无线控制器ACL配置实例

文档 ID: 71978

介绍 前提 要求 使用的设备 惯例 **无线控制器ACL** 无线控制器ACL 无线控制器上配置ACL需注意 配置无线控制器ACL 配置允许访客用户服务的规则 配置CPU的ACL 验证 排障 NetPro论坛 - 特殊的会话

相关信息

介绍

本文档介绍如何在无线控制器(WLC)上配置访问控制列表(ACL)来过滤进入和离开无线局域网的 流量。

前提

要求

在尝试配置前,确保你满足如下的要求:

- 具备配置无线控制器和轻量级无线接入点进行基本工作的知识
- 具备轻量级无线接入点协议(LWAPP)和无线安全方法的基本知识

使用的设备

本文档中的信息基于如下的软件和硬件版本:

- 思科2000系列无线控制器,固件版本4.0
- 思科1000系列轻量线无线接入点
- 思科802.1 1a/b/g无线网卡,固件版本2.6
- 思科Aironet Desktop Utility (ADU),版本2.6

本文档中的信息来自特定实验环境的设备。文档中所有的相关设备都是从默认配置开始的。如果你的网络环境是在线的,确保要了解任何一条命令的潜在影响。

要了解更多文档惯例的信息,请参见思科技术提示惯例。

无线控制器ACL

无线控制器上的ACL用于限制或允许无线客户端访问无线局域网内的服务。

在无线控制器固件版本4.0之前,ACL在Management Interface上是旁路的,所以你不能影响去往无线控制器的流量,除非通过Management Via Wireless的选项来避免无线客户端管理控制器。因此,ACL只能用于动态的Interface。在无线控制器固件版本4.0中,有CPU ACL可以过滤去往Management Interface的流量。如何配置CPU ACL的例子稍后会在文档中列出。

你可以定义最多64个ACL,每个ACL最多64条规则。每条规则有影响行为的参数。当一个数据包匹配了一条规则的所有参数,相应的行为就会运用到这个数据包上。你可以通过GUI或CLI配置ACL。

在配置无线控制器ACL前,你需要了解一些规则:

- 如果源和目的都是any,则这个ACL的方向可以是any.
- 如果源或目的之一不是any, 那么过滤器的方向必须指定,并且反方向的相反语句必须定义。
- 无线控制器的inbound和outbound方向概念并非直观上的。它是从无线控制器面向无线客户端的角度 看的,并非从无线客户端的角度。因此,inbound方向是指数据包从无线客户端进入无线控制器, outbound方向是指数据包从无线控制器出去到无线客户端去。
- 在ACL的末尾有隐式的deny。

无线控制器上配置ACL需注意

无线控制器上的ACL与路由器上的工作是不一样的。当你在无线控制器上配置ACL时,有一些事项 要注意:

- 当你想要拒绝或允许IP的数据包时,最常见的错误是选择IP。因为你选择的是IP数据包里面的内容, 这样就导致拒绝或允许IP数据包内的IP信息。
- 控制器的ACL无法禁止1.1.1.1(virtual IP地址),因此无法禁止无线客户端的DHCP包。
- 控制器的ACL无线禁止组播和广播的数据包,因为这些包是发送到无线接入点的management interface上的。
- 不像路由器那样,ACL应用到端口上后会控制双向的流量。如果你忘记了在回来的数据流的ACL 上打开策略,就会导致出问题。
- 控制器的ACL只能禁止IP数据包。你不能禁止2层的ACL或3层的非IP的数据包。
- 控制器的ACL不像路由器那样用反掩码。在这里,255的意思是完全匹配IP地址的8位数字。
- 控制器的ACL是由软件实现的。

配置无线控制器ACL

本章节描述如何在无线控制器上配置ACL。目标是配置ACL允许访客访问如下的服务:

- 无线客户端与DHCP服务器之间的DHCP数据
- 网络中所有的设备之间的ICMP数据
- 无线客户端与DNC服务器之间的DNS数据

• Telnet服务到特定的子网

无线客户端的所有其他服务都必须被禁止。根据如下步骤,用无线控制器GUI配置ACL:

1. 进入无线控制器GUI,选择 Security > Access Control Lists.

Access Control Lists的页面显示出来。这个页面上列出了在无线控制器上配置的ACL,你也可以 编辑或删除任何一个ACL。创建一个新的ACL,点击 New.

G · O · E Ø	6 P + 8 6.	Address 🔊 https	r://172.16.1.40/sc	reens,fre 👱 🛃 Go	Links Norton Ani	alinus 😫 •	🔊 – 8 ×
Cerco Sverran	MONITOR WLANS COM	ITROLLER WIRELESS	SECURITY	MANAGEMENT	Save Config COMMANDS HE	uration Ping	Logout Refresh
Security	Access Control Lists						New
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 Summary Client Evolusion Policies AP Authentication / MFP Management Frame Protection							
Web Login Page							
CIDS Sensors Shunned Clients							
8)	CERTAIN PLANTS FO	252.00.5159.5505	REAL PROPERTY			🕲 Inte	rnet

2. 输入ACL的命名,点击 Apply.

你可以输入最多32个字母数字的字符。在这个例子中,ACL的命名是 Guest-ACL. ACL 创建之后,点击 Edit 来为ACL创建规则。



3. 当 Access Control Lists > Edit 的页面显示出来,点击 Add New Rule. 则

Access Control Lists > Rules > New 的页面显示出来。

3 · 0 · 2	6 Pt.	🛛 🗟 · 🚴 "	Address 1 Mtps:	//172.16.1.40/so	eens,fire 🛩	🔁 Go	Linia	Norton Antilla	us 😵 •	<u>र्थ</u> – 8 ×
Canca Syntama	Contraction of the	States and the states	A REAL PROPERTY AND				S	ave Configura	ition Ping Li	ogaut Refresh
A. h. march	MONITOR W	LANS CONTROLL	ER WIRELESS	SECURITY	MANAG	EMENT	сомма	NDS HELP	nied certificate	
Security	Access Contr	ol Lists > Edit					1	< Back	Add New	Rule
AAA	General									
RADIUS Authentication RADIUS Accounting	Access List Nam	Guest-AC	-							
Local Net Users MAC Filtering	Seq Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest	DSCP	Direction		
Disabled Clients User Login Policies AP Policies										
Access Control Lists										
Web Auth Certificate										
Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Gustam Signatures Summary Client Exclusion Policies AP Authentication / MPP Management France Protection										
Web Login Page										
Sensors Shunned Clients										
Done	THE STORES		U.S. COM						🜍 interne	t

- 4. 配置允许访客用户访问如下服务的规则:
 - 无线客户端与DHCP服务器之间的DHCP数据
 - 网络中所有的设备之间的ICMP数据
 - 无线客户端与DNC服务器之间的DNS数据
 - Telnet服务到特定的子网

配置允许访客服务的规则

本章节举例说明如何为如下的服务配置规则:

- 无线客户端与DHCP服务器之间的DHCP数据
- 网络中所有的设备之间的ICMP数据
- 无线客户端与DNC服务器之间的DNS数据
- Telnet服务到特定的子网
- 1. 为了配置DHCP服务的规则,选择源和目的的IP地址范围。

在这个例子中源地址用 **any**,表示任何无线客户端都可以访问到DHCP服务器。在这个例子中,服务器172.16.1.1作为DHCP和DNS服务器。因此,目的IP地址是172.16.1.1/255.255.255.255 (使用主机的掩码).

Because DHCP is a UDP based protocol,因为DHCP是基于UDP的协议,因此在Protocol的下拉菜单中选择 UDP。如果你在前一步中选择TCP或UDP,2个附加的参数显示出来:源端口

和目的端口。指定源端口和目的端口。在这条规则中,源端口是 DHCP Client 而目的端口 是 DHCP Server.

选择ACL应用的方向。因为这条规则是用于从客户端到服务器,这里选择 Inbound. 在Action 的下拉菜单中,选择 Permit 使这个ACL允许从无线客户端到DHCP服务器的DHCP包。默认的 参数是Deny。点击 Apply.

ince Statter	Contraction of the second		In the local design of the	Save Confi	guration Ping Logout Refres
A. A. Margarette	MONITOR WLANS	CONTROLLER WIRELES	SS SECURITY MANAGEM	ENT COMMANDS H	ELP
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	1 Any V IP Address V UDP V	1P Address 172-16-1-1	Netmask 255.255.255.255	
Access Control Lists	Source Port	DHCP Client			
Web Auth Certificate	Destination ford	France Party and			
Wireless Protection	Destination Port	DHCP server			
Trusted AP Policies Rogue Policies	DSCP	Any 🖌			
Standard Signatures Custom Signatures	Direction	Inbound 👻			
Signature Events Summary Client Exclusion Policies AP Authentication / MIP Management Frame Protection	Action	Permit 💌]
Web Login Page					
CIDS Sensors Shunned Clients					

如果源或目的之一不是 any, 那么反方向的相反语句必须定义。如下是例子。

Ance Statement	MONITOR WLANS	CONTROLLER WIRELES	ss security manage	Save Conf MENT COMMANDS H	iguration Ping	Logout Refres
Security AAA General RADIUS Authentication RADIUS Aucounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Polisies Access Control Lists Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rague Policies Standard Signatures Signature Events Summary Client Exclusion Policies AP Authentication / MIP Management Frame Protection Web Login Page CIDS Sensors Shunned Clients	Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	s > Rules > New 2 IP Address Any UDP UDP DHCP Server DHCP Client Any Outbound Permit	IP Address 172.16.1.1	Netmask 255.255.255	< Back	Apply

2. 为了定义允许所有设备之间的ICMP包的规则,在源和目的中选择 any,这是默认的参数。

在Protocol的下拉菜单中选择 ICMP 。因为这个例子中源和目的都选择了 any ,你可以不指定 方向,可以用默认的参数 any 。并且,反方向的相反语句也不需要。

在Action的下拉菜单中,选择 Permit 使这个ACL允许所有设备之间的ICMP数据包。点击Apply.

G · O · E	6 P * 0	Address	https://172.16.1.40	lscreens,fire 🗙 🛃 Go	Links No	orton Anklivirus 🙆 •	💐 - 8 ×
Casca Stattan	Constanting of the	ACCOUNTS OF A DESCRIPTION OF A DESCRIPTI	CHARLEN CHARLES		Save	Configuration Ping	Logout Refresh
A. A. Bernsteine	MONITOR WLANS	CONTROLLER W	IRELESS SECURIT	Y MANAGEMENT	COMMANDS	HELP	STATE OF BELLEVILLE
Security	Access Control List	s > Rules > New				< Back	Apply
AAA General	Sequence	3					
RADIUS Authenticetion RADIUS Accounting Local Net Users	Destination	Any 💌					
MAC Filtering Disabled Clients User Login Policies	Protocol	ICMP	×				
AP Pelicies Access Control Lists	DSCP	Any 💌					
Web Auth Certificate	Direction	Any 👻					
Wireless Protection Policies Trusted AP Policies	Action	Permit					
Rogue Policies Standord Signatures Custom Signatures Summary Client Exclusion Policies AP Authonitoston / MTP Management Frame Protection							
Web Login Page							
CIDS Sensors Shunned Clients							
Done		STREET, POST		DECKIA SCIENC		ini 🌒	ernet

3. 类似的,为允许无线客户端的DNS服务和Telnet到特定的子网创建规则。如下是配置举例。

ANDION	nes Brattan	Service of the service of the	Contraction of the second second	and the second second	Save Confr	guration Ping	Logout Re
Script Amount	A. A.	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGE	MENT COMMANDS H	ELP	and the second
American Barrow Bar	ecurity	Access Control Lis	ts > Rules > New			< Back	Apply
	AA	Sequence	4				
Address Workshow Address <td>General RADIUS Authentication</td> <td>Source</td> <td>Any 🔛</td> <td></td> <td></td> <td></td> <td></td>	General RADIUS Authentication	Source	Any 🔛				
	ADJUS Accounting Local Net Users NAC Filtering	Destination	IP Address 👻	IP Address 172.16.1.1	Netmask 255.255.255.255		
	Disabled Clients User Legin Palicies AP Policies	Protocol	UDP 💌				
Provide State	xess Control Lists	Source Part	Any 💌				
Normal Strategy Strategy <t< td=""><td>reless Protection</td><td>Destination Port</td><td>DNS 💌</td><td></td><td></td><td></td><td></td></t<>	reless Protection	Destination Port	DNS 💌				
Provense light for the former of the former	rusted AP Policies	DSCP	Any 💌				
	Standard Signatures	Direction	Inbound 🐱				
A backgened frage be be be be be be be be be b	lignature Events Jummary Jient Exclusion Policies	Action	Permit 💌				
handban Bearden Bearden Bearden Bearden Bearden Control Lists Control Lis	IP Authentication / MFP Rahagement Frame						
ex Login Property Control Lists Provide States Control Lists Provide States Control Lists Provide States Control Lists Provide States Control Lists Provide States Control Lists Control	Protection						
Preserve Preserve Image: Preserve Image: Preserve Image: Preserve Image: Preserve Image: Preserve Image: Preserve Image: Preserve Image: Preserve Image: Preserve <	eb Login Page DS						
Andread Ceens Image: Control Lists Andread Antonication Antonication Antonication <	Sensors						
Control Lists Automation	sintelied mediata						
Image: Second Lists And control Lists Second Lists							
Image: Second Displayer Image: Seco							
Image: Control Lists Control Lists <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
Control Lass > Rules > Nov							
Control Lists Control C							
All and all all all all all all all all all al		1				and test	(ma)
And the control discovered by the							
Address							
A defension of the set	3 · 🖸 📓 📓	6 P + 8	🗟 • 🍓 🕺 Address 🕘 https:	//172.16.1.40/screens/fre 🛩	🔁 Go Links Norton A	ntiffrus 🚱 -	- N
NUMBER WANG CONTROLLER WERLES SECURITY MANAGEMENT COMMANDS HEIM	ics Stattan		And I have been added	and some state of the second	Save Confe		
Access Control Lists > Rules > New Sequence MADUS Account of Lists > Rules > New Sequence Source IP Address IP Address New Sequence Source IP Address IP A	A A DESCRIPTION					sumstam Ping	Logout Re
A A Constral LACDUS Authonitation LACDUS Authonitation LACDUS Authonitation LACDUS Authonitation MAC Tilerag Destination Any V Protocol UDP V Source Port Dest Source Port Dest Source Port Dest Source Port Dest Destination Port Any V Destination Port Any V		MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGER	MENT COMMANDS H	puration Ping ELP	Logout Re
Address Netmask NacNus Authentication Source IP Address Netmask NacNus Authentication Any Intelline Intelline NacNus Action Protocol UDP Intelline Intelline NacNus Action NacNus Action NacNus Action NacNus Action NacNus Action NacNus Action Naction NacNus Action NacNus	scurity	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGER	MENT COMMANDS H	puration Ping	Logout Re
NACUEY Accounting Joe Lagin Policies Proficies Cess Control Lists ceb Auth Certificate Incless Protection Rices Randard Stignatures Surtice Signatures Surtice Signatures Surtice Page DS Bensors Dsmined Clients	curity	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGER	MENT COMMANDS H	puration Ping ELP < Back	Apply
Waching Ser Login Policies Ar Policies Ar Policies Costs Control Lists eb Auth Certificate Interses Protection Interses Protection Source Port DSCP Any DSCP Any DSCP Cinetions Outbound Action	ccurity LA General NADIUS Authentication	MONITOR WLANS Access Control List Sequence Source	CONTROLLER WIRELESS	P Address	MENT COMMANDS H	curation Ping ELP < Back	Apply
VP Policies ccss Control Lists eb Auth Certificate irreless Protection icics forgue Relicies control Lips icics icics irreless Protection icics control Lips icics icics irreless Protection icics icics control Lips icics icics icics control Lips icics icics icics control Lips icics icics icics icics icics icits	curity IA Janeral ADIUS Authentication IADIUS Accounting Jocal Net Users	MONITOR WLANS Access Control List Sequence Source Destination	CONTROLLER WIRELESS ts > Rules > New S IP Address V Any V	IP Address 172.16.1.1	MENT COMMANDS H Netmask 255.255.255.255	puration Ping ELP < Back	Apply
Cerso Control Cisco ebb Auth Cericita ebb Auth Cericita increases Protection licies ioguar Palisios OS Persors ioguar Palisios	curity A Janeral IADIUS Authentication IADIUS Accounting Jocal Net Users Mac Filtering Is abled Clients Iser Login Policies	MONITOR WLANS Access Control List Sequence Source Destination Protocol	CONTROLLER WIRELESS ts > Rules > New 5 1P Address V Any V UDP V	IP Address 172.16.1.1	MENT COMMANDS H Netmask 255.255.255.255	guration Ping ELP < Back	Apply
Inteless Protection	curity A Jeneral ADUS Authentication IADUS Accounting ocal Net Users MC Filtering Neabled Clients Iser Login Policies P Policies	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W UDP VIDP VIDP VIDP VIDP VIDP VIDP VIDP VIDP VIDP VIDP VIDP VIDP VIDE	IP Address 172.16.1.1	MENT COMMANDS H	guration Ping ELP < Back	Apply
Irusted AP Policies Isopus Policies Sundard Signatures Untom Signatures Sonature Events Untom Policies Action Permit V Athenbican / MPP Basgement Frame ratection Bellogin Page DS Bensors Bunned Clients	curity A Janoral IADIUS Authentication IADIUS Accounting acal Net Users IAC Filtering Neabled Clients Iser Login Policies Prolocies cess Control Lists eb Auth Certificate	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port	CONTROLLER WIRELESS ts > Rules > New S IP Address ♥ Any ♥ UDP ♥ DNS ♥ Any ♥	IP Address 172.16.1.1	MENT COMMANDS H Netmask 255.255.255.255	curation Ping ELP < Back	Apply
Action Permit M Justam Signatures Justam Signatures Action Permit M International Signatures Action Permit M Action Permit M International Signatures Permit M International Signatures Action Permit M International Signatures International Signatures International Signatures Action Permit M International Signatures International Signatures	A Jeneral ADUS Authentication ADUS Accounting ocal Net Users AC Fibering Neabled Clients Iser Login Policies P Policies cess Control Lists eb Auth Certificate reless Protection licies	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port Destination Port	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W DNS W Any W Any W	IP Address 172.16.1.1	MENT COMMANDS H	guration Ping ELP < Back	Apply
Defensive Events Internary Authenticetion / MPP Kanagement Frame Pratection eb Login Page DS Enumed Clients	curity A Seneral ADJUS Authentication ADJUS Accounting Joad Net Users AC Filtering Joad Hot Cients Seer Loain Policies Policies cess Control Lists eb Auth Certificate irreless Protection ficies Irrusted AP Policies Trusted AP Policies	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction	CONTROLLER WIRELESS IS > Rules > New S IP Address M Any M UDP ONS Any M Any M Cutbound M	P Address 172.16.1.1	MENT COMMANDS H	eurstion Ping- ELP < Back	Apply
Automation / MPP Anagement Frame Protection eb Legin Page DS Jensors Journed Clients	ccurity LA Seneral ADDUS Authentication ADDUS Authentication ADDUS Accounting acal Net Users ACC Fibering Nisabled Clients Ser Login Policies Prolicies cess Control Lists eb Auth Certificate ircless Protection licies Irusted AP Policies Togue Policies Trasted AP Policies	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address ♥ Any ♥ UDP ENS Any ♥ Any ♥ Cutbound ♥ Russeit ■	IP Address 172.16.1.1	MENT COMMANDS H	euration Ping 	Apply
Acogeneer Frame Pratection DS Eensors ENunned Clients	A Curity A Control Automication ADDIUS Automication ADDIUS Accounting ADDIUS Accounting ADDIUS Accounting ACC Fibering Divabled Clents Ser Loain Policies AP Policies AP Policies Excess Control Lists eb Auth Certificate Irreless Protection Micles Trusted AP Policies Rogue Policies Sandard Signatures Custom Signatures Signature Events Signature Events Signature Events	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address V Any V UDP V DNS V Any V Corbound V Permit V	SECURITY MANAGER	MENT COMMANDS H	eurstion Ping 	Apply
eb Login Page DS Ensors Enunned Clients	Accurity A Constant Const	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W UDP UDP V DNS Any W Cutbound W Permit W	IP Address 172.16.1.1	MENT COMMANDS H	eurstion Ping ELP < Back	Apply
DS Sensors Seturned Clients	AA General RADIUS Authentication RADIUS Activentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clents User Login Policies AP Policies ccess Control Lists eb Auth Certificate licess Protection licites Trusted AP Policies Rogues Policies Standard Signatures Custom Signatures Standard Signatures Summary Client Exclusion Policies AP Authentication / MFP Ranagement Frame Protection	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address M Any W UDP V DNS Any W Any W Outbound M Permit W	IP Address 172.16.1.1	MENT COMMANDS H	eurstion Ping ELP < Back	Apply
Sensors Shunned Clients	AA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clents User Login Policies AP Policies Cress Control Lists Trated AP Policies Rogue Policies Standard Signatures Standard Signatures Summary Clent Exclusion Policies AF Authentication / NPP Repagement Frame Pratection Teb Login Page	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W UDP UDP V DNS Any W Cutbound W Permit W	IP Address 172.16.1.1	MENT COMMANDS H	eurstion Ping ELP < Back	Αρρίγ
	ecurity AA General RADIUS Authentication RADIUS Accounting Local Net Users MAC filtering Disabled Clents User Login Policies AP Policies Cress Control Lists Vab Auth Certificate Arieless Protection Olicies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Summary Client Exclusion Policies AP Authentication / HPP Napagement Prame Pratection Creb Login Page IDS	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W UDP UDP V DNS Any W Cutbound W Permit W	SECURITY MANAGER	MENT COMMANDS H	surstion Ping ELP < Back	Αρρίγ
	ecurity AA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Fibering Disabled Clients User Login Policies AP Policies Cress Control Lists Creb Auth Certificate Arieless Protection afficies Rogue Policies Rogue Policies Rogue Policies Summary Client Exclusion Policies Sumary Client Exclusion Policies AP Authentication / APP Management Frame Protection Creb Lagin Page IDS Sensors	MONITOR WLAVIS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W UDP UDP V DNS Any W Cutbound W Permit W	SECURITY MANAGER	MENT COMMANDS H	eurstion Ping ELP < Back	Apply
	AA General RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Divabled Clients User Login Policies AP Policies AP Policies Costs Control Lists Veb Auth Certificate Vireless Protection Officies Trusted AP Policies Rogue Policies Standard Signatures Signature Events Summary Client Exclusion Policies Signature Events Summary Client Exclusion Policies AP Authenticetion / NPP Management Frame Pratection Veb Login Page CIOS Sensors Sound Clients	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address ♥ Any ♥ UDP V DNS Any ♥ Any ♥ Cutbound ♥ Permit ♥	SECURITY MANAGER	MENT COMMANDS H	eurstion Ping ELP < Back	Apply
	ecurity AA General RADIUS Authentication RIDIUS Accounting Local Net Users MAC Fibering Disabled Clients User Login Policies AP Policies CCESS Control Lists robe Auth Certificate Vireless Protection dicices Trusted AP Policies Rogue Policies Standard Signatures Signature Events Signature Events Signature Events Signature Events Signature Events Signature Events Signature France Protection Veb Login Page IDS Sensors Shunned Clients	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address ♥ Any ♥ UDP V DNS Any ♥ Cutbound ♥ Permit ♥	P Address 172.16.1.1	MENT COMMANDS H	eurstion Ping ELP < Back	Apply
	ecurity AA General RADIUS Authentication RADIUS Activentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Cecss Control Lists Veb Auth Certificate Arreless Protection olicies Arrated AP Policies Reque Pelicies Standard Signatures Signature Events Signature Events Signature Events Signature Events Signature Events Signature Frame Protection Collent Exclusion Policies AP Automiscition / MPP Management Frame Protection	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W UDP DNS Any W Cutbound W Permit W	P Address 172.16.1.1	MENT COMMANDS H	eurstion Ping ELP < Back	Apply
	ecurity AA General RADIUS Authentication RADIUS Acthentication RADIUS Acthentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Ccess Control Lists Veb Auth Certificate Arietes Protection Client Exclusion Policies AP Autentication Policies Summary Cient Exclusion Policies AP Autentication / MPP Menagement Frame Protection	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address W UDP UDP UDP W Any W Cutbound W Permit W	P Address 172.16.1.1	MENT COMMANDS H	euration Ping	Apply
	ecurity AA General RADIUS Authentication RADIUS Authentication RADIUS Active Isolabled Clents User Login Policies AP Policies ccess Control Lists reb Auth Certificate Arteless Protection olicies Trusted AP Policies Regue Pelicies Standard Signatures Custom Signatures Signature Events Signature Events Signature Events Signature Events Signature Frame Protection (to Login Page Ebunned Clents	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address M UDP UDP ONS Any Outbound M Permit M	IP Address 172.16.1.1	MENT COMMANDS H	eurstion Ping	Apply
	AA General RADIUS Authentication RADIUS Authentication RADIUS Action local Net Users MAC Filtering Disabled Clents User Login Policies AP Policies ccess Control Lists reb Auth Certificate (incless Protection blicies Trusted AP Policies Regues Policies Standard Signatures Signature Events Signature Events Signature Events Signature Events Signature Events Signature Events Signature Frame Protection (bb Login Page Dunned Clents)	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address M UDP UDP V DNS Any Outbound W Permit W	IP Address 172.16.1.1	MENT COMMANDS H	eurstion Ping	Apply
	curity A Jeneral JaDUS Authentication (ADUS Accounting acal Net Users Mac Filtering Nabled Clients See Login Policies Prolocies cess Control Lists de bath Certificate de bath Certificate insted AP Policies candard Signatures Signature Events Jummary Lient Exclusion Policies P Authentication / NPP Kabagement Frams rutection et Login Page DS Jensors Jumned Clients	MONITOR WLANS Access Control List Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	CONTROLLER WIRELESS IS > Rules > New S IP Address W Any W UDP ONS Any W Cutbound W Permit W	P Address 172.16.1.1	MENT COMMANDS H	eurstion Ping	Apply

定义这条规则,允许无线客户端的Telnet服务。

1 Bratama	Start Little Start Startes					
all algebra	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEME	NT COMMANDS H	€LP	Silver and all
urity	Access Control Lists	>Rules > New			< Back	Apply
	Sequence	6				
meral DIUS Authentication	Source	Any 💌				
ACTION Accounting scal Net Users AC Filtering	Destination	IP Address 💌	IP Address 172.18.0.0	Netmask 255.255.0.0		
sabled Clients ser Login Policies P Policies	Protocol	тср				
ess Control Lists	Source Port	Any 💌				
b Auth Certificate	Destination Post	Talaat				
eless Protection cles	Cresumentin Port	Teines				
usted AP Policies igue Policies	DSCP	Any 😪				
andard Signatures istom Signatures	Direction	Inbound 😪				
gnature Events Immary	Action	Permit 🐱				
Authentication / MFP hagement Frame					-	
otection h Login Rage						
is countrage						
ensors						
numped converses						
ttps://172.16.1.40/screens/b	an a				e int	ernet
ttps://172.16.1.40/screens/b	erce Juli	· P * Atten Stur	10173 16 1 40/segger (Fr. 10)	50 Links Bioston	 Jub Antibio (19) 	ernet 🎊 -
ttps://172.16.1.40/screens/bx	arner Itali	🕉 • 🍓 🍟 Address 👰 https	://172.16.1.40/screens/fire 💙 💽	Go Links ³⁹ Norton J Save Conf	andsilvirus 🥸 • Inguration Ping	ernet
tps://172.16.1.40/screens/b) - 🕑 - 💌 🙆	NONITOR WLANS	CONTROLLER WIRELESS	://172.16.1.40/screens/Fite <table-cell> 💽 SECURITY MANAGEME</table-cell>	Go Links ¹⁹ Norton J Save Conf NT COMMANDS H	antilikrus 🧐 - Inguration Ping HELP	ernet
tps://172.15.1.40/screena@u	Access Control Lists	Address Mtps	://172.16.1.40/screers,fire 😪 争 SECURITY MANAGEME	Go Links ^W Norton J Save Conf NT COMMANDS H	Antsilvirus 😵 • Inguration Ping IELP < Back:	ernet
tps://172.16.1.40/screens/bu	arner Jtail MONITOR WLANS Access Control Lists Sequence	Address Mttps CONTROLLER WIRELESS	://172.16.1.40/screens/fite <table-cell> 💽 SECURITY MANAGEME</table-cell>	Go Linis ³⁹ Norton Save Conf NT COMMANDS H	AndiVirus 😵 - Inguration Ping HELP < Back	ernet Logout 1 Apply
tps://172.16.1.40/screens/b • ② • 🔊 🔊 surity urity hereral pDUS Authentication	MONITOR WLANS Sequence Source	Address Mtps CONTROLLER WIRELESS > Rules > New 7 IP Address M	://172.16.1.40/screens/fire <table-cell> 💽 SECURITY MANAGEME IP Address 172.18.0.0</table-cell>	Go Linis ³⁹ Norton J Save Conf NT COMMANDS H Netmask 255.255.0.0	AntiWeus 😵 - Aguration Ping HELP Kack	ernet
tps://172.16.1.40/screens/b tps://172.16.1.40/screens/b top://lineral top://li	arrer. Itali MONITOR WLANS Access Control Lists Sequence Source Destination	Address Mittee CONTROLLER WIRELESS > Rules > New 7 IP Address M Any M	://172.16.1.40/screens/Fre V SECURITY MANAGEME IP Address 172.18.0.0	Go Links ^{III} Norton J Save Conf NT COMMANDS H Netmask [255.255.0.0	AndiVrus 😵 - Inguration Ping IELP C Back	ernet Apply
pri//172.16.1.40/screens/b pri//172.16.1.40/screens/b String String A brity crity crity brity crit	Access Control Lists Sequence Source Destination Protocol	Address Mtps CONTROLLER WIPELESS > Rules > New 7 IP Address M Any M TCP	IP Address 172-18-0-9	Go Linis ¹⁴ Norton J Save Conf NT COMMANDS H Netmask 255.255.0.0	AntSilveus 😵 - Inguration Ping KELP < Back	ernet
tps://172.16.1.40/screens/b tps://172.16.1.40/screens/b trainers/ trainers	Access Control Lists Sequence Source Destination Protocol Source Port	Address Mttps CONTROLLER WIPELESS > Rules > New 7 IP Address M Any TCP Teinet	IP Address	Go Links ^{**} Norton / Save Conf NT COMMANDS F Netmask 255.255.0.0	AndiVrus 😵 - Inguration Ping IELP	ernet Logoot I i Apply
tps://172.16.1.40/screens/b tps://172.16.1.40/screens/b trutity according to the second se	arner Atnië Control Lists Sequence Source Destination Protocol Source Port Destination Port	Address Mttps CCONTROLLER WIFELESS > Rules > New 7 IP Address V Any V TCP V Telnet	IP Address	Go Linis ³⁹ Norton J Save Conf NT COMMANDS H Netmask 255.255.0.0	AndiVeus 😵 • AndiVeus 😵 • Anguration Ping HELP	ernet Logout 1 Apply
ttps://172.16.1.40/screens/b ttps://172.16.1.40/screens/b Curity A aneral ADUS Authentication ADUS Authentication ADUS Accounting ADUS Accounting ADUS Accounting AC Filtering isabled Clients Ser Lagin Policies P Policies cress Control Lists to Auth Certificate release Protection licitas	Access Control Lists Sequence Source Destination Protocol Source Port Destination Part Destination Part	Address Mittes	IP Address 172.18.0.0	Go Linis ¹⁴ Norton J Save Conf NT COMMANDS H Netmask 255.255.0.0	Antibilitus 😵 - Inguration Ping IELP < Back	erret
ttps://172.16.1.40/screene@ ttps://172.16.1.40/screene@ Curity A A A A A A A A A A A A A	Arree. Itali MONITOR WLANS Access Control Lists Sequence Source Destination Protocol Source Port Destination Port Destination Port Destination Port	Address Mttps CCONTROLLER WIPELESS Rules > New 7 IP Address Any TCP Teinet Any X	://172.16.1.40/screens,fire V SECURITY MANAGEME IP Address 172.16.0.0	Ge Linis ¹⁰ Norton J Save Conf NT COMMANDS H Netmask 255.255.0.0	AntiVirus 😵 - Inguration Ping IELP	Armet
ttps://172.16.1.40/screens/b ttps://172.16.1.40/screens/b Content ttps://172.16.1.40/screens/b Content Con	Access Control Lists Sequence Source Destination Protocol Source Port Destination Port Destination Port Direction	Address Mittee CONTROLLER WIRELESS > Rules > New 7 IP Address M Any TCP Teinet Any M Outbound M	I/172.16.1.40/screens/fire V	Go Linés ^{**} Norton Save Conf NT COMMANDS F Netmask 255.255.0.0	AntiVirus 😵 - Inguration Ping HELP	erret Logout F Apply
ttps://172.16.1.40/screens/b ttps://172.16.1.40/screens/b Curity A eneral ADUS Authentication ADUS Accounting scal Net Users AC Fittering isabled Clients ser Login Palicies Prolocies tess Control Lists th Auth Certificate reless Protection Icles protection Control Lists th Auth Certificate reless Protection Icles protection Icles protection Icles protection Icles protection Icles protection Icles	Access Control Lists Sequence Source Destination Protocol Source Port Destination Port Destination Port Destination Port Direction Action	Address Mittee CONTROLLER WIPELESS > Rules > New 7 IP Address M Any TCP Telnet Any Outbound Permit M	IP Address 172.16.0.0	Go Linis ³⁹ Norton J Save Conf NT COMMANDS H Netmask 255.255.0.0	AndSWrus 😵 - AndSWrus 😵 - Inguration Ping HELP	ernet Logout A Apply
ttps://172.16.1.40/screena@ ttps://172.16.1.40/screena@ ttps://172.16.1.40/screena@ Curity A eneral ADRUS Authentication ADRUS Authentication ADRUS Authentication ADRUS Accounting country A curity A eneral ADRUS Authentication ADRUS Accounting country A Curity A curity Curity Curity A curity Curity	Access Control Lists Sequence Source Destination Protocol Source Port Destination Port Destination Port Direction Action	Address Mttps CCNTROLLER WIRELESS > Rules > New 7 IP Address M Any TCP Teinet Any Outbound Permit M	IP Address 172.18.0.0	Go Links ¹⁰ Norton / Save Conf NT COMMANDS + Netmask 255.255.0.0	AntiVirus 😵 - Inguration Ping IELP	Arnet
ttps://172.16.1.40/screena/b ttps://172.16.1.40/screena/b Comment ttps://172.16.1.40/screena/b ttps://inter- ttps://inter	Access Control Lists Sequence Source Destination Pratocol Source Port Destination Port Direction Action	Address Mittee CONTROLLER WIRELESS > Rules > New 7 IP Address M Any TCP Telnet Any Outbound Permit M	IP Address 172.16.0.0	Go Links ¹⁰ Norton / Save Conf NT COMMANDS F Netmask 255.255.0.0	AntiVirus 😵 - Inguration Ping HELP	Arriet Logout F Apply
ttps://172.16.1.40/screens/b ttps://172.16.1.40/screens/b Curity A eneral ADUS Authentication ADUS Authentication ADUS Authentication ADUS Accounting bood Net Users AC Filtering isabled Clients ser Legin Policies Prolocies cess Control Lists the Auth Certificate releas Protection licies rusted AP Policies custed AP Policies pature Events untendry Bandures ignatures ignatures pature Events untendry Policies Policies Policies cate of France Pathentication / MPP abagemeet france releasion	Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	Address Mittee CONTROLLER WIRELESS > Rules > New 7 IP Address M Any TCP Telnet Any Outbound Permit M	IP Address 172.18.0.0	Go Linis ¹⁹ Norton A Save Conf NT COMMANDS H Netmask 255.255.0.0	AndSWrus 😵 - AndSWrus 😵 - Inguration Ping +ELP < Back	Arriet
tps://172.16.1.40/screens/b tps://172.16.1.40/screens/b tps://iritering scale and the science of the science	Access Control Lists Sequence Source Destination Protocol Source Port Destination Port DSCP Direction Action	Address Mittee CONTROLLER WIPELESS > Rules > New 7 IP Address M Any TCP Telnet Any Outbound Permit M	IP Address 172.16.0.0	Go Linis ³⁴ Norton J Save Conf NT COMMANDS H Netmask 255.255.0.0	AndSWrus 😵 - AndSWrus 😵 - Inguration Ping HELP Kack	Arriet

Internet

在 ACL > Edit 的页面上,列出了ACL中定义的所有规则。

-

rity	Acce	ss Contr	ol Lists > Edit						< Back		Add New	Rule
and a second	Gene	ral										
DIUS Authentication DIUS Accounting al Net Users C Filtering	Acces	s List Nam Action	e Guest-A	ACL	Destination IP/Nosk		Protocol	Source Port	Dest Port	DSCP	Direction	
abled Clients r Login Policies Policies	1	Permit	0.0.0.0	1	172.16.1.1 255.255.255.255	1	UDP	DHCP Client	DHCP Server	Any	Inbound	Edit
ss Control Lists Auth Certificate	2	Permit	172.16.1.1 255.255.255.255	1	0.0.0.0	1	UDP	DHCP Server	DHCP Client	Any	Outbound	Edit Remove
less Protection les	з	Permit	0.0.0.0	1	0.0.0.0	1	ICMP	Any	Any	Any	Any	Edit
sted AP Policies jue Policies odard Siconbures	4	Permit	0.0.0.0	/	172.16.1.1 255.255.255.255	1	UDP	Any	DNS	Any	Inbound	Edit Remove
stom Signatures nature Events	5	Permit	172.16.1.1 255.255.255.255	1	0.0.0.0	1	UDP	DNS	Any	Any	Outbound	Edit Remove
nt Exclusion Policies Authentication / MFP	6	Permit	0.0.0.0	/	172.18.0.0 255.255.0.0	1	TCP	Any	Teinet	Any	Inbound	Edit Remove
tection	7	Permit	172.18.0.0 255.255.0.0	1	0.0.0.0	1	TCP	Teinet	Any	Any	Outbound	Edit Remove
sars inned Clients												

- 4. ACL创建完成后,需要应用到动态的Interface上。为了应用ACL,选择 Controller > Interfaces, 然后编辑想要应用ACL的Interface。
- 5. 在动态的Interface的 Interfaces > Edit 页面上,从ACL下拉菜单中选择适当的ACL。如下是配置举例。

NITOR WLANS CONTR erfaces > Edit terface Name Gu erface Address NAN Identifier P Address letmask iateway	oller WIRELESS SECURITY eest 172.19.1.10 255.255.0.0	MANAGEMENT	COMMANDS	HELP < Back	Apply
erfaces > Edit neral Information terface Name Gu erface Address /LAN Identifier P Address letmask iateway	1 172.19.1.10 255.255.0.0	-		< Back	Apply
neral Information terface Name Gu erface Address /LAN Idontifier P Address letmask iateway	1 172.19.1.10 255.255.0.0	-			
terface Name Gu erface Address 'LAN Identifier P Address letmask iateway	1 172.19.1.10 255.255.0.0	m.			
terface Name Gu erface Address /LAN Identifier P Address letmask iateway	1 172.19.1.10 255.255.0.0	-			
erface Address /LAN Identifier P Address letmask Sateway	1 172.19.1.10 255.255.0.0				
rLAN Identifier P Address Jetmask Jateway	1 172.19.1.10 255.255.0.0				
P Address letmask lateway	172.19.1.10 255.255.0.0				
letmask Jateway	255.255.0.0				
iateway	A second state of the seco				
	172.19.1.50				
ysical Information					
ort Number	1				
nfiguration					
Juorantine					
CP Information					
rimary DHCP Server	172.16.1.1				
iecondary DHCP Server					
cess Control List					
ICL Name	Guest-ACL				
e: Changing the Interface par porarily disabled and thus ma te clients.	rameters causes the WLANs to be ay result in loss of connectivity for				
	sical Information ort Number infiguration Userantine CP Information rimary DHCP Server secondary DHCP Server cess Control List CL Name e: Changing the Interface pa parally disabled and thus m is clients.	sical Information ort Number	sical Information iverantine CP Information rimary DHCP Server cecondary DHCP Server cess Control List CL Name CL Name CL Name Cuest-ACL for consectivity for e cleants.	sical Information iverantine CP Information rimary DHCP Server cecondary DHCP Server	stical Information I uprentine CP Information rimary DHCP Server CCP Server CCE Name CL Name CL NAME

这一步完成后,ACL就会允许或拒绝无线网络中使用这个动态的Interface的流量。

Note: 关于在无线控制器上如何用CLI来创建ACL的信息,参见Using the CLI to Configure Access Control Lists。

Note: 本文档中假定WLAN和动态Interface都已经配置好了。关于如何在无线控制器上配置动态 Interface的信息,参见文档Wireless LAN Controllers Configuration Example的VLANs一节。

配置CPU的ACL

以前,无线控制器上的ACL无法过滤去往Management和AP Management端口的LWAPP数据流量, LWAPP控制流量和mobility流量。为了解决这个问题,过滤LWAPP和mobility流量,在无线控制器固件 版本4.0中引进了CPU ACL。

配置CPU ACL包括2个步骤:

- 1. 为CPU ACL配置规则。
- 2. 在无线控制器上应用CPU ACL。

配置CPU ACL的规则的方法与其他的ACL类似。如下是一个CPU ACL的配置例子,允许控制器 (Management Interface的IP地址是172.16.1.40, AP Management Interface的IP地址是172.16.1.41)和轻量 级无线接入点(IP地址是172.16.1.70)之间的LWAPP数据和控制流量,其他的轻量级无线接入点的流量 都被过滤掉。

这个例子中的CPU ACL同样允许Management Interface的IP地址是172.16.1.40的控制器和Management Interface的IP地址是172.16.1.30的控制器之间的mobility流量。

ecurity	Acce	ss Contr	ol Lists > Edit						< Back		Add New	Rule
A	Gene	ral										
ADIUS Authentication ADIUS Accounting Ical Net Users AC Filtering	Acces	s List Nam Action	source IP/Ma	iCL sk	Destination		Protocol	Source	Dest	DSCP	Direction	
isabled Clients ser Login Policies P Policies	1	Permit	172.16.1.40	s /	172.16.1.70 255.255.255.255	1	UDP	12223	Any	Any	Outbound	Edit Remove
ess Control Lists b Auth Certificate	2	Permit	172.16.1.70 255.255.255.25	s′	172.16.1.40 255.255.255.255	1	UDP	Any	12223	Any	Inbound	Edit Remove
reless Protection licles	з	Permit	172.16.1.41 255.255.255.25	s /	172.16.1.70 255.255.255.255	1	UDP	12222-12223	Any	Any	Outbound	Edit Remove
rusted AP Policies ogue Policies tandard Signatures	4	Permit	172.16.1.70 255.255.255.25	s /	172.16.1.41 255.255.255.255	1	UDP	Any	12222-12223	Any	Inbound	Edit Remove
ustom Signatures ghature Events	5	Permit	172.16.1.40 255.255.255.25	s /	172.16.1.30 255.255.255.255	1	TCP	16665-16667	Any	Any	Outbound	Edit Remove
lient Exclusion Policies P Authentication / MFP anagement Frame ratection	6	Permit	172.16.1.30 255.255.255.25	s /	172.16.1.40 255.255.255.255	/	UDP	Any	16666-16667	Any	Inbound	Edit Remove
b Login Page	1											
95 ensors hunned Clients												

当CPU ACL创建完成后,你需要应用到无线控制器上。在无线控制器的CLI上输入如下命令,把CPU ACL 应用到无线控制器上:

<Cisco Controller>config acl cpu <name of the ACL> <wired/wireless/both>

<Cisco Controller>config acl cpu CPU_ACL wired

输入如下命令禁用CPU ACL:

<Cisco Controller>config acl cpu none

Note: 这个例子中给出了如何配置只允许LWAPP和mobility流量的说明,当你在为ACL创建规则时,确保允许无线网络需要的所有协议,因为在每个ACL的最后有一条隐式的deny。

验证

思科推荐你用无线客户端测试一下ACL以确保你配置正确。如果不能正常运作,则在ACL的页面上检查ACL并且检查ACL是否应用到了控制器的Interface上。

你可以用如下的 show 命令来验证你的配置:

show acl summary 使用 show acl summary 这条命令来列出在控制器上配置的ACL。
 如下是举例:

(Cisco Controller) > show acl summary

● show acl detailed ACL_Name 列出ACL的具体信息。

如下是举例:

(Cisco Controller) >show acl detailed Guest-ACL

		Source	Destination		Source
I	Dir	IP Address/Netmask	IP Address/Netmask	Prot	Rang
1	In	0.0.0/0.0.0	172.16.1.1/255.255.255.255	17	68-6
2	Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	67-6
3	Any	0.0.0/0.0.0	0.0.0/0.0.0.0	1	0-6
4	In	0.0.0/0.0.0	172.16.1.1/255.255.255.255	17	0-6
5	Out	172.16.1.1/255.255.255.255	0.0.0/0.0.0.0	17	53-5
6	In	0.0.0/0.0.0	172.18.0.0/255.255.0.0		60-6
7	Out	172.18.0.0/255.255.0.0	0.0.0/0.0.0.0	6	23-2

● show acl cpu 使用 show acl cpu 这条命令来列出CPU ACL。

如下是举例:

(Cisco Controller) >show acl cpu

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

排障

控制器固件版本4.2.61.0或更高版本中,可以配置ACL计数器。ACL计数器可以帮助确定哪个ACL应用到 了通过控制器的数据包。这个特性在系统排障时非常有用。

ACL计数器在如下的控制器上有:

- 4400系列
- 思科WiSM
- Catalyst 3750G 集成无线控制器交换机

根据如下步骤起用这个特性:

1. 点击 Security > Access Control Lists > Access Control Lists 打开 Access Control Lists 页面。

这个页面上列出在控制器上配置的所有的ACL。

2. 为了查看数据包有没有命中控制器上配置的ACL,选中 Enable Counters 并且点击 Apply. 在 默认情况下是没有选中的。 3. 如果你要把ACL的计数器清零,把鼠标指针放在ACL的蓝色的下拉箭头上,选择 Clear Counters.

NetPro论坛 – 特殊的会话

Networking Professionals Connection是一个让网络专家们分享网络解决方案、产品和技术相关的问题、建议及信息的论坛。这些特殊的链接是一些在这个技术领域内最新的会话。

NetPro论坛 - 无线的特殊的会话

Wireless - Mobility: WLAN Radio Standards

Wireless - Mobility: Security and Network Management

Wireless - Mobility: Getting Started with Wireless

Wireless - Mobility: General

相关信息

- VLANs on Wireless LAN Controllers Configuration Example
- Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)
- Cisco Wireless LAN Controller Configuration Guide, Release 4.0
- Wireless Support Page
- Technical Support & Documentation Cisco Systems

Contacts & Feedback | Help | Site Map

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks of Cisco Systems, Inc.

更新: Jan 21, 2008

文档 ID: 71978