在无线局域网控制器上配置ACL示例

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 <u>规则</u> <u>WLC 上的 ACL</u> <u>在WLC 中配置ACL时的注意事项</u> <u>在 WLC 上配置 ACL</u> <u>配置允许访客用户服务的规则</u> <u>配置 CPU ACL</u> <u>验证</u> <u>故障排除</u> 相关信息

简介

本文档介绍如何在无线局域网控制器(WLAN)上配置访问控制列表(ACL),以过滤通过WLAN的流量 。

先决条件

要求

Cisco 建议您了解以下主题:

- •如何配置WLC和轻量接入点(LAP)以实现基本操作
- •基本了解轻量接入点协议 (LWAPP) 和无线安全方法

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行固件 4.0 的 Cisco 2000 系列 WLC
- Cisco 1000 系列 LAP
- •运行固件版本 2.6 的 Cisco 802.11a/b/g 无线客户端适配器
- Cisco Aironet Desktop Utility (ADU) 版本 2.6

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

规则

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

WLC 上的 ACL

WLC 上的 ACL 旨在限制或允许无线客户端访问其 WLAN 上的服务。

在WLC固件版本4.0之前,ACL在管理接口上被绕过,因此您不能影响发往WLC的流量,您只能使用Management Via Wireless选项阻止无线客户端管理控制器。所以,ACL 只能应用到动态接口。 在 WLC 固件版本 4.0 中有能过滤发送到管理接口的数据流的 CPU ACL。有关详细信息,请参阅<u>配</u> 置CPU ACL部分。

您最多能定义 64 个 ACL,每个有 64 个规则(或过滤器)。每个规则有影响其操作的参数。当数据 包匹配规则的所有参数时,为该规则设置的操作将应用到数据包。您能通过 GUI 或 CLI 配置 ACL。

以下是您在 WLC 上配置 ACL 时应理解的规则:

- 如果sourceanddestination为any,则此ACL的应用方向可以为any。
- 如果sourceordestination不是any,则必须指定过滤器的方向,并且必须创建相反方向的逆语句。
- WLC的入站和出站概念是不直观的。它是从面向无线客户端的 WLC 角度,而不是从客户端的 角度。因此,入站方向意味着数据包从无线客户端发往 WLC,而出站方向意味着从 WLC 退出 到无线客户端的数据包。
- ACL 末尾存在隐式拒绝。

在WLC中配置ACL时的注意事项

WLC 中的 ALC 与路由器中 ALC 工作方式不同。在 WLC 中配置 ACL 时需要记住以下事项:

- 当您打算拒绝或允许 IP 数据包通过时,最容易犯的错误是选择 IP。由于您选择IP数据包中的内容,因此您拒绝或允许IP-in-IP数据包。
- 控制器ACL无法阻止WLC虚拟IP地址,因此也无法阻止无线客户端的DHCP数据包。
- 控制器ACL无法阻止从有线网络接收的发往无线客户端的组播流量。控制器ACL处理从无线客 户端发起的、发往同一控制器上的有线网络或其他无线客户端的组播流量。
- 不同于路由器,ACL应用到接口后可在两个方向控制数据流,但它不执行状态防火墙。如果您 忘记在ACL中打开一个用于返回流量的孔,则会导致问题。
- •控制器 ACL 仅阻止 IP 信息包。您不能阻止第 2 层或第 3 层的非 IP 数据包。
- •控制器 ACL 不使用类似路由器的反掩码。这里的 255 表示准确匹配该 IP 地址的八位组。
- 控制器上的 ACL 在软件中完成并影响转发性能。

注:如果将ACL应用于接口或WLAN,无线吞吐量会降低,并可能导致数据包丢失。为了提高 吞吐量,请从接口或 WLAN 上删除 ACL 并且将 ACL 移至相邻的有线设备。

在 WLC 上配置 ACL

此部分描述如何在 WLC 上配置 ACL。目标是配置允许访客客户端访问这些服务的 ACL:

•无线客户端和 DHCP 服务器之间的动态主机配置协议 (DHCP)

- 网络中所有设备之间的 Internet 控制消息协议 (ICMP)
- •无线客户端和 DNS 服务器之间的域名系统 (DNS)
- •特定子网的 Telnet

必须为无线客户端阻塞所有其他服务。要使用WLC GUI创建ACL,请完成以下步骤:

1. 转到 WLC GUI 并选择 Security > Access Control Lists。出现 Access Control Lists 页。此页 列出了在 WLC 上配置的 ACL。您也可以利用它编辑或删除其中任一 ACL。要创建新的 ACL,请单击 New。

G · O · 🔊 🖉	6 P 🛠 C) 🙆 · 🍓 🐴	ddress 🔬 https:/	/172.16.1.40/so	reens,lfre 🎽 🔁 Go	Links Nort	on AnkiWirus 🥸	•	= 0' ×
Enses Statema						Save C	onfiguration	Ping Logout i	Refresh
A. A. Barrenser	MONITOR WLA	NS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP		
Security	Access Control	Lists						New	\mathbb{D}
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Name								
Access Control Lists									
Web Auth Certificate									
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Man agement Frame Protection									
Web Login Page CIDS Sensors Shunned Clients									
6)				2				Internet	1210

访问控制列表

2. 输入 ACL 的名称并单击 Apply。最多可以输入 32 个字母数字字符。在本例中,ACL 的名称是 Guest-ACL。创建ACL后,单击Edit为ACL创建规则。



输入ACL的名称

3. 当 Access Control Lists > Edit 页出现时,单击 Add New Rule。出现 Access Control Lists > Rules > New 页。

⊙ · ⊙ · ≥ ≥	🏠 🔎 👷 🧭 🍰 🕺 Address 🕘 https://172.16.1.40/screens/Fre 🗹 🔁 Go 🛛 Linis 🕺 Norton Antilinus 🥸 - 🦉 – 👘
Cinco Station	Save Configuration Ping Logout Refres
Security	Access Control Lists > Edit Add New Rule
ARA General RADIUS Authentication RADIUS Authentication Local Net Users MAC Filtering Disabled Clients User Logn Policies AP Policies	General
	Access List Name Guest-ACL Seq Action Source IP/Mask Destination Protocol Source Dest DSCP Direction IP/Mask Protocol Port Port
Access Control Lists	
Web Auth Certificate	
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	
Web Login Page	
Sensors Shunned Clients	
Done	(A) Totamat

添加新的ACL规则

4. 配置允许访客用户使用这些服务的规则:无线客户端和 DHCP 服务器之间的 DHCP网络中所 有设备之间的 ICMP无线客户端和 DNS 服务器之间的 DNS特定子网的 Telnet

配置允许访客用户服务的规则

此部分给出了如何为以下服务配置规则的示例:

- •无线客户端和 DHCP 服务器之间的 DHCP
- 网络中所有设备之间的 ICMP
- 无线客户端和 DNS 服务器之间的 DNS
- •特定子网的 Telnet
- 1. 为了定义 DHCP 服务的规则,请选择来源和目标 IP 范围。此示例使用 any 来源,这意味着允许任意无线客户端访问 DHCP 服务器。在本例中,服务器 172.16.1.1 作为 DHCP 和 DNS 服务器。因此,目标 IP 地址是 172.16.1.1/255.255.255.255(带主机掩码)。由于 DHCP 是基于 UDP 的协议,请从 Protocol 下拉字段中选择 UDP。如果在上一步中选择TCP或UDP,则会显示两个附加参数:源端口和目标端口。指定来源及目标端口详细信息。对于此规则,来源端口是 DHCP 客户端,并且目标端口是 DHCP 服务器。选择 ACL 将应用的方向。由于此规则是从客户端到服务器,所有此示例使用 入站。从 Action 下拉框中选择 Permit 让此 ACL 允许 DHCP 数据包从无线客户端发送到 DHCP 服务器。默认值是"Deny"。单击 Apply。

168 STATEM					iguration Ping Logo	ut Refre
<u>A. A.</u>	MONITOR WLANS	CONTROLLER WIRELES	IS SECURITY MANAGE	MENT COMMANDS	IELP	
Recurity	Access Control List	s > Rules > New			< Back A	pply
AA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Fithering Disabled Clients	Sequence Source Destination	1 Any 💙 IP Address 💙	IP Address 172.16.1.1	Netmask 255.255.255.255]	
User Login Policies AP Policies	Protocol	UDP 👻				
Access Control Lists	Source Port	DHCP Client				
Web Auth Certificate Wireless Protection Policies	Destination Port	DHCP Server				
Trusted AP Policies Rogue Policies Standard Signatures	DISCP	Any 💌 Inbound 💌				
Signature Events Summary Client Exclusion Policies AP Authentication / NEP Management Frame Protection	Action	Permit 👻				
Veb Login Page						
CIDS Sensors Shunned Clients						
					and togenet	

选择Permit以使ACL允许DHCP数据包如果来源和目标不是 any,则必须创建相反方向的逆向语句。下面是一个示例。

G · O · 🗷 🖻	0 2 2 6 0	Address 🕘 https:	//172.16.1.40/screens/fra 🎽 🛃 G	Lines Norton Ar	valvirus 😡 -	
Alles adds.	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HE	LP	Logout Kerresi
Security	Access Control Lists	s > Rules > New			< Back	Apply
AAA General RADIUS Authentication	Sequence Source	2 IP Address	IP Address	Vetmask 255.255.255.255		
RADIUS Accounting Local Net Users MAC Filtering	Destination	Any 👻				
Disabled Clients User Login Policies	Protocol	UDP 💌				
Access Control Lists	Source Port	DHCP Server 👻				
Web Auth Certificate	Destination Port	DHCP Client				
Wireless Protection Policies Trusted AP Policies	DSCP	Any 👻				
Rogue Policies Standard Signatures	Direction	Outbound 💌				
Custom Signatures Signature Events Summery Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Action	Permit 💌				
Web Login Page						
CIDS Sensors Shunned Clients						
9					 Inte 	met

源或目标设置为"任意"

2. 为了定义规则以允许 ICMP 数据包在所有设备之间传输,请在 Source 和 Destination 字段中选择 any。这是默认值。从 Protocol 下拉式字段中选择 ICMP。由于此示例在 Source 和 Destination 字段中使用 any 字段,因此您无需指定方向。可以保留默认值 any。并且无需创 建相反方向的逆向语句。从 Action 下拉框中选择 Permit,让此 ACL 允许 DHCP 数据包从无 线客户端发送到 DHCP 服务器。单击 Apply。

G · O · E	6 P 🛠 🛛 6	Address 🔬 https:	//172.16.1.40/scre	ens,lfre 🌱 🛃 Go	Links Nort	on Ankilvirus 😣 🔹	🥂 – 8 ×
Cinca Station	and the second		and the second		Save C	onfiguration Ping	Logout Refresh
<u>_AliAh.</u> International	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	- Sector Production
Security	Access Control Lists	s > Rules > New				< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users	Sequence Source Destination	3 Any V Any V					
Disabled Clients User Login Policies AP Policies	Protocol	ICMP 💌					
Access Control Lists	DSCP	Any 💌					
Web Auth Certificate	Direction	Any 💌					
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summery Client Exclusion Policies AP Authentication / MFP	Action	Permit					
Management Frame Protection							
Web Login Page							
CIDS Sensors Shunned Clients							
🛃 Done				NO INCOM		🌍 Inte	privot

允许导致ACL允许从DHCP服务器到无线客户端的DHCP数据包

:

 同样,请创建规则允许 DNS 服务器访问所有无线客户端以及允许无线客户端的 Telnet 服务器 访问特定子网。以下是一些示例

				Save Conf	iguration Ping	Logout Refres
A. A. Inspections	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS H	ÆLP	ante de la competencia
Security	Access Control Lis	ts > Rules > New			< Back	Apply
	Sequence	3				
General						
RADIUS Authentication RADIUS Accounting	Source	Any 📉				
Local Net Users MAC Filtering	Destination	Any 💌				
Disabled Clients User Login Policies	Protocol	ICMP 🗸				
AP Policies	DSCP	Any v				
Access Control Lists		intry into				
Wireless Protection	Direction	Any M				
Policies Trusted AP Policies Rogue Policies	Action	Permit 🥢				
Standard Signatures						
Signature Events						
Client Exclusion Policies AP Authentication / MFP						
Protection						
Web Login Page						
CIDS Sensors						
Shunned Clients						
•						
g Done					uno 😡	sennet
创建允许DNS服务器	法问前右工佬友自					
	切凹川有兀线谷厂	户端的规则		10		
3 · 0 · 12	6月月九线各方	自端的规则 合・ る [*] Address 創 https	//172.16.1.40/screens/fre 🌱 🛃 G	io Links Norton /	Antildrus 🙆 •	ây <u>- 8 -</u>
	60回加有元线各广	¹ 端的规则 合・ 🍣 🎽 Address 🗃 Https	//172.16.1.40/screens/fre 💙 🔁 G	o Linis ³⁹ Norton / Save Conf	Intillinus 🙆 -	togout Refres
	の回用有元线各F	¹ 端的规则 会・ ふ [*] Address 創 Https CONTROLLER WIRELESS	I//172.16.1.40/screens,fire ♥ 🔁 G SECURITY MANAGEMENT	io Linis ³⁹ Norton / Save Conf COMMANDS H	Andilizus 🛞 • Iguration Ping IELP	Logout Refres
	の回用有元线各 の P 会 の MONITOR WLANS Access Control Lis	¹³ 端的规则 る・ み ¹⁰ Address 創 Https CONTROLLER WIRELESS ts > Rules > New	J/172.16.1.40/screens,fire V 🕑 G	io Linis ³⁰ Norton / Save Conf COMMANDS H	Antilians 😧 • Iguration Ping IELP	Logout Refres
	の回り用有元线合 の の い TOR WLANS Access Control Lis Sequence	¹ 端的规则 ②・ 過 ^{**} Address 創 https CONTROLLER WIRELESS ts > Rules > New 4	.//172.16.1.40/screens/fre Y 🔁 G	io Linis ³⁹ Notion / Save Conf COMMANDS H	Antilikus 🚱 • Iguration Ping rELP < Backs	Apply
C C C C C C C C C C C C C C C C C C C	MONITOR WLANS Access Control Lis Sequence Source	¹ 端的规则 ②・③ ^{**} Address 創 Https CONTROLLER WIRELESS ts > Rules > New 4 Any ビ	//172.16.1.40/screens,fire ♥ 🔁 G	io Linis ³⁹ Norton J Save Conf COMMANDS H	Antilikus 🚱 • Iguration Ping i€LP < Back	Apply
C C C C C C C C C C C C C C C C C C C	MONITOR WLANS Access Control Lis Sequence Source Destination	¹¹ 端的規则 ②・③ ^{***} Address 創 Https CONTROLLER WIRELESS ts > Rules > New 4 Any IP Address マ	IP Address	ie Linis ³⁹ Norton / Save Conf COMMANDS H COMMANDS H	Antilikus 🚱 • Iguration Ping i€LP < Back	Apply
C C C C C C C C C C C C C C C C C C C	MONITOR WLANS Access Control Lis Sequence Source Destination Protocol	¹¹ 端的規则 CONTROLLER WIRELESS ts > Rules > New 4 Any IP Address マ UDP	IP Address	ie Linis ³⁹ Norton / Save Conf COMMANDS H COMMANDS H	Antilikus 🚱 • Iguration Ping i€LP < Back	Apply
C C C C C C C C C C C C C C C C C C C	MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port	当端的規则 CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥	I/172.16.1.40/screens,fire V 2 G SECURITY MANAGEMENT IP Address 172.16.1.1	io Linis Norton / Save Conf COMMANDS H	Antilikus 🚱 • Iguration Ping KELP < Back	Apply
C · C · C · C · C · C · C · C · C · C ·	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port	当端的規则 CONTROLLER WIRELESS ts > Rules > New 4 Any ▼ IP Address ▼ UDP ▼ Any ▼ DNS ▼	IP Address	ie Linis Norton / Save Conf COMMANDS H	kntilvirus 🚱 • Iguration Ping ÆL₽	Apply
Control of the second of the s	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port Destination Port	当端的规则 CONTROLLER WIRELESS ts > Rules > New 4 Any IP Address ♥ UDP Any NS ♥	IP Address	ie Linis ³⁹ Norton / Save Conf COMMANDS H COMMANDS H	Antilikus 🚱 • Iguration Ping i€LP < Back	Apply
C C C C C C C C C C C C C C C C C C C	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction	当端的規则 ◇ ・ ◇ [●] Address ④ https CONTROLLER WIRELESS ts > Rules > New 4 Any ▼ IP Address ▼ UDP ▼ Any ▼ INS ▼ Any ▼	IP Address	e Linis Norton / Save Conf COMMANDS H	kntilvirus 🚱 • Iguration Ping ÆL₽	Apply
C Custom Signatures Custom Sign	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction	当端的规则 CONTROLLER WIRELESS CONTROLLER WIRELESS ts > Rules > New 4 Any ▼ IP Address ▼ UDP ▼ Any ▼ DNS ▼ Any ▼ Inbound ▼	IP Address	o Linis Norton / Save Conf COMMANDS H Netmask 255.255.255.255	Antilikus 🚱 • Iguration Ping €LP < Back	Apply
Control Division and a second	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	¹ 端的规则 CONTROLLER WIRELESS CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address	io Linis Norton / Save Conf COMMANDS H	Antilikus 🚱 • Iguration Ping ÆLP < Back	Apply
Custom Signatures Custom Signatures Signature Events Signature Events Signa	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	当端的規则 ◇ ・ ◇ [≫] Address ④ https CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address	ie Linis Norton / Save Conf COMMANDS H	Antilikus 🚱 • Iguration Ping ÆLP	Apply
Control Control Control of the second	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	当端的规则 CONTROLLER WIRELESS CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ DNS ♥ Inbound ♥ Permit ♥	IP Address	e Linis Norton / Save Conf COMMANDS H	AndiVirus 🚱 • Iguration Ping ÆL₽	Apply
C Customerson and a constraint of the second and a constraint	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	¹ 端的规则 CONTROLLER WIRELESS ts > Rules > New 4 Any ▼ IP Address ▼ UDP ▼ Any ▼ DNS ▼ Any ▼ Inbound ▼ Permit ▼	IP Address	o Linis Norton / Save Conf COMMANDS H Netmask 255.255.255.255	Antilikus 🚱 • Iguration Ping €LP < Back	Apply
Cito Sontrol Control Control Control Control Control Control Control Control Control Control Control Control Control C	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	当端的规则 CONTROLLER WIRELESS CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address 172.16.1.1	A Linis Norton / Save Conf COMMANDS H	Antilikus 🚱 • Iguration Ping r∈LP < Back	Apply
Client Exclusion Policies Access Control Lists Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Policies Access Control Lists Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection Web Login Page CIDS Sensors Shunned Clients	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	¹ 端的规则 CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address 172.16.1.1 172.16.1.1	Linis Norton / Save Conf COMMANDS H	Antilikus 🚱 • Iguration Ping ELP < Back	Apply
City of the second seco	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	当端的规则 CONTROLLER WIRELESS CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address	o Linis Norton / Save Conf COMMANDS H	Antilikus <table-cell> • Iguration Ping ELP</table-cell>	Apply
Construction Co	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	¹ 端的规则 CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address	O Linis Norton / Save Conf COMMANDS H Netmask 255.255.255.255	Antilikus <table-cell> •</table-cell>	Apply
Control Control Control of the second	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	¹ 端的规则 CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address 172.16.1.1 IP Address 172.16.1.1	Ave Conf Save Conf COMMANDS H Netmask 255.255.255.255	Antilikus 🚱 • Iguration Ping r∈LP < Back	Apply
Cite Control Lists Control Lis	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	¹ 端的规则 CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	IP Address	Linis Norton / Save Conf COMMANDS H Netmask 255.255.255.255	Andilvirus 😧 • Inguration Ping ELP <back< td=""><td>Apply</td></back<>	Apply
Construction Co	MONITOR WLANS MONITOR WLANS Access Control Lis Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	¹ 端的规则 CONTROLLER WIRELESS ts > Rules > New 4 Any ♥ IP Address ♥ UDP ♥ Any ♥ Inbound ♥ Permit ♥	SECURITY MANAGEMENT	COMMANDS H Netmask 255.255.255	Antilikus <table-cell> • Isguration Ping ELP</table-cell>	Apply

aca Stateme dia atha	MONITOR V	VLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	Save Confi COMMANDS HI	guration Ping	Logout Refr
ecurity	Access Cont	rol Lists > Rules > Nev	N			< Back	Apply
IAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AD Policies	Sequence Source Destination Protocol	5 IP Address V Any V UDP	IP Addr 172.16	ess Ne 1.1 2	tmask 55.255.255.255		
Iccess Control Lists	Source Port	DNS	~				
Veb Auth Certificate Vireless Protection Volicies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection Veb Login Page CIDS Sensors	Destination Por DSCP Direction Action	t Any v Any v Cutbound v Permit v					
Shunned Clients							

net Station	MONITOR WLANS	CONTROLLER WIRELES	S SECURITY MANAGEMI	Save Con ENT COMMANDS H	iguration Ping HELP	Logout Refres
Security	Access Control List	s > Rules > New			< Back	Apply
AAA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Sequence Source Destination Protocol	6 Any 💌 IP Address 💌 TCP 💌	IP Address 172.18.0.0	Netmask 255.255.0.0]	
Access Control Lists	Source Port	Any 🔛				
Web Auth Certificate	De ational de Dant					
Wireless Protection Policies Trusted AP Policies Roque Policies Standard Signatures Custom Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	Destination Port DSCP Direction Action	Teinet 💌 Any 💌 Inbound 🛩 Permit 💌				
Web Login Page CIDS Sensors Shunned Clients						
Aller Hills I Aller and	and an abula					

						-				and an		-
ecunity	Acces	s Contro	ol Lists > Edit						< Back		Add New	Rule
IAA	Gene	ral										
RADIUS Authentication RADIUS Accounting	Access List Name Guest-ACL											
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Seq	Action	Source IP/Mas	k	Destination IP/Mask		Protocol	Source Port	Dest Port	DSCP	Direction	
	1	Permit	0.0.0.0	/	172.16.1.1 255.255.255.255	1	UDP	DHCP Client	DHCP Server	Any	Inbound	Edit Remove
cess Control Lists	2	Permit	172.16.1.1 255.255.255.255	/	0.0.0.0	1	UDP	DHCP Server	DHCP Client	Any	Outbound	Edit Remove
reless Protection licies	з	Permit	0.0.0.0	/	0.0.0.0	1	ICMP	Any	Any	Any	Any	Edit Remove
rusted AP Policies ogue Policies	4	Permit	0.0.0.0	/	172.16.1.1 255.255.255.255	1	UDP	Any	DNS	Any	Inbound	Edit Remove
Custom Signatures Signature Events	5	Permit	172.16.1.1 255.255.255.255	/	0.0.0.0	/	UDP	DNS	Any	Any	Outbound	Edit Remove
Summary Client Exclusion Policies AP Authentication / MFP Management Frame Protection	6	Permit	0.0.0.0	/	172.18.0.0 255.255.0.0	/	TCP	Any	Teinet	Any	Inbound	Edit Remove
	7	Permit	172.18.0.0	1	0.0.0.0	1	TCP	Teinet	Any	Any	Outbound	Edit

Shunned Clients

Done 🔁

编辑页面列出为ACL定义的所有规则

- 4. ACL 创建后,需要应用到动态接口。为了应用 ACL,请选择 Controller > Interfaces 并且编辑 您要应用 ACL 的接口。
- 5. 在动态接口的 Interfaces > Edit 页,从 Access Control Lists 下拉菜单中选择适当的 ACL。下面是一个示例。

3 · 🕤 🖻 🖻	🕼 🔎 🛧 🚱 🙆 👌	Address 1/172.16.1.40/so	reens/fra 🛩 🛃 Go	Links Nort	on AntiVirus 😫 🔹	
area Storeau				Save C	onfiguration Ping	Logout Refre
A. A.	MONITOR WLANS CONTR	OLLER WIRELESS SECURITY	MANAGEMENT	COMMANDS	HELP	
Controller	Interfaces > Edit				< Back	Apply
General Inventory	General Information					
nterfaces	Interface Name G	uest				
Internal DHCP Server Mobility Management	Interface Address					
Mobility Groups Mobility Statistics	VLAN Identifier	1				
Ports	IP Address	172.19.1.10				
Master Controller Mode	Netmask	255.255.0.0				
Network Time Protocol	Gateway	172.19.1.50				
205 Profiles	Physical Information					
	Port Number	1				
	Configuration					
	Quarantine					
	DHCP Information					
	Primary DHCP Server	172.16.1.1				
	Secondary DHCP Server					
	Access Control List					
	ACL Name	Guest-ACL V				
	Note: Changing the Interface pa temporarily disabled and thus m some clients.	rameters causes the WLANs to be ay result in loss of connectivity for				
1			10470212-0347	630 I I	int 🕲 Int	ernet

从Access Control List菜单中选择适当的ACL

完成后,ACL 允许或拒绝使用此动态接口的 WLAN 上的数据流(根据配置的规则)。接口 ACL 只能在连续模式中应用到 H-Reap AP,而非独立模式。

注意:本文档假设已配置WLAN和动态接口。请参阅<u>在无线LAN控制器上配置VLAN</u>或有关如 何在WLC上创建动态接口的信息。

配置 CPU ACL

以前,WLC 上的 ACL 没有选项来过滤发送到管理和 AP 管理器接口的 LWAPP/CAPWAP 数据流、 LWAPP/CAPWAP 控制数据流和移动数据流。为了解决此问题并过滤 LWAPP 和移动数据流 ,WLC 固件版本 4.0 引入了 CPU ACL。

CPU ACL 的配置包括两个步骤:

- 1. CPU ACL 的配置规则。
- 2. 在 WLC 上应用 CPU ACL。

CPU ACL的规则必须配置与其他ACL类似。

验证

Cisco 建议您使用无线客户端测试您的 ACL 配置以确保正确配置。如果它们无法正常运行,请验证 ACL网页上的ACL,并验证您的ACL更改是否已应用到控制器接口。

您也可使用这些 show 命令验证您的配置:

• **show acl summary** — 为了显示在控制器上配置的 ACL,请使用 show acl summary 命令。示 例如下:

(Cisco Controller) >show acl summary

ACL Name	Applied
Guest-ACL	Yes

• **show acl detailedACL_Name** — 显示有关已配置ACL的详细信息。示例如下: (Cisco Controller) > **show acl detailed Guest-ACL**

	Source	Destination	S	Source Port
Dest Por	t			
I Dir	IP Address/Netmask	IP Address/Netmask	Prot	Range
Range	DSCP Action			
1 In	0.0.0/0.0.0.0	172.16.1.1/255.255.255.255	17	68-68
67-67	Any Permit			
2 Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	67-67
68-68	Any Permit			
3 Any	0.0.0/0.0.0.0	0.0.0/0.0.0.0	1	0-65535
0-65535	Any Permit			
4 In	0.0.0/0.0.0.0	172.16.1.1/255.255.255.255	17	0-65535
53-53	Any Permit			
5 Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	53-53
0-65535	Any Permit			
6 In	0.0.0/0.0.0.0	172.18.0.0/255.255.0.0		60-65535
23-23	Any Permit			
7 Out	172.18.0.0/255.255.0.0	0.0.0/0.0.0.0	б	23-23
0-65535	Any Permit			

• **show acl cpu** — 为了显示 CPU 上配置的 ACL,请使用 show acl cpu 命令。示例如下: (Cisco Controller) > **show acl cpu**

CPU Acl Name..... CPU-ACL Wireless Traffic..... Enabled Wired Traffic..... Enabled

故障排除

控制器软件版本4.2.x或更高版本允许您配置ACL计数器。ACL计数器可帮助确定哪些ACL应用于通 过控制器传输的数据包。当您对系统进行故障排除时此功能非常有用。

ACL 计数器在这些控制器上可用:

- •4400 系列
- Cisco WiSM
- Catalyst 3750G 集成无线局域网控制器交换机

- 1. 选择 Security > Access Control Lists > Access Control Lists 以打开 Access Control Lists 页。 此页列出了为此控制器配置的所有 ACL。
- 2. 要查看数据包是否命中控制器上配置的任何ACL,请选中Enable Counters复选框并单击 Apply。否则,请保留复选框空白。这是默认值。
- 3. 如果要清除 ACL 的计数器,将光标停留在该 ACL 的蓝色下拉箭头上,并选择 Clear counters。

相关信息

- Cisco 无线 LAN 控制器配置指南 6.0 版
- 在无线局域网控制器上配置VLAN
- 排除轻型 AP 无法加入 WLC 的问题
- <u>思科技术支持和下载</u>

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)。