可以使用**show access-list**名稱 | *number*命令以排解組態疑難問題。**show ip access-list**命令會提供一個封包數量，顯示所命中的ACL專案。

避免使用CLI和Web瀏覽器介面來配置無線裝置。如果使用CLI配置無線裝置，Web瀏覽器介面可能會顯示對配置的不準確解釋。但是，不準確並不意味著無線裝置配置錯誤。例如，如果使用CLI配置ACL，Web瀏覽器介面可以顯示以下消息：



如果您看到以下訊息，請使用CLI刪除ACL，然後使用Web瀏覽器介面重新配置它們。

相關資訊

- 配置過濾器
- 無線支援頁面
- 技術支援與文件 - Cisco Systems