在WLC上的ACL配置：规则，限制以及范例

介绍

本文提供了在 WLC 上配置 ACL 的相关信息。本文解释了当前 ACL 的限制和规则，并给了相关的示例。但是并不意味着本文是来代替“ACLs on Wireless LAN Controller Configuration Example”的，而是提供了进一步的补充。（如果参考在 WLC 上的 ACL 配置，请参考以下网址：
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00807810d1.shtml

对于二层 ACL 或者更加灵活的三层 ACL 规则，思科建议在连接ＷＬＣ的最近的路由器上进行配置。

当配置ＡＬＣ时，最常见的错误是，为了允许或禁止 IP 包，将协议字段设置为 IP（protocol=4），因为这个字段，实际配置的是在 IP 数据包中封装的类型，比如ＴＣＰ，ＵＤＰ或者ＩＣＭＰ，它会转变为允许或者拒绝 IP-in-IP 数据包，除非你想阻塞移动ＩＰ数据包，否则，在 ACL 配置中绝对不能选择 IP。思科 BUG ID CSCsh22975 改正 IP 为 IP-in-IP。

配置条件

必要条件

在配置前，请先确定掌握以下知识点：

（1） 知道如何配置ＷＬＣ和ＬＡＰ的基本操作；

（2） 了解ＬＷＡＰＰ和无线安全技术的基本知识；

使用说明

本文中无特殊的软件或硬件版本限制

规定

请参考以下网址（思科技术小窍门），获得更多信息
http://www.cisco.com/en/US/tech/tk801/tk36/technologies_tech_note09186a0080121ac5.shtml

在ＷＬＣ上的ＡＣＬ的作用

ACL 策略包含一行或多行 ACL，最后是隐含的“Deny any any”。每行ＡＣＬ包含以下部分：
（１） 序列号
（２） 方向
（３） 源ＩＰ地址和掩码
（４） 目的ＩＰ地址和掩码
（５） 协议
（６） 源端口
（７） 目的端口
（８） ＤＳＣＰ
（９） 动作
本文对以上各组成部分进行描述
（１） 序列号

表明 ACL 的顺序，数据包按照 ACL 的顺序匹配，直到符合一条策略，当 ACL 已经创建好后，也可以随时插入添加的 ACL 语句。例如，如果已经创建了一个 ACL 语句 1，当想在它之前插入一条语句，新创建的语句为 1，插入后，原来的语句会随着新插入的序列改变。

（２） 方向

WLC 对哪个方向的数据做 ACL 匹配，有三种方向，进，出，和任何方向，这些所谓的方向，是对 WLC 而言，非无线的客户端。

- 进方向-数据包是从无限客户端发送出来，进行 ACL 检查
- 出方向-数据包是发送给无线客户端，进行 ACL 检查
- 任何方向-任何进或者出的方向

当配置 0.0.0.0/0.0.0.0 时，意味着任何方向，当想对特定的协议或者端口在进出方向使用 ACL 时，可以使用任何方向配置，当定义了特定的 IP 地址段时，必须定义进或者是出方向。

（３） 源 IP 地址和掩码

定义源地址，地址段取决于配置的掩码，使用掩码来确定是否有正确的 IP 数据包匹配。

【译者注】在 WLC 中配置 ACL 的掩码和在 IOS 里面的掩码含义是不一样的，在 WLC 中，255 意味着严格匹配，0 作为通配符，每位一对一匹配。

在掩码中，1 意思为严格匹配对应的位，255 意味着严格匹配对应的 8 位字符，0 意味着忽略此位，0.0.0.0/0.0.0.0 意味着所有。

（４） 目的地址和掩码

按照以上的规则，同样定义

（５） 协议

在 IP 包中定义协议，某些定义的协议可以自动转换成对应的数值：

Any：所有协议都会被匹配

TCP：协议号 6

UDP：协议号 17

ICMP：协议号 1

ESP：协议号 50

AH：协议号 51

GRE：协议号 47

IP：协议号 4

在 IP 之上的以太：协议号 97

OSPF：协议号 89

其他：需要定义

（６） 源端口

只能定义 TCP 或者 UDP，数值从 0-65535

（７） 目的端口

只能定义 TCP 或者 UDP，数值从 0-65535

（８） 服务差别代码（DSCP）

可以通过定义的 DSCP，匹配对应的 IP 数据包，数值从 0-63

（９） 动作

拒绝或者允许

ACL 规则和限制

在 WLC 上 ACL 的限制

（１） 不能看到 ACL 是否对数据包有匹配

（２） 不能对匹配的数据包做 LOG

（３） 只有以太协议号为 0x0800 的 IP 数据包才可以被 ACL 匹配，其他类型的数据，例如，ARP 不能被 ACL 检测

（４） 每个 WLC 只能配置 64 条 ACL，每个ＡＣＬ只能有６４条语句

（５） ＡＣＬ不会对广播或者组播数据有影响

（６） 在ＷＬＣ版本４．０之前，ＡＣＬ对管理接口的数据不起作用，在版本４．０之后，可以通过建立ＣＰＵ的ＡＣＬ对管理数据生效，请参考以下网址：

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00807810d1.shtml#cpuacl

（７） ＡＣＬ的生效要考虑ＷＬＣ的负荷能力

（８） ＡＣＬ不能阻止到达虚拟接口 1.1.1.1 的数据，所以，无线客户端不能阻止ＤＨＣＰ

（９） ＡＣＬ不对服务端口的数据生效

在ＷＬＣ上ＡＣＬ的规则

（１） 在ＡＣＬ中，只能定义（ＵＤＰ，ＴＣＰ，ＩＣＭＰ等）协议类型，因为ＡＣＬ是用来对ＩＰ数据做限制。

（２） 如果配置了任何方向，那么源和目的都是 0.0.0.0/0.0.0.0

（３） 如果源和目的都不是任何，那么一定要定义方向

（４） 在ＡＣＬ中，默认最后是拒绝所有的数据包。如果数据包没有匹配任何 ACL 规则，它最终会被控制器丢弃。

配置

ＤＨＣＰ，ＰＩＮＧ，ＨＴＴＰ和ＤＮＳ的范例

在这个配置下，无线客户端只能有以下能力：

（１） 收到ＤＨＣＰ的地址（ＡＣＬ不对ＤＨＣＰ生效）

（２） ｐｉｎｇ以及被ｐｉｎｇ

（３） 出方向的ＨＴＴＰ连接

（４） ＤＮＳ请求

ＡＣＬ中包含以下语句：

（１） ＩＣＭＰ的任何方向

（２） 任何进入的ＤＮＳ的ＵＤＰ数据

（３） 任何出方向的ＤＮＳ的ＵＤＰ数据

（４） 任何进方向的ＨＴＴＰ的ＴＣＰ数据

（５） 任何返回的ＨＴＴＰ数据

通过 **show acl detailed "MY ACL 1** 察看ＡＣＬ的配置

（６） Seq Direction Source IP/Mask Dest IP/Mask Protocol Src Port Dest Port DSCP Action

（７） --- --------- --- --- --- --- --- --- ---

（８） 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

（９） 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

（１０） 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

通过ＧＵＩ方式察看

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

ＤＨＣＰ，ＰＩＮＧ，ＨＴＴＰ和ｓｃｃｐ的范例

在这个配置中，７９２０ＩＰ电话的功能：

（１） 收到ＤＨＣＰ地址

（２） ｐｉｎｇ和被ｐｉｎｇ

（３） 允许进方向的ＤＮＳ回复

（４） ＩＰ电话和ＣＭ的连接

（５） 出方向的ＩＰ电话和ＴＦＴＰ服务器的连接

（６） ７９２０和其他ＩＰ电话的连接

（７） 不允许出方向的ＩＰ电话的ｗｅｂ以及目录访问

ＡＣＬ语句包含以下语法：

（１） 允许任何方向的ＩＣＭＰ

（２） 进方向的ＩＰ电话到ＤＮＳ的连接（ＵＤＰ５３）

（３） 出方向的ＤＮＳ服务器到ＩＰ电话的回复（ＵＤＰ５３）

（４） 进方向的ＩＰ电话与ＣＭ的ＴＣＰ２０００的连接

（５） 出方向的ＣＭ到ＩＰ电话的ＴＣＰ２０００的连接

（６） ＩＰ电话到 TFTP 服务器的 UDP69 的连接

（７） IP 电话之前的 SCCP 的 UDP 连接

7920IP 电话的网段是 10.2.2.0/24，CM 地址 10.1.1.0/24，DNS 服务器地址 172.21.58.8，通过 **show acl detail Voice** 查看

（８） Seq Direction Source IP/Mask Dest IP/Mask Protocol Src Port Dest Port DSCP Action

（９） --- --------- ---------- ---------- -------- -------- --------- ---- ------

（１０） 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

（１１） 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

（１２） 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

（１３） 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

（１４） 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

（１５） 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

（１６） 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

（１７） 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

（１８） 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

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：7920IP 电话的端口

（１） 到 CCM（TFTP）的 UDP69 连接

（２） 到 CCM（WEB）的 TCP80 连接

（３） 到ＣＣＭ（ＶＯＩＣＥ）语音ＴＣＰ２０００连接

（４） 到 CCM（安全语音信号）TCP2443 连接

（５） 到 CAPF 数字证书 TCP3804 连接

（６） 电话之间的语音信号 UDP 16384 – 32768 的连接

【译者注】CCM 只使用 24576-32768

（７） 到 DNSUDP53 的连接

（８） 到 DHCP 的 UDP67，68 的连接

CM5.0 的端口介绍：

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/5_0/50plrev2.pdf

CM4.1 的端口介绍：

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/port/4_1/41plrev2.pdf