WLC上的ACL — 規則、限制和範例

目錄

簡介

本檔案將提供無線LAN控制器(WLC)上的存取控制清單(ACL)的相關資訊。本檔案將說明目前的限制和規則，並提供相關範例。不應將本文作為對無線LAN控制器組態範例ACL的替代，而是為了提供補充資訊。

注意：對於第2層ACL或第3層ACL規則中的其他靈活性，思科建議您在連線到控制器的第一跳路由器上配置ACL。

最常見的錯誤發生在ACL行中的協定欄位設定為IP(protocol=4)，目的是允許或拒絕IP資料包。由於此欄位實際上會選擇封裝在IP封包中的內容，例如TCP、使用者資料包通訊協定(UDP)和網際網路控制訊息通訊協定(ICMP)，因此會轉換為封鎖或允許IP內IP封包。除非您想要封鎖行動IP封包，否則不得在任何ACL行中選取IP。思科錯誤ID CSCsh2975(僅供註冊客戶使用)將IP變更為IP內IP。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解如何設定WLC和輕量型存取點(LAP)以達成基本操作
- 輕量型存取點通訊協定(LWAPP)和無線安全方法的基礎知識

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

瞭解WLC上的ACL

ACL由一條或多條ACL行組成，在ACL末尾隨一個隱含的「deny any any」。每行具有以下欄位：

- 序列號
- 方向
- 源IP地址和掩碼
- 目標IP地址和掩碼
- 通訊協定
- Src埠
- 目標埠
- DSCP
- 動作

本檔案將說明以下每個欄位：

- **Sequence Number** — 指示ACL行針對資料包的處理順序。封包會根據ACL處理，直到它與第一個ACL行相符。此功能也允許您在ACL中的任何位置插入ACL行，即使在建立ACL之後也是如此。例如，如果您的ACL行的序列號為1，則可以通過在新的ACL行中輸入序列號1來插入新的ACL行。這會自動將ACL中的當前行下移。
- **Direction** — 告知控制器要強制執行ACL行的方向。有三個方向：傳入、傳出和任意。這些方向是從相對於WLC的位置而不是從無線使用者端取得的。傳入 — 檢查來自無線客戶端的IP資料包是否與ACL線路匹配。傳出 — 檢查目的地為無線使用者端的IP封包是否與ACL線路相符。Any — 檢查來自無線客戶端且目的地為無線客戶端的IP資料包，看它們是否與ACL線路匹配。ACL行同時應用於入站和出站方向。**注意：**為方向選擇Any時，應該使用的唯一地址和掩碼是0.0.0.0/0.0.0.0(Any)。不能使用「任意」方向指定特定主機或子網，因為需要換行以交換地址或子網以允許返回流量。Any方向只應在以下特定情況下使用：要在兩個方向上阻止或允許特定IP協定或埠、前往無線客戶端（出站）和來自無線客戶端（入站）。指定IP地址或子網時，必須將方向指定為「入站」或「出站」，並為相反方向的返回流量建立第二個新ACL行。如果將ACL套用到介面，且並不特別允許傳回流量，則傳回流量會被ACL清單結尾的隱含「deny any any」拒絕。
- **源IP地址和掩碼** — 定義從單個主機到多個子網的源IP地址，具體取決於掩碼。遮罩會與IP位址結合使用，以決定當將IP位址與封包中的IP位址進行比較時，應該略過IP位址中的哪些位元。**注意：**WLC ACL中的遮罩與Cisco IOS® ACL中使用的萬用字元或反向遮罩不同。在控制器ACL中，255表示完全符合IP位址中的八位元，而0表示萬用字元。地址和掩碼逐位組合。掩碼位1表示檢查相應的位值。遮罩中的規範255表示檢查的封包IP位址中的八位元必須與ACL位址中的對應八位元完全相符。遮罩位0表示不檢查（忽略）對應位值。遮罩中的指定0表示忽略了檢查的封包IP位址中的八位元組。0.0.0.0/0.0.0.0相當於「任意」IP地址（0.0.0.0作為地址，0.0.0.0作為掩碼）。
- **目標IP地址和掩碼** — 遵循與源IP地址和掩碼相同的掩碼規則。
- **Protocol** — 指定IP資料包報頭中的協定欄位。為方便客戶起見，某些協定編號在下拉選單中進行了轉換。不同值包括：任意（所有協定號均匹配）TCP（IP協定6）UDP（IP協定

17）ICMP（IP協定1）ESP（IP協定50）AH（IP協定51）GRE（IP協定47）IP(IP協定4 IP-in-IP [CSCsh22975])Eth Over IP（IP協定97）OSPF（IP協定89）其他（請具體說明）Any值匹配資料包的IP報頭中的任何協定。這用於完全阻止或允許特定子網的IP資料包。選擇IP以匹配IP-in-IP資料包。常用的選擇是UDP和TCP，它們用於設定特定的源埠和目的埠。如果選擇Other，則可以指定IANA 定義的任何IP資料包協定編號。
- **Src Port** — 只能為TCP和UDP協定指定。0-65535等效於任何埠。
- **Dest Port** — 只能為TCP和UDP協定指定。0-65535等效於任何埠。
- **區別服務代碼點(DSCP)** — 允許您指定特定的DSCP值以在IP資料包報頭中匹配。下拉選單中的選項是特定或Any。如果配置特定值，則在DSCP欄位中指定該值。例如，可以使用0到63之間的值。
- **Action** — 這2個操作為deny或permit。Deny阻止指定的資料包。Permit轉發資料包。

ACL規則和限制

基於WLC的ACL的限制

以下是基於WLC的ACL的限制：

- 您看不到封包與哪個ACL行相符(請參閱思科錯誤ID CSCse36574(僅限註冊客戶)。
- 無法記錄與特定ACL行相符的封包(請參閱思科錯誤ID CSCse36574(僅限註冊客戶))。
- IP資料包（乙太網協定欄位等於IP [0x0800]的任何資料包）是ACL檢查的唯一資料包。ACL無法阻止其他型別的乙太網資料包。例如，ACL無法阻止或允許ARP資料包（乙太網協定0x0806）。
- 一個控制器最多可以配置64個ACL；每個ACL最多可以配置64行。
- ACL不會影響從存取點(AP)和無線使用者端轉送或轉送到這些存取點的多點傳送和廣播流量(請參閱思科錯誤ID CSCse65613(僅限註冊客戶))。
- 在WLC 4.0版之前，ACL會在管理介面上繞過，因此您無法影響目的地為管理介面的流量。在WLC 4.0版之後，您可以建立CPU ACL。有關如何配置此型別ACL的詳細資訊，請參閱配置CPU ACL。**注意：**應用於管理介面和AP管理器介面的ACL將被忽略。WLC上的ACL旨在封鎖無線和有線網路之間的流量，而不是有線網路和WLC之間的流量。因此，如果要防止特定子網中的AP完全與WLC通訊，則需要在間歇性交換機或路由器上應用訪問清單。這將阻止從這些AP(VLAN)到WLC的LWAPP流量。
- ACL與處理器相關，可能會影響控制器在重負載下的效能。
- ACL無法阻止對虛擬IP地址(1.1.1.1)的訪問。因此，無法阻止無線客戶端的DHCP。
- ACL不會影響WLC的服務連線埠。

基於WLC的ACL的規則

以下是適用於基於WLC的ACL的規則：

- 您只能在ACL行的IP報頭（UDP、TCP、ICMP等）中指定協定號，因為ACL僅限於IP資料包。如果選擇IP，則表示您要允許或拒絕IP內IP資料包。如果選擇Any，則表明您要允許或拒絕具有任何IP協定的資料包。
- 如果為方向選擇Any，則源和目標應為Any(0.0.0.0/0.0.0.0)。
- 如果源IP地址或目標IP地址不是Any，則必須指定過濾器的方向。此外，必須為返回流量建立相反方向的反向語句（交換源IP地址/埠和目標IP地址/埠）。
- ACL的結尾有隱含的「deny any any」。如果封包與ACL中的任何行都不相符，就會被控制器

捨棄。

組態

使用DHCP、PING、HTTP和DNS的ACL示例

在此組態範例中，使用者端只能執行以下操作：

- 接收DHCP地址（ACL無法阻止DHCP）
- Ping並被ping（任何ICMP訊息型別 — 不能限製為僅ping）
- 建立HTTP連線（出站）
- 網域名稱系統(DNS)解析（傳出）

為了設定這些安全要求，ACL必須允許以下行：

- 任一方向的任何ICMP訊息（不能限製為僅ping）
- 任何到DNS入站的UDP埠
- DNS到任何UDP埠出站（返回流量）
- 任何到HTTP入站的TCP埠
- HTTP到任何TCP埠出站（返回流量）

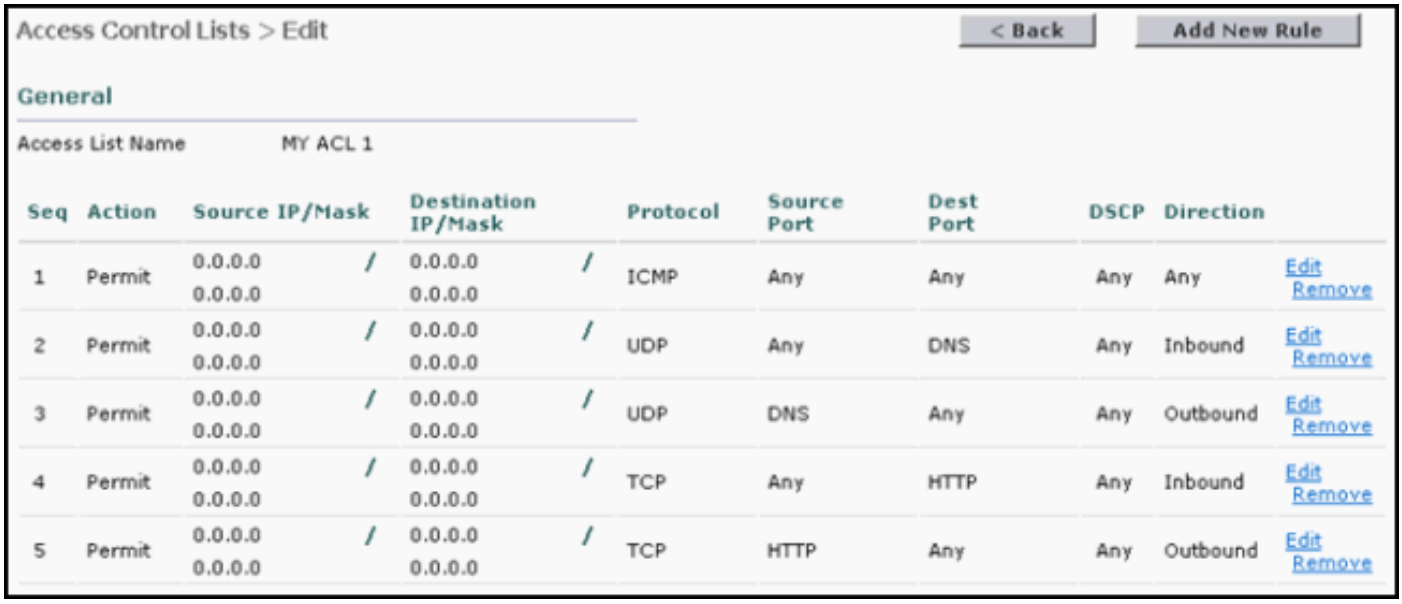
以下是ACL在**show acl detailed "MY ACL 1"**（如果ACL名稱超過1個單詞，才需要引號）命令輸出中的樣子：

```
Seq  Direction  Source IP/Mask   Dest IP/Mask     Protocol  Src Port  Dest Port  DSCP  Action
---  ---------  ---------------  ---------------  --------  --------  ---------  ----  ------
1      Any      0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     1      0-65535   0-65535     Any  Permit
2      In       0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     17     0-65535   53-53       Any  Permit
3      Out      0.0.0.0/0.0.0.0  0.0.0.0/0.0.0.0     17     53-53     0-65535     Any  Permit
```

如果您在DNS和HTTP ACL行中指定無線客戶端所在的子網而不是Any IP地址，則ACL可能會更受限制。

注意：DHCP ACL線路不能進行子網限制，因為客戶端最初使用0.0.0.0接收其IP地址，然後通過子網地址更新其IP地址。

下面是GUI中相同ACL的樣子：



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name MY ACL 1

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	HTTP	Any	Inbound	Edit Remove
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any	Any	Outbound	Edit Remove

使用DHCP、PING、HTTP和SCCP的ACL示例

在此配置示例中，7920 IP電話僅能：

- 接收DHCP地址（無法被ACL阻止）
- Ping並被ping（任何ICMP訊息型別 — 不能限製為僅ping）
- 允許DNS解析（入站）
- 與CallManager的IP電話連線，反之亦然（任意方向）
- 到TFTP伺服器的IP電話連線（在與UDP埠69進行初始TFTP連線後，CallManager使用動態埠）（出站）
- 允許7920 IP電話與IP電話通訊（任意方向）
- 禁止IP電話Web或電話目錄（出站）。這是透過ACL結尾的隱含「deny any any」ACL行完成的。這將允許IP電話之間的語音通訊以及IP電話和CallManager之間的正常啟動操作。

為了設定這些安全要求，ACL必須允許以下行：

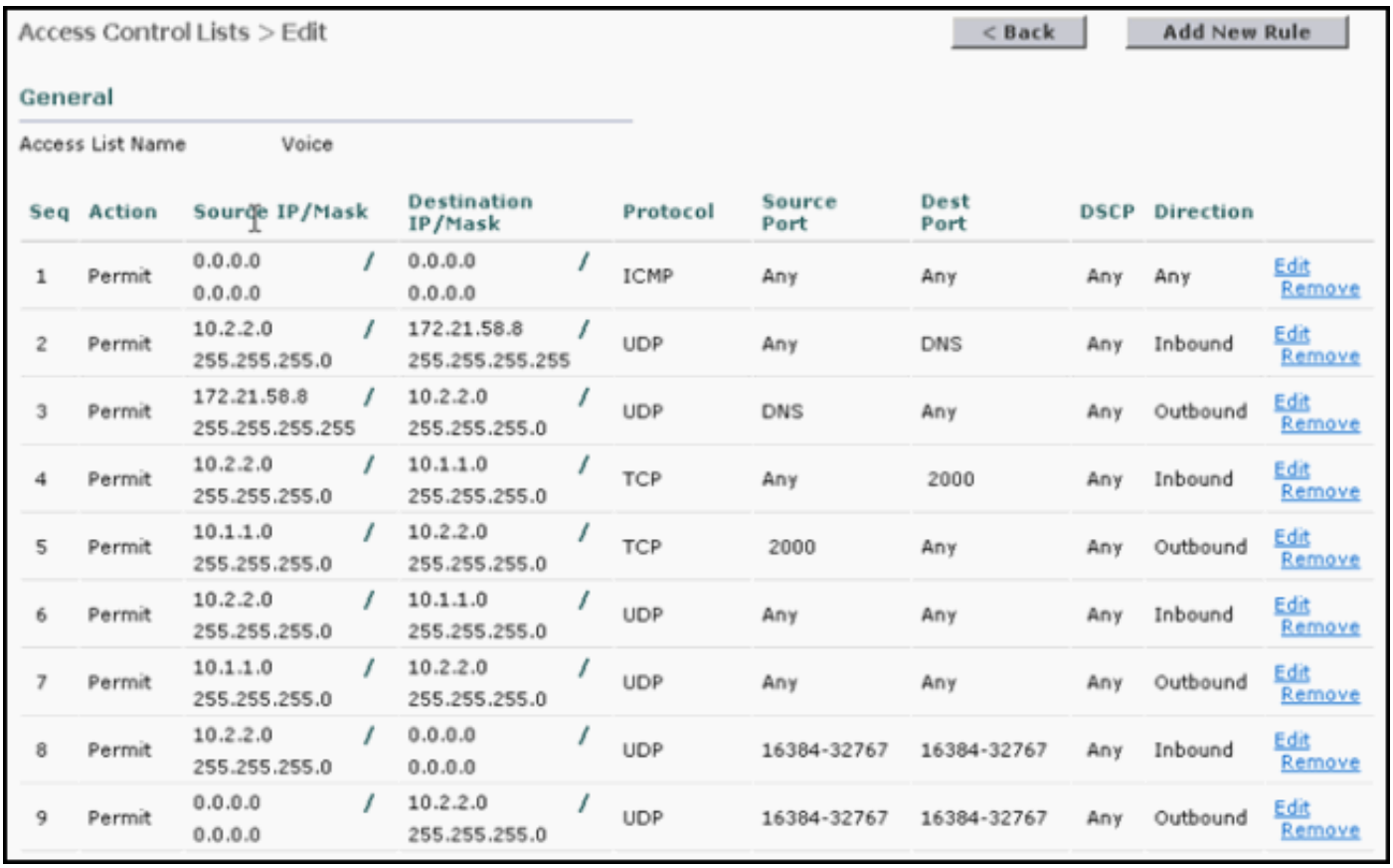
- 任何ICMP訊息（不能限製為僅ping）（任意方向）
- DNS伺服器的IP電話（UDP埠53）（入站）
- DNS伺服器到IP電話（UDP埠53）（出站）
- 到CallManager TCP埠2000的IP電話TCP埠（預設埠）（入站）
- 從CallManager到IP電話的TCP埠2000（出站）
- IP電話到TFTP伺服器的UDP埠。這不能限製為標準TFTP埠(69)，因為CallManager在初次連線請求資料傳輸後使用動態埠。
- 用於IP電話之間的音訊流量RTP的UDP埠(UDP16384口)-32767（任意方向）

在本例中，7920 IP電話子網為10.2.2.0/24,CallManager子網為10.1.1.0/24。DNS伺服器是172.21.58.8。以下是**show acl detail Voice**命令的輸出：

```
Seq Direction Source IP/Mask          Dest IP/Mask            Protocol Src Port  Dest Port  DSCP
Action
--- --------- --------------          --------------          -------- --------  ---------  ----
------
1     Any     0.0.0.0/0.0.0.0         0.0.0.0/0.0.0.0            1     0-65535   0-65535    Any
Permit
2     In      10.2.2.0/255.255.255.0 172.21.58.8/255.255.255.255 17    0-65535   53-53      Any
Permit
```

```
3     Out     172.21.58.8/255.255.255.255 10.2.2.0/255.255.255.0 17    53-53     0-65535    Any
Permit
4     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     6     0-65535   2000-2000  Any
Permit
5     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     6     2000-2000 0-65535    Any
Permit
6     In      10.2.2.0/255.255.255.0  10.1.1.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
7     Out     10.1.1.0/255.255.255.0  10.2.2.0/255.255.255.0     17    0-65535   0-65535    Any
Permit
8     In      10.2.2.0/255.255.255.0  0.0.0.0/0.0.0.0            17 16384-32767 16384-32767 Any
Permit
9     Out     0.0.0.0/0.0.0.0         10.2.2.0/255.255.255.0     17 16384-32767 16384-32767 Any
Permit
```

在GUI中看起來就是這樣的：



Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Any	Edit Remove
2	Permit	10.2.2.0 / 255.255.255.0	172.21.58.8 / 255.255.255.255	UDP	Any	DNS	Any	Inbound	Edit Remove
3	Permit	172.21.58.8 / 255.255.255.255	10.2.2.0 / 255.255.255.0	UDP	DNS	Any	Any	Outbound	Edit Remove
4	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	TCP	Any	2000	Any	Inbound	Edit Remove
5	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	TCP	2000	Any	Any	Outbound	Edit Remove
6	Permit	10.2.2.0 / 255.255.255.0	10.1.1.0 / 255.255.255.0	UDP	Any	Any	Any	Inbound	Edit Remove
7	Permit	10.1.1.0 / 255.255.255.0	10.2.2.0 / 255.255.255.0	UDP	Any	Any	Any	Outbound	Edit Remove
8	Permit	10.2.2.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	UDP	16384-32767	16384-32767	Any	Inbound	Edit Remove
9	Permit	0.0.0.0 / 0.0.0.0	10.2.2.0 / 255.255.255.0	UDP	16384-32767	16384-32767	Any	Outbound	Edit Remove

附錄：7920 IP電話埠

以下是7920 IP電話用於與Cisco CallManager(CCM)和其他IP電話通訊的埠的摘要說明：

- 電話至CCM [TFTP]（UDP埠69最初更改為動態埠[短暫]以進行資料傳輸） — 用於下載韌體和配置檔案的簡單檔案傳輸協定(TFTP)。
- Phone to CCM [Web Services， Directory]（TCP埠80） — 用於XML應用程式、身份驗證、目錄、服務等的電話URL。這些埠可基於每個服務進行配置。
- Phone to CCM [語音信令]（TCP埠2000） — 瘦客戶端控制協定(SCCP)。此埠是可配置的。
- 電話至CCM [安全語音信令]（TCP埠2443） — 安全瘦客戶端控制協定(SCCP)
- Phone to CAPF [Certificates]（TCP埠3804） — 用於向IP電話頒發本地有效證書(LSC)的證書頒發機構代理功能(CAPF)偵聽埠。
- Voice Bearer to/from Phone [Phone Calls](UDP埠16384 - 32768) — 即時協定(RTP)、安全即時協定(SRTP)。**注意**：CCM僅使用UDP埠24576-32768，但其他裝置可以使用全範圍。

- IP Phone to DNS Server [DNS]（UDP埠53） — 當系統配置為使用名稱而不是IP地址時，電話使用DNS解析TFTP伺服器的主機名、CallManager和Web伺服器主機名。
- IP電話到DHCP伺服器[DHCP]（UDP埠67 [客戶端]和68 [伺服器]） — 電話使用DHCP檢索IP地址（如果未進行靜態配置）。

CallManager 5.0用於通訊的埠可在Cisco Unified CallManager 5.0 TCP和UDP埠使用中找到。它也有用於與7920 IP電話通訊的特定埠。

CallManager 4.1用於通訊的埠可在Cisco Unified CallManager 4.1 TCP和UDP埠使用中找到。它也有用於與7920 IP電話通訊的特定埠。

相關資訊

- **無線LAN控制器上的ACL組態範例**
- **思科無線LAN控制器組態設定指南4.0版**
- **技術支援與文件 - Cisco Systems**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。