WLC上的ACL — 规则、限制和示例

目录

简介

本文档提供有关无线LAN控制器(WLC)上的访问控制列表(ACL)的信息。本文档说明当前限制和规则，并提供相关示例。本文档并非要取代无线LAN控制器配置示例中的ACL，而是为了提供补充信息。

注意：对于第2层ACL或第3层ACL规则中的其他灵活性，Cisco建议您在连接到控制器的第一跳路由器上配置ACL。

在ACL行中将协议字段设置为IP(protocol=4)，目的是允许或拒绝IP数据包时会出现最常见的错误。由于此字段实际上选择封装在IP数据包中的内容，例如TCP、用户数据报协议(UDP)和Internet控制消息协议(ICMP)，因此它转换为阻止或允许IP-in-IP数据包。除非您想要阻止移动IP数据包，否则不得在任何ACL行中选择IP。Cisco Bug ID CSCsh22975（仅限注册客户）将IP更改为IP-in-IP。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 关于如何配置WLC和轻量级接入点(LAP)以满足基本运作的知识
- 基本了解轻量接入点协议 (LWAPP) 和无线安全方法

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

了解WLC上的ACL

ACL由一条或多条ACL行组成，在ACL末尾随附一个隐式“deny any any”。每行都有以下字段：

- 序列号
- 方向
- 源IP地址和掩码
- 目的IP地址和掩码
- 协议
- 源端口
- 目的端口
- DSCP
- 操作

本文档介绍以下每个字段：

- **Sequence Number** — 指示根据数据包处理ACL行的顺序。根据ACL处理数据包，直到它与第一个ACL行匹配。它还允许您在ACL中的任何位置插入ACL行，即使在创建ACL之后也是如此。例如，如果您的ACL行序列号为1，则可以通过在新的ACL行中输入序列号1将新的ACL行插入到前面。这会自动将ACL中的当前行向下移动。
- **Direction** — 告知控制器在哪个方向上实施ACL行。有3个方向：入站、出站和任意。这些方向是从相对于WLC而不是无线客户端的位置获取的。入站 — 检查源自无线客户端的IP数据包是否与ACL行匹配。出站 — 检查发往无线客户端的IP数据包是否与ACL行匹配。Any — 检查从无线客户端发往无线客户端的IP数据包，以查看它们是否与ACL行匹配。ACL行同时应用于入站和出站方向。**注意：**为方向选择Any时，应使用的唯一地址和掩码是0.0.0.0/0.0.0.0(Any)。不能使用“Any”方向指定特定主机或子网，因为需要换行地址或子网以允许返回流量。Any方向应仅在以下特定情况下使用：要阻止或允许两个方向的特定IP协议或端口、转至无线客户端（出站）和来自无线客户端（入站）。指定IP地址或子网时，必须将方向指定为Inbound或Outbound，并为相反方向的返回流量创建第二个新ACL行。如果将ACL应用于接口，并且没有明确允许返回流量返回，则返回流量会被ACL列表末尾的隐式“deny any any”拒绝。
- **Source IP Address and Mask** — 定义从一台主机到多个子网的源IP地址，具体取决于掩码。掩码与IP地址结合使用，以便确定当将IP地址与数据包中的IP地址进行比较时，应该忽略IP地址中的哪些位。**注意：**WLC ACL中的掩码与Cisco IOS® ACL中使用的通配符或反掩码不同。在控制器ACL中，255表示完全匹配IP地址中的二进制八位数，而0表示通配符。地址和掩码逐位组合。掩码位1表示检查相应的位值。掩码中指定为255表示检查的数据包的IP地址中的二进制八位数必须与ACL地址中相应的二进制八位数完全匹配。掩码位0表示不检查（忽略）对应位值。掩码中指定0表示忽略检查的数据包IP地址中的二进制八位数。0.0.0.0/0.0.0.0相当于“任意”IP地址（0.0.0.0作为地址，0.0.0.0作为掩码）。
- **Destination IP Address and Mask** — 遵循与源IP地址和掩码相同的掩码规则。
- **Protocol** — 指定IP数据包报头中的协议字段。为了方便客户，某些协议编号被转换，并在下拉菜单中定义。不同的值为：任意（所有协议编号均匹配）TCP（IP协议6）UDP（IP协议17）ICMP（IP协议1）ESP（IP协议50）AH（IP协议51）GRE（IP协议47）IP(IP协议4 IP-in-

IP [CSCsh22975])Eth Over IP（IP协议97）OSPF（IP协议89）其他（请具体说明）Any值匹配数据包的IP报头中的任何协议。这用于完全阻止或允许传入/传出特定子网的IP数据包。选择IP以匹配IP-in-IP数据包。常用的选择是UDP和TCP，它们用于设置特定的源端口和目的端口。如果选择Other，则可以指定IANA定义的任何IP数据包协议号。

- **Src Port** — 只能为TCP和UDP协议指定。0-65535等同于任意端口。
- **Dest Port** — 只能为TCP和UDP协议指定。0-65535等同于任意端口。
- **Differentiated Services Code Point(DSCP)** — 允许您指定特定的DSCP值以匹配IP数据包报头。下拉菜单中的选项是特定或Any。如果配置特定值，则在DSCP字段中指明值。例如，可以使用0到63之间的值。
- **Action** — 这2个操作为deny或permit。拒绝阻止指定的数据包。允许转发数据包。

ACL规则和限制

基于WLC的ACL的限制

以下是基于WLC的ACL的限制：

- 您看不到数据包匹配的ACL行(请参阅Cisco Bug ID CSCse36574(仅限注册客户)。
- 您无法记录与特定ACL行匹配的数据包(请参阅Cisco Bug ID CSCse36574(仅限注册客户))。
- IP数据包（以太网协议字段等于IP [0x0800]的任何数据包）是ACL检查的唯一数据包。其他类型的以太网数据包无法被ACL阻止。例如，ACL无法阻止或允许ARP数据包（以太网协议0x0806）。
- 一个控制器最多可以配置64个ACL；每个ACL最多可以配置64行。
- ACL不会影响从接入点(AP)和无线客户端转发或向其转发的组播和广播流量(请参阅Cisco Bug ID CSCse65613(仅限注册客户))。
- 在WLC版本4.0之前，ACL在管理接口上被绕过，因此您不能影响发往管理接口的流量。在WLC版本4.0之后，您可以创建CPU ACL。有关如何配置此类ACL的详细信息，请参阅配置CPU ACL。**注意：应**用于管理接口和AP管理器接口的ACL将被忽略。WLC上的ACL旨在阻止无线和有线网络之间的流量，而不是有线网络和WLC之间的流量。因此，如果要阻止特定子网中的AP完全与WLC通信，则需要在间歇性交换机或路由器上应用访问列表。这将阻止从这些AP(VLAN)到WLC的LWAPP流量。
- ACL与处理器相关，可能会在重负载下影响控制器的性能。
- ACL无法阻止对虚拟IP地址(1.1.1.1)的访问。因此，无法阻止无线客户端的DHCP。
- ACL不会影响WLC的服务端口。

基于WLC的ACL的规则

以下是基于WLC的ACL的规则：

- 您只能在ACL行的IP报头（UDP、TCP、ICMP等）中指定协议号，因为ACL仅限于IP数据包。如果选择IP，则表明您希望允许或拒绝IP-in-IP数据包。如果选择Any，则表明您希望允许或拒绝使用任何IP协议的数据包。
- 如果为方向选择Any，则源和目标应为Any(0.0.0.0/0.0.0.0)。
- 如果源IP地址或目标IP地址不是Any，则必须指定过滤器的方向。此外，必须为返回流量创建相反方向的逆向语句（交换源IP地址/端口和目标IP地址/端口）。
- ACL末尾有一个隐式“deny any any”。如果数据包与ACL中的任何行都不匹配，则被控制器丢弃。

配置

DHCP、PING、HTTP和DNS ACL示例

在此配置示例中，客户端只能：

- 接收DHCP地址（ACL无法阻止DHCP）
- Ping并被执行ping操作（任何ICMP消息类型 — 不能限制为ping操作）
- 建立HTTP连接（出站）
- 域名系统(DNS)解析（出站）

要配置这些安全要求，ACL必须允许以下行：

- 任一方向的任何ICMP消息（不能限制为ping）
- 任何UDP端口到DNS入站
- DNS到任意UDP端口出站（返回流量）
- 任何到HTTP入站的TCP端口
- HTTP到任意TCP端口出站（返回流量）

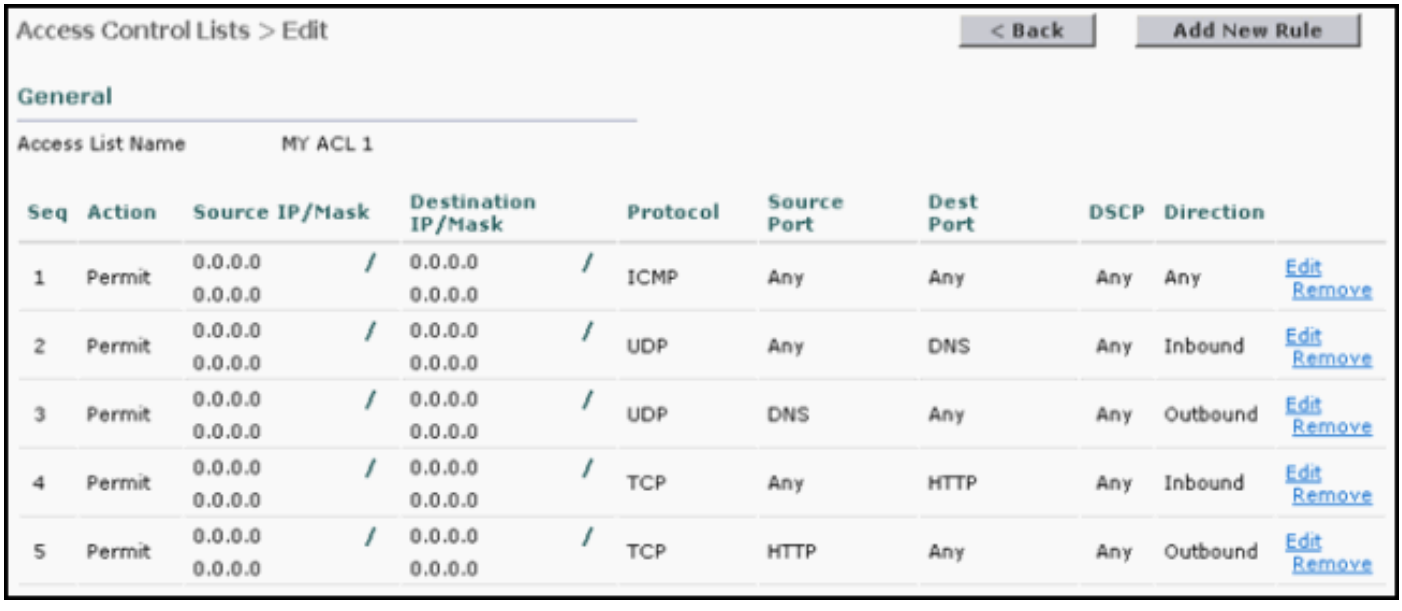
下面是**show acl detailed "MY ACL 1"**（仅当ACL名称大于1个字时才需要引号）命令输出中的ACL的样子：

```
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
```

如果在DNS和HTTP ACL行中指定无线客户端所在的子网而不是Any IP地址，则ACL可能更受限制。

注意：DHCP ACL线路不能进行子网限制，因为客户端最初使用0.0.0.0接收其IP地址，然后通过子网地址更新其IP地址。

下面是GUI中相同ACL的样子：



DHCP、PING、HTTP和SCCP的ACL示例

在此配置示例中，7920 IP电话只能：

- 接收DHCP地址（无法被ACL阻止）
- Ping并被执行ping操作（任何ICMP消息类型 — 不能限制为ping操作）
- 允许DNS解析（入站）
- 与CallManager的IP电话连接，反之亦然（任意方向）
- 到TFTP服务器的IP电话连接（CallManager在与UDP端口69建立初始TFTP连接后使用动态端口）（出站）
- 允许7920 IP电话与IP电话通信（任意方向）
- 禁止IP电话Web或电话目录（出站）。这是通过ACL末尾的隐式“deny any any”ACL行完成的。这将允许IP电话之间的语音通信以及IP电话和CallManager之间的正常启动操作。

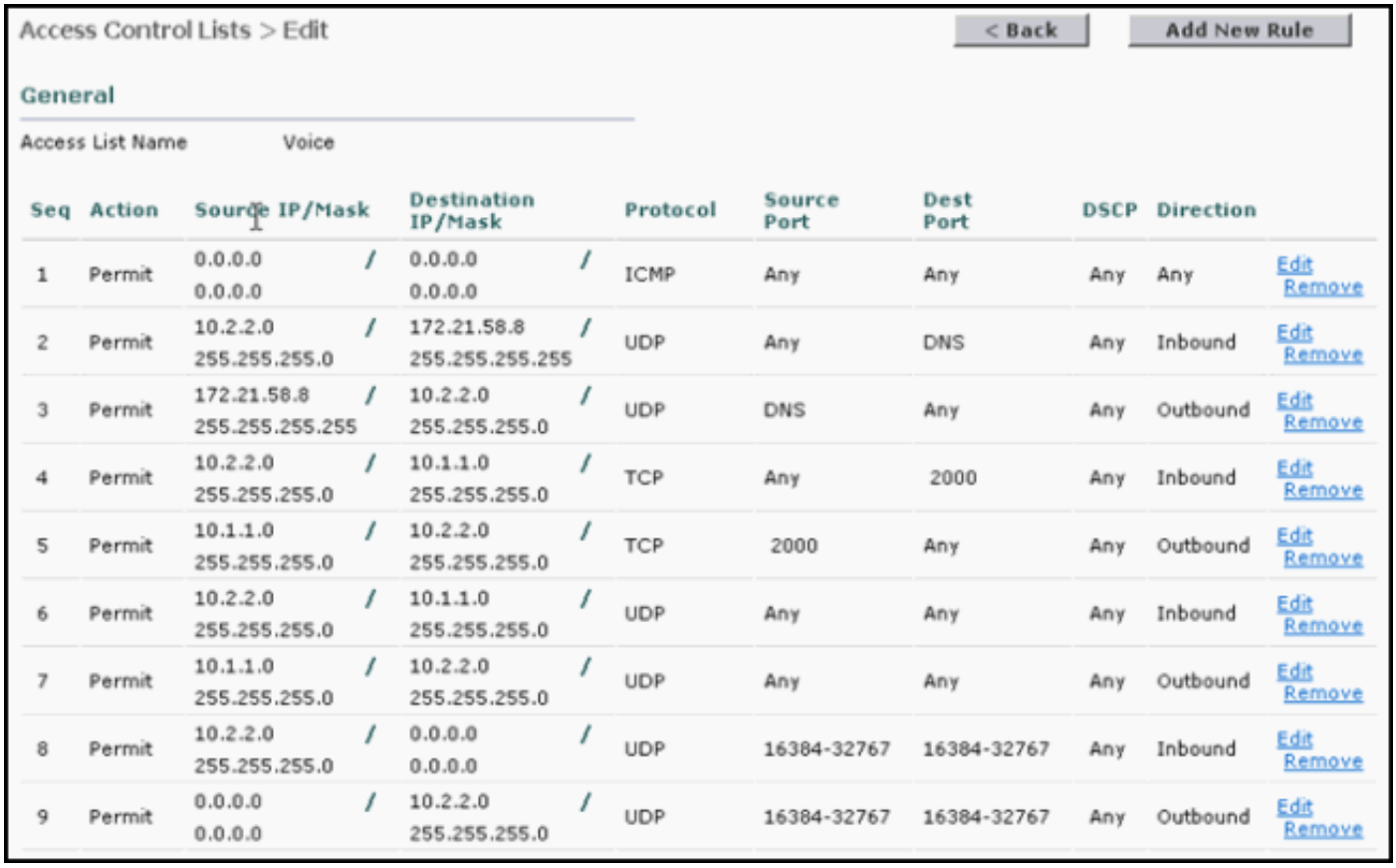
要配置这些安全要求，ACL必须允许以下行：

- 任何ICMP消息（不能限制为ping）（任意方向）
- IP电话到DNS服务器（UDP端口53）（入站）
- DNS服务器到IP电话（UDP端口53）（出站）
- IP电话TCP端口到CallManager TCP端口2000（默认端口）（入站）
- 从CallManager到IP电话的TCP端口2000（出站）
- IP电话到TFTP服务器的UDP端口。这不能限制为标准TFTP端口(69)，因为CallManager在初始连接请求数据传输后使用动态端口。
- 音频流量的UDP端口IP电话之间的RTP(UDP端口16384-32767)（任意方向）

在本示例中，7920 IP电话子网为10.2.2.0/24,CallManager子网为10.1.1.0/24。DNS 服务器为172.21.58.8。以下是**show acl detail Voice**命令的输出：

```
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中看起来就是这样的：



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name: Voice

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

附录：7920 IP电话端口

以下是7920 IP电话用于与Cisco CallManager(CCM)和其他IP电话通信的端口的概要说明：

- Phone to CCM [TFTP]（UDP端口69最初更改为动态端口[Temporal]进行数据传输）— 用于下载固件和配置文件的简单文件传输协议(TFTP)。
- Phone to CCM [Web Services， Directory]（TCP端口80）— 适用于XML应用、身份验证、目录、服务等的电话URL。这些端口可基于每个服务进行配置。
- Phone to CCM [语音信令]（TCP端口2000）— 瘦客户端控制协议(SCCP)。此端口可配置。
- Phone to CCM [安全语音信令]（TCP端口2443）— 安全瘦客户端控制协议(SCCP)
- Phone to CAPF [Certificates]（TCP端口3804）— 用于向IP电话颁发本地有效证书(LSC)的证书颁发机构代理功能(CAPF)侦听端口。
- Voice Bearer to/from Phone [Phone Calls](UDP端口16384 - 32768) — 实时协议(RTP)、安全实时协议(SRTP)。**注意**：CCM仅使用UDP端口24576-32768，但其他设备可以使用全范围。
- IP Phone to DNS Server [DNS]（UDP端口53）— 当系统配置为使用名称而不是IP地址时，电话使用DNS解析TFTP服务器的主机名、CallManager和Web服务器的主机名。
- IP Phone to DHCP server [DHCP]（UDP端口67 [客户端]和68 [服务器]）— 电话使用DHCP检索IP地址（如果未静态配置）。

CallManager 5.0用于通信的端口可在Cisco Unified CallManager 5.0 TCP和UDP端口使用中找到。它还具有用于与7920 IP电话通信的特定端口。

在Cisco Unified CallManager 4.1 TCP和UDP端口使用中可找到CallManager用于通信的端口。它还具有用于与7920 IP电话通信的特定端口。

相关信息

- 无线 LAN 控制器中的 ACL 配置示例
- Cisco 无线 LAN 控制器配置指南 4.0 版
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。