在无线局域网控制器的ACL ：规则、限制和示例

目录

简介

本文在无线局域网控制器(WLCs)提供关于访问控制列表(ACL)的信息。本文解释当前限制和规则，并且提供相关示例。本文没有被认为是ACL的一更换在无线局域网控制器配置示例，但是提供补充信息。

注意： 对于Layer2 ACL或另外的灵活性在第3层ACL规则，思科建议您配置ACL在第一跳跃路由器连接对控制器。

多数常见错误发生，当Protocol字段设置为IP (protocol=4)时在ACL线路打算允许或拒绝IP信息包。由于此字段实际上选择什么被封装在IP数据包里面，例如TCP、用户数据报协议(UDP)和互联网控制消息协议(ICMP)，翻译成阻塞或允许IP在IP数据包。除非要阻塞Mobile IP数据包，在任何ACL线路不能选择IP。Cisco Bug ID CSCsh22975 (仅限注册用户)更改IP对IP在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。

了解在WLC的ACL

ACL隐式跟随的由一个或更多ACL线路制成“拒绝所有其中任一”在ACL结束时。每条线路有这些字段：

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

本文描述这些字段中的每一个：

- **序号**—指示命令ACL线路处理数据包。数据包处理ACL，直到匹配第一条ACL线路。在ACL创建以后，它也允许您插入ACL线路任何地方在ACL。例如，如果有一条ACL线路用序号1，您能通过放置插入在前面的一条新的ACL线路，如果它在序号1在新的ACL线路。这自动地移动当前线路下来在ACL。
- **方向**—告诉强制执行ACL线路的方向的控制器。有3个方向：入站，出站和其中任一。这些方向从位置被采取相对WLC而不是无线客户端。入站—从无线客户端发出的IP信息包被检查发现他们是否匹配ACL线路。出站— IP信息包被注定对无线客户端被检查发现他们是否匹配ACL线路。其中任一— IP信息包发出从无线客户端和被注定对无线客户端被检查发现他们是否匹配ACL线路。ACL线路应用对入站和出站方向。**注意：** 应该使用的唯一的地址和掩码，当您为方向时选择其中任一是0.0.0.0/0.0.0.0 (其中任一)。因为新的一行将要求与被交换的地址或子网允许回程数据流，您不能指定一台特定主机或分支子网与“任何”方向。应该只使用在特定的情况下所有方向您要阻塞或允许一个特定IP协议或端口两个方向的地方，去无线客户端(出站)和来自无线客户端(入站)。当您指定IP地址或子网时，您必须指定方向作为入站或出站和创建回程数据流的秒钟新建的ACL线路在相反的方向。如果ACL应用对接口，并且通过不特别地允许回程数据流上一步，回程数据流由隐式拒绝“拒绝所有其中任一”在ACL列表结束时。
- **源IP地址和掩码**—定义了从单个主机的IP原地址到多个子网，依靠掩码。掩码与IP地址一道用于为了确定应该忽略IP地址的哪些位，当该IP地址与在数据包时的IP地址比较。**注意：** 在WLC ACL的掩码不是类似用于Cisco IOS ACL的通配符或反面掩码。在控制器ACL中，而0是通配符，255正确地含义匹配在IP地址的八位位组。地址和掩码逐渐被结合。掩码位1含义检查相应位值。规格255在掩码指示在被检查必须完全地匹配与在ACL地址的对应的八位位组数据包的IP地址的八位位组。掩码位0含义不检查(忽略)该相应位值。规格0在掩码指示在被检查忽略数据包的IP地址的八位位组。0.0.0.0/0.0.0.0与“所有” IP地址(0.0.0.0作为地址和0.0.0.0是等同的作为掩码)。
- **目的IP地址和掩码**—遵从掩码规则和源IP地址和掩码一样。
- **协议**—指定在IP数据包报头的Protocol字段。某些协议号在下拉菜单翻译为了客户方便和定义。

不同的值是：其中任一(所有协议号匹配)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在IP [CSCsh22975])在IP (IP协议97)的EthOSPF (IP协议89)其他(请指定)所有值匹配在数据包的IP报头的任何协议。这用于完全阻塞或允许到/从特定子网的IP信息包。匹配IP在IP数据包的挑选IP。提供设置特定源及目的地端口的普通的选择是UDP和TCP。如果选择其他，您能指定IANA定义的其中任一IP数据包协议号 。

- **Src波尔特**—能为TCP和UDP协议只指定。0-65535与所有端口是等同的。
- **目的端口**—能为TCP和UDP协议只指定。0-65535与所有端口是等同的。
- **差分服务代码点**—在IP数据包报头允许您指定特定DSCP值匹配。在下拉菜单的选择是特定或其中任一。如果配置特定，您指示在DSCP字段的值。例如，可以使用从0的值到63。
- **操作**— 2操作是拒绝或允许。丢弃块指定的数据包。Permit转发数据包。

ACL规则和限制

WLC的限制根据ACL

这些是限制关于基于WLC的ACL ：

- 您看不到什么ACL线路由数据包(参考的Cisco Bug ID CSCse36574 (仅限注册用户))匹配。
- 您不能记录匹配一条特定ACL线路的数据包(参考的Cisco Bug ID CSCse36574 (仅限注册用户))。
- IP信息包(有以太网Protocol字段的任何数据包相等与IP [0x0800])是ACL检查的唯一的数据包。以太网数据包的其他类型不可能由ACL阻塞。例如， ARP数据包(以太网协议0x0806)不可能由ACL阻塞或允许。
- 控制器能有配置的64个ACL;每个ACL能有至最多64条线路。
- ACL不影响转发或给接入点的组播和广播数据流(AP)和无线客户端(参考的Cisco Bug ID CSCse65613 (仅限注册用户))。
- 在WLC版本4.0前， ACL在管理接口绕过，因此您不能影响流量被注定对管理接口。在WLC版本4.0以后，您能创建CPU ACL。参考请配置CPU ACL关于如何配置此种ACL的更多信息。**注意：** ACL应用对管理和Ap-manager接口忽略。在WLC的ACL没有设计阻塞无线之间的流量和有线网络、有线网络和没有WLC。所以，如果要防止在某些子网的AP整个通信与WLC，您需要运用在您的断断续续交换机或路由器的一访问列表。这将阻塞从那些的LWAPP流量AP (VLAN)对WLC。
- ACL从属处理机，并且能影响控制器的性能在重载下。
- ACL不能阻止对虚拟IP地址(1.1.1.1)的访问。所以， DHCP不可能为无线客户端阻塞。
- ACL不影响WLC的服务端口。

WLC的规则根据ACL

这些是基于WLC的ACL的规则：

- 您能只指定在IP报头(UDP、TCP、ICMP等等)的协议号在ACL线路，因为ACL限制到仅IP信息包。如果IP选择，这表明您要允许或丢弃IP在IP数据包。如果其中任一选择，这表明您要允许或丢弃有所有IP协议的数据包。
- 如果为方向选择其中任一，源和目的应该是其中任一(0.0.0.0/0.0.0.0)。
- 如果来源或目的IP地址不是其中任一，必须指定过滤器的方向。并且，必须为回程数据流创建一个相反语句(当被交换的源IP地址/端口和目的IP地址/端口)在相反的方向。
- 隐式“拒绝所有其中任一”在ACL结束时。如果数据包不匹配在ACL的任何线路，由控制器丢弃。

配置

ACL示例用DHCP、PING、HTTP和DNS

在本例中配置示例，客户端是只能：

- 接收DHCP地址(DHCP不可能由ACL阻塞)
- ping和ping (任何ICMP消息类型-不能限制只ping)
- 做HTTP连接(出站)
- 域名系统(DNS)解决方法(出站)

为了配置这些安全需求， ACL必须有准许的线路：

- 其中任一ICMP信息在任何一个方向(不能限制只ping)
- 入站的DNS的任何UDP端口
- 对出站任何UDP的端口的DNS (回程数据流)
- 对入站的HTTP的任何TCP端口
- 对出站任何的TCP端口的HTTP (回程数据流)

这是什么ACL看起来象在**被选派"我的ACL 1"** (报价单只是必要的ACL名称是否是超过1个词)命令输出的**显示ACL** ：

```
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
```

ACL可以更加限制式，如果指定子网无线客户端继续下去而不是在DNS和HTTP ACL线路的所有IP地址。

注意： 使用0.0.0.0， DHCP ACL线路不可以是作为客户端限制的子网最初收到其IP地址，然后通过子网地址更新其IP地址。

这是什么同样ACL看起来象在GUI ：

与DHCP、PING、HTTP和SCCP的ACL示例

在本例中配置示例， 7920 IP电话是只能：

- 接收DHCP地址(不能由ACL阻塞)
- ping和ping (任何ICMP消息类型-不能限制只ping)
- 允许DNS解析(入站)
- 对反之亦然CallManager的IP电话连接(任何方向)
- 对TFTP server的IP电话连接(CallManager在对(出站) UDP的端口69)的最初的TFTP连接以后使用动态端口
- 允许7920个IP电话对IP电话通信(任何方向)
- 禁止IP电话Web或给目录打电话(出站)。这通过隐式执行"拒绝所有任何" ACL线路在ACL结束时。这将允许IP电话之间的语音通信以及正常启动在IP电话和CallManager之间的操作。

为了配置这些安全需求， ACL必须有准许的线路：

- 其中任一ICMP信息(不能限制只ping) (任何方向)

- 对DNS服务器((入站) UDP的端口53)的IP电话
- 对IP电话((出站) UDP的端口53)的DNS服务器
- IP电话CallManager TCP端口的2000年((入站)的默认端口) TCP端口
- 从CallManager的TCP端口2000年到IP电话(出站)
- 从IP电话的UDP端口到TFTP server。这不可能限制到标准的TFTP端口(69)，因为CallManager使用一个动态端口，在初始连接请求数据传输后。
- 音频数据流RTP的UDP端口在IP电话(UDP ports16384-32767) (任何方向)之间

在本例中， 7920 IP电话子网是10.2.2.0/24，并且CallManager子网是10.1.1.0/24。DNS服务器是172.21.58.8。这是从**显示ACL详细信息语音指令的**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
```

这是什么看起来象在GUI ：

附录：7920个IP电话端口

这些是端口的概况说明7920 IP电话用途通信与Cisco CallManager (CCM)和其他IP电话：

- 给对CCM [TFTP]打电话(UDP端口69然后最初变成数据传输的动态端口[Ephemeral]) —用于的简单文件传输协议(TFTP)下载固件和配置文件。
- 给对CCM [Web Services， Directory] (TCP端口80)打电话—给XML应用程序、验证、目录、服务等等的URL打电话。这些端口是可配置在a每个服务基本类型。
- 给对CCM [Voice Signaling] (TCP端口打电话2000) —小型客户机控制协议(SCCP)。此端口可配置。
- 对CCM [Secure Voice Signaling] (TCP端口2443) —安全小型客户机控制协议(SCCPS)的电话
- 给对CAPF [Certificates] (TCP端口3804)打电话—认证机关发出的局部重要的证书(LSCs)代理功能(CAPF)监听端口对IP电话。
- 到/从电话[Phone Calls]的语音持票人(UDP端口16384 – 32768) —实时协议(RTP)，安全实时协议(SRTP)。**注意：** CCM只使用UDP端口24576-32768，但是其它设备能使用全程。
- 对DNS服务器[DNS] (UDP端口53)的IP电话—电话使用DNS解析TFTP服务器、CallManager和Web服务器主机名主机名，当系统配置使用名称而不是IP地址时。
- 对DHCP服务器[DHCP] (UDP端口67 [client] & 68 [server])的IP电话—电话使用DHCP检索IP地址，如果不静态配置。

端口5.0 CallManager用途沟通与可以在Cisco Unified CallManager 5.0 TCP找到和UDP波尔特使用情况。使用与7920个IP电话联络的它也有特定端口。

端口4.1 CallManager用途沟通与可以在Cisco Unified CallManager 4.1 TCP找到和UDP波尔特使用情况。使用与7920个IP电话联络的它也有特定端口。

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