在Catalyst 9800上配置可下载ACL并对其进行故 障排除

目录
<u>简介</u>
<u>背景信息</u>
<u>先决条件</u>
· <u>要求</u>
使用的组件
<u>将dACL与802.1x SSID一起使用</u>
<u>网络图</u>
<u>WLC 配置</u>
ISE 配置
每用户dACL
每结果dACL
<u>有关将dACL与CWA SSID配合使用的说明</u>
<u>验证</u>
<u>故障排除</u>
<u>核对清单</u>
<u>WLC一站式反射</u>
WLC Show命令
条件调试和无线电主动跟踪
<u>数据包捕获</u>
RADIUS客户端身份验证
<u>DACL下载</u>
<u>ISE操作日志</u>
RADIUS客户端身份验证
DACL下载

简介

本文档介绍如何在Catalyst 9800无线LAN控制器(WLC)上配置可下载ACL (dACL)并对其进行故障排除。

背景信息

在Cisco IOS®和IOS XE®交换机中,dACL已支持多年。dACL是指发生身份验证时,网络设备从 RADIUS服务器动态下载ACL条目,而不是具有ACL的本地副本并且仅分配ACL名称。提供更完整 的<u>Cisco ISE配置示例</u>。本文档重点介绍自17.10版本以来支持用于中心交换的dACL的Cisco Catalyst 9800。

先决条件

本文档的思想是通过基本SSID配置示例演示Catalyst 9800上的dACL使用情况,展示如何完全自定 义这些dACL。

在Catalyst 9800无线控制器上,可下载ACL包括

- <u>从Cisco IOS XE Dublin 17.10.1</u>版本<u>开始</u>支持。
- 仅支持具有本地模式接入点的集中式控制器(或Flexconnect集中式交换)。FlexConnect本地 交换不支持dACL。

要求

Cisco 建议您了解以下主题:

- Catalyst Wireless 9800配置型号。
- 思科IP访问控制列表(ACL)。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- Catalyst 9800-CL(v.都柏林17.12.03)。
- ISE(版本3.2)。

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。

配置

在本配置指南中,即使方法不同(例如WLAN身份验证、策略配置等),最终结果也是相同的。在 此展示的场景中,两个用户身份定义为USER1和USER2。两者都被授予了访问无线网络的权限。 ACL_USER1和ACL_USER2分别分配给Catalyst 9800从ISE下载的dACL。

将dACL与802.1x SSID一起使用

网络图



WLC 配置

有关Catalyst 9800上的802.1x SSID配置和故障排除的详细信息,请参阅<u>在Catalyst 9800无线控制</u> 器系列上配置802.1X身份验证</u>配置指南。

步骤1:配置SSID。

使用ISE作为RADIUS服务器,配置经802.1x身份验证的SSID。在本文档中,SSID命名为 "DACL_DOT1X_SSID"。

<u>从 GUI:</u>

导航到配置>标签和配置文件> WLAN,然后创建与下面所示类似的WLAN:

Cisco Cata	alyst 9800-CL Wireless Controller		Welcome admin	* * & B & B & B & C	Search APs and Clients Q	•
Q Search Menu Items	Configuration * > Tags & Profiles * > WLAN	5 Enable WLAN Disable WLAN			WLAN Wizard	
Monitoring	Selected WLANs : 0	v ID	▼ ccin	▼ 2.4/6 GHz Casurity	< Gild Security	*
Configuration		\$ 2	DACL_DOT1X_SSID	[WPA2][802.1x][AES]	1 - 1 of 1 items	Ċ
C Licensing						
X Troubleshooting						
Walk Me Through 3						

<u>从CLI:</u>

WLC#configure terminal WLC(config)#wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID WLC(config-wlan)#security dot1x authentication-list DOT1X WLC(config-wlan)#no shutdown

第二步:配置策略配置文件。

配置与上述定义的SSID一起使用的策略配置文件。在此策略配置文件中,确保从"Advanced"选项卡 配置AAA Override,如屏幕截图所示。 在本文档中,使用的策略配置文件是"DACL-8021X"。

如前提条件部分所述,dACL仅支持集中交换/身份验证部署。确保以这种方式配置策略配置文件。

<u>从 GUI:</u>

导航到Configuration > Tags & Profiles > Policy,选择使用的策略配置文件,并按所示进行配置。





<u>从CLI:</u>

WLC#configure terminal WLC(config)#wireless profile policy DACL-8021X WLC(config-wireless-policy)#aaa-override WLC(config-wireless-policy)#vlan VLAN_1413 WLC(config-wireless-policy)#no shutdown

第三步:将策略配置文件和SSID分配给使用的策略标记。

<u>从 GUI:</u>

导航到配置>标签和配置文件>标签。在Policy tags选项卡中,创建(或选择)使用的标记,并向其 分配步骤1-2期间定义的WLAN和策略配置文件。



<u>从CLI:</u>

WLC#configure terminal WLC(config)#wireless tag policy default-policy-tag WLC(config-policy-tag)#description "default policy-tag" WLC(config-policy-tag)#wlan DACL_DOT1X_SSID policy DACL-8021X

第四步:允许供应商特定属性。

可下载ACL通过ISE和WLC之间的RADIUS交换中的供应商特定属性(VSA)传递。使用这些CLI命令 ,可以在WLC上启用对这些属性的支持。

<u>从CLI:</u>

WLC#configure terminal WLC(config)#radius-server vsa send authentication

第五步:配置默认授权列表。

使用dACL时,必须通过RADIUS实施网络授权,WLC才能授权对配置的802.1x SSID进行身份验证 的任何用户。实际上,不仅身份验证,而且授权阶段也在RADIUS服务器端处理。因此,在这种情 况下,需要授权列表。

确保9800配置中包含默认网络授权方法。

<u>从 GUI:</u>

导航到Configuration > Security > AAA,然后从AAA Method List > Authorization选项卡创建与所示 类似的授权方法。

Cisco Catalyst 9800-CL Wirele	ss Controller		Welcome admin 🗌 🐔 🦷		Search APs and Clients Q	Feedback 🖌
Q, Search Menu Items	surity * > AAA Show Me How 🧿					
Dashboard Monitoring	AAA Method List AAA Advanced					
Configuration	+ Add × Delete					
Administration Accounting	Name default	Type Type Group Type exec local	Group1 N/A	Group2	Group3 T	Group4 T N/A
* Troubleshooting	default default 1	network group	radius	N/A	N/A	N/A 1 - 2 of 2 items
(Walk Me Through)						

```
<u>从CLI:</u>
```

```
WLC#configure terminal
WLC(config)#aaa authorization network default group radius
```

ISE 配置

当使用ISE在无线环境中实施dACL时,可以采用两种常见配置:

- 1. 每用户dACL配置。借助此功能,每个特定身份都分配了一个dACL,这要归功于自定义身份字 段。
- 2. 每结果dACL配置。当选择此方法时,将根据用户与使用的策略集匹配的授权策略将特定 dACL分配给用户。

每用户dACL

步骤1:定义dACL自定义用户属性

要将dACL分配给用户身份,首先必须在创建的身份上配置此字段。默认情况下,在ISE上,没有为 创建的任何新身份定义"ACL"字段。要解决此问题,可以使用"自定义用户属性"(Custom User Attribute)并定义新的配置字段。为此,请导航到管理>身份管理>设置>用户自定义属性。使用"+"按 钮可添加与显示内容类似的新属性。 在本示例中,自定义属性的名称是ACL。

≡ Cisco ISE		Administration · Identity	Management		🔺 License Warning Q	\$ 50 \$
Identities Groups	External Identity Sources	Identity Source Sequences	Settings			
User Custom Attributes						$All \sim - \nabla$
User Authentication Settings	Mandat Attribu	te Name	∧ Data Type			
Endpoint Custom Attributes	Firstna	ne	String			
REST ID Store Settings	Lastnar	ne	String			
	Name		String			1
	Passwo	ord (CredentialPassword)	String			
	✓ User Custom Att	ributes				
	Attribute Name	Description	Data Type	Parameters	Default Value Mandato	ry
	ACL		String ~	String Max length	+ 0 (i +
					Save	Reset

完成此配置后,使用"保存"按钮保存更改。

第二步:配置dACL

导航到策略>策略元素>结果>授权>可下载ACL在ISE上查看和定义dACL。使用"添加"按钮可创建一 个新按钮。

≡ Cisco ISE			Polic	y · Policy Elements	🔺 License Warning 🔍 ⊘ 💭 🐡
Dictionaries C	onditions	Results			
Authentication	>	Dow	nloadable ACL	S	
Authorization Authorization Profiles Downloadable ACLs	~	🖉 Edit	+ Add Duplicate	Delete	Selected 0 Total 7 🥃 🕸
			Name	Description	
Profiling	>		ACL_USER1	ACL assigned to USER1	
Posture	>		DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic	
Client Provisioning	>		DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic	
			PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic	
			PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic	
			test-dacl-cwa		
			test-daci-dot1x		

这将打开"New Downloadable ACL"配置表单。在本示例中,配置以下字段:

- 名称:定义的dACL的名称。
- 说明(可选):有关所创建dACL用法的简要说明。
- IP版本:在定义的dACL中使用的IP协议版本(版本4、6或两者)。
- DACL内容:根据Cisco IOS XE ACL语法的dACL内容。

在本文档中,使用的dACL是"ACL_USER1",此dACL允许除发往10.48.39.186和10.48.39.13的流量 以外的任何流量。

字段配置完毕后,请使用"提交"按钮创建dACL。

重复此步骤,为第二个用户ACL_USER2定义dACL,如图所示。

≡ Cisco ISE			Policy	🛕 License Warning Q ⊘ 🔎 🐡	
Dictionaries Cond	ditions	Results			
Authentication	>	Dow	nloadable ACLs	3	
Authorization	~				Selected 0 Total 8 🦪 🚸
Authorization Profiles		🖉 Edit	🕂 Add 🛛 Duplicate 👩	Delete	all \sim $~$ ∇
Downloadable Acts			Name	Description	
Profiling	>		ACL_USER1	ACL assigned to USER1	
Posture	>		ACL_USER2	ACL assigned to USER2	
Client Provisioning	>		DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic	
			DENY_ALL_IPV6_TRAFFIC	Deny all joy6 traffic Deny all joy8 traffic	
			PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic	
			PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic	
			test-dacl-cwa		
			test-daci-dot1x		

第三步:将dACL分配给已创建的身份

创建dACL后,可以使用第1步中创建的用户自定义属性将其分配给任何ISE身份。为此,请导航到 管理>身份管理>身份>用户。与往常一样,使用"添加"按钮创建用户。



在"New Network Access User"(新网络访问用户)配置表中,定义所创建用户的用户名和密码。使 用自定义属性"ACL"将第2步中创建的dACL分配给身份。在本示例中,定义了使用ACL_USER1的身 份USER1。

- Class ISE	Administration Identity ++	
E CISCO ISE	Administration - Identity Management	License Warring Q, O (24)
Identities Groups Ext	ernal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Notwork Access Users List > USER1	
	✓ Network Access User	
	* Username USER1	
	Status 🔤 Enabled 🗸	
	Account Name Alias	
	[mai	
	✓ Passwords	
	Password Type: Internal Users	
	Password Lifetime: Vrith Expiration ① Password Integrine in 53 days Networ Expires ①	
	Password Re-Enter Password	
	* Login Password	
	Enable Password Generate Password 🔘	
	> User Information	
	> Account Options	
	> Account Disable Policy	
	✓ User Custom Attributes	
	E ACL * ACL_USER1	
	✓ User Groups	
	🗄 Select an Item. 🗸 💿 🔴	
		- Ease - Roset

正确配置字段后,使用"提交"按钮创建身份。

重复此步骤以创建USER2并为其分配ACL_USER2。

E Cisco ISE	Administration - Identity Management	🔺 License Warning Q 💿 🕫 🗇
Identities Groups Ex	ernal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected O Total 3 🔮 🚭
	🖉 Edit 🕂 Add 🛞 Charge Status V 🕁 Import 🖒 🗴 Export V 🔋 Defets V 📋 Depters	$a_{i} \sim - \nabla$
	Status Username 🔿 Description : First Name Last Name Email Address User Identity Groups Admin	
	Oisabled 1 adminuser admin-group	
	Enabled 1 USER1	
	Enabled 1 USER2	
	Network Access Users	

第四步:配置授权策略结果。

配置身份和分配的dACL后,仍必须配置授权策略,以便匹配与现有授权公共任务定义的自定义用户 属性"ACL"。要执行此操作,请导航到策略>策略元素>结果>授权>授权配置文件。使用"添加 "(Add)按钮定义新的授权策略。

- 名称:授权策略的名称,此处"9800-DOT1X-USERS"。
- Access Type:此策略匹配时使用的访问类型,此处为ACCESS_ACCEPT。
- 常见任务:将"DACL名称"与内部用户的InternalUser:<创建的自定义属性的名称>进行匹配。 根据本文档中使用的名称,配置文件9800-DOT1X-USERS已配置为InternalUser:ACL的 dACL。

≡ Cisco ISE	Policy - Policy Elements	🔺 License Warning	Q (1)	9 Q
Dictionaries Conditions	Results			
Authentication	Authorization Profiles 2 New Authorization Profile Authorization Profile			
Authorization Profiles				
Downloadable ACLs	* Namo 9800-DOT1X-USERS			
	Description Authoritation profile for 802.1x users using dACLs.			
Profiling >				
Posture >	* Access Type ACCESS_ACCEPT ~			
Client Provisioning	Network Device Profile 🗰 Claco 🗸 😑			
	Service Template			
	Track Movement			
	Agentless Posture			
	Passive Identity Tracking 🔲 💿			
	Common Tasks			
	DACL Name InternalUser:ACL			I
	IPv6 DACL Name			
	ACL (Filter-ID)			
	C una mun marca mit			

第五步:使用策略集中的授权配置文件。

授权配置文件正确定义后,仍需要成为用于对无线用户进行身份验证和授权的策略集的一部分。导 航到策略>策略集,打开所使用的策略集。

此处,身份验证策略规则"Dot1X"匹配通过有线或无线802.1x建立的任何连接。授权策略规则 "802.1x用户dACL"对使用的SSID实施条件(即Radius-Called-Station-ID包含 DACL_DOT1X_SSID)。如果在"DACL_DOT1X_SSID" WLAN上执行授权,则使用步骤4中定义的 配置文件"9800-DOT1X-USERS"对用户进行授权。

Cisco ISI	E		Policy · Policy Sets		A License Warning	Q (0)	,a
olicy Sets	s→ D	efault		1	Reset Policyset Hitcounts		Save
Status	Poli	cy Set Name D	scription Conditions		Allowed Protocols / Server	Sequenc	e Hit
Q Sea	rch						
0	D	efault	Default policy set		Default Network Access	∞ ~+	76
✓ Authentic	ation I	Policy (2)					
🕂 Sta	tus	Rule Name	Conditions		Use	Hits A	ction
Q 50	arch						
					All_User_ID_Stores 🛛 😒 🗸		
•	2	Dot1X	OR Wired_802.1X		> Options	65	<u>نې</u>
	-						
		Default			All_User_ID_Stores 🛛 🗸	10	{ô}
					> Options		
> Authoriza	ation P	olicy - Local Exceptions					
> Authoriza	ation P	olicy - Global Exceptions					
✓ Authoriza	ation P	olicy (2)					
			Result	Its			
🕂 Sta	itus	Rule Name	Conditions Profile	les	Security Groups	Hits A	ction
Q Se	arch						
		802.1x Users dACL	Radius-Called-Station-ID CONTAINS DACL_DOTIX_SSID	D-DOT1X-USERS × +	Select from list \sim +	65	(ĝ}
	_						

每结果dACL

为避免将特定dACL分配给ISE上创建的每个身份这一艰巨任务,您可以选择将dACL应用于特定策略结果。然后,根据在使用的策略集的授权规则上匹配的任何条件应用此结果。

步骤1:配置dACL

从<u>每用户dACL</u>部分执行相同的步骤2以定义所需的dACL。此处是ACL_USER1和ACL_USER2。

第二步:创建身份

导航到管理>身份管理>身份>用户,使用"添加"按钮创建用户。

E Cisco ISE	Administration - Identity Manag	gement	🔺 License Warning Q 💮 🔎	ø
Identities Groups External Identit	ty Sources Identity Source Sequences S	ettings		
Users Network Scan Res	vork Access Users	xport 🗸 👩 Delete 🗸 🏹 Duplicate	Selected 0 Total 1 📿 🎕	}
	Status Username A Description First	Name Last Name Small Address Users	ser Identity Groups Admin	
0	Disabled <u> s</u> adminuser	ð	idmin-group	
				I
	Add Status Miniput Status Status Bisabled	xport V Delete V Duplicate Name Last Name <u>Freed Address User</u>	Selected 0 Total 1 🤪 All ~ ser Identity Groups Admin Idmin-group	2

在"New Network Access User"(新网络访问用户)配置表中,定义所创建用户的用户名和密码。

≡ Cise	co ISE					Administration - Identity M	anagement	License Warning	Q (0 52	Φ
Identities	Groups	External	Identity Sources	Identity Source Sequence	ea Settings					
Users Latert Manual N	ietwork Scan Res		Webwork Access Users Li	int > New Network Access User						
			V Network Acce	ess User			_			
			* Usemame	USER 1]			
			Status	Enabled 🗸			-			
			Account Name Alla	ati	0					
			Ernall							
			- Daeswords							
			Pattword Type:	Internal Users						
			With Expiratio	n: ()						
			 Never Expires 	0						
				Password	Re-Enter Password					
			* Login Password			Generate Password	1			
			Enoble Password			Generate Password	-			
			> User Informa	tion						
			> Account Opti	ions						
			> Account Disa	ble Policy						
			> User Custom	Attributes						
			> User Groups							
								Submit	Carcel	

重复此步骤以创建USER2。

E Cisco ISE	Administration - Identity Management	🔺 License Riemang 🔍 🛞 528 dij
Identities Groups Ex	ternal Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	
		Selected O Total 3 🜔 🔕
	∕isi +AAS & Change Status ∨ do lagent & Expert ∨ ① Deleta ∨ ① Deleta >	м ~
	Status Username 🔿 Description First Name Last Name Email Address User Identity Groups Admin	
	OSsabled 1 edminuser admin-group	
	D Brunne Toorus	
	Menancia Access Union	

第四步: 配置授权策略结果。

配置身份和dACL后,仍必须配置授权策略,以便将特定dACL分配给匹配此条件的用户,以使用此 策略。为此,请导航到策略>Policy元素>结果>授权>授权配置文件。使用"添加"(Add)按钮定义新的 授权策略并填写这些字段。

- 名称:授权策略的名称,此处"9800-DOT1X-USER1"。
- Access Type:此策略匹配时使用的访问类型,此处为ACCESS_ACCEPT。
- 常见任务:将内部用户的"DACL名称"与"ACL_USER1"进行匹配。根据本文档中使用的名称 ,配置文件9800-DOT1X-USER1使用配置为"ACL_USER1"的dACL进行配置。

≡ Cisco ISE	Policy · Policy Elements	A License Warring	ର ୭	1
Dictionaries Conditions	Results			
Authoritarian > Authoritarian > Authoritarian > Authoritarian > Pretiling > Pretiling > Pretiling > Citert Previsioning >	Advectation Profiles * Namo 9800-D0TIX-USEN1 Description			
	Common Tasks Cont. Nerre ACL_USER1 If the DACL Nerre ACL_USER1 If the DACL Nerre ACL_USER1 ACL_USER1 ACL_USER1 ACL_USER1			
	✓ Attributes Details Asses free - ACCRS_ACCEPT MCL + ACL_ISOPS	Submit	0	encel

重复此步骤,创建策略结果"9800-DOT1X-USER2",并将"ACL_USER2"分配为DACL。

Dictionaries Conditions Results	dard Authorization Profiles weret an to Addividuation > System > Backup & Ressons > Policy Expose + Add ① Dudrawe ② Declars Nerma 9000-001114.USD31	ri Pago Na A	Selected	0 Tatal 13 🦪 M 🗸
Authoritantina >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	dard Authorization Profiles west parts Administration > System > Backup & Resource > Policy Export + AAR ① Duplication @ Duplication @ Duplication Name Profiles #800-D0111X USD31 @ Diplication	rt Pago Na A	Selecter	0 Tatal 13 🦪 M 🗸
Acthologian Profiles Devriseden ACs Profiles Profiles Parare Clam Provided and Clam	veret ge te Adrivitetration > System > Backup & Rescore > Policy Dupor + Ade () Dupture () Onetes Neme Prefix 9600-0011X USD31 () ()	nt Page Ne ^	Selected	10 Total 13 🦪
Autorization Profiles Developable ACLs Profiles Pannes Client Provisions	+ ASE () Displaces () Debries Nerne Prefix 9900-D011X-USEX1 (E) (C)	1e ^	Selector	10 Tasal 13 🦪
Profiles Pactore Client Provisions	+ A52 () Duplicate () Delete Nerrie Profile 0000-D01134-USD31 () () ()	1a ^)	Passibilia	AL Y
Profiling > N Pactare > Client Provisioning > 0	Neme Profile 9000-0011X-USDI1 & Ci	la ^)	Percention	
Pasture > Client Provisioning >	9800-D011X-USD11 #2 CH		westerproven	
Client Provisioning		isea 🕕		
	9800-D011X-U3692 ## Cit	isca 🕡		
	9600-D011X-USDRS # Ge	iaca 🕕	Authorization profile for 802.1x users using dACLs.	
	Steck_Windess_Access At Cit	isca 🕕	Default profile used to block wireless devices. Ensure that you configure a NULL ROUTE ACL on the Wireless LAN Controller	
0 4	Cisso_P_Phones # Ci	laca 🕕	Default profile used for Cisco Phones.	
0 4	Cisco_Temporal_Onboard ## Cit	isca 🕕	Onboard the device with Cisco temporal agent	
0 4	Cisco_WebArth At Cit	isco 🕡	Default Profile used to redirect users to the CWIA portal.	
0	Internal/Deprétation	inca 🕡		
0	NSP_Orboard de Cit	isea 🕕	Onboard the device with Native Supplicant Provisioning	
0	Nos_Cisco_P_Phones ALCI	ises 🕜	Default Profile used for Non Cisco Phones.	
0 4	utw 🗠 Cit	inca 🕡	Default profile used for UDN.	
	GenyAccess		Default Profile with access type as Access-Reject	
0 -	Permithecess		Default Profile with access type as Access-Accept	

第五步:使用策略集中的授权配置文件。

一旦授权配置文件得到正确定义,它仍需要成为用于对无线用户进行身份验证和授权的策略集的一 部分。导航到策略>策略集,打开所使用的策略集。

此处,身份验证策略规则"Dot1X"匹配通过有线或无线802.1X建立的任何连接。授权策略规则 "802.1X User 1 dACL"对使用的用户名实施条件(即InternalUser-Name CONTAINS USER1)。如 果使用用户名USER1执行授权,则使用步骤4中定义的配置文件"9800-DOT1X-USER1"对用户进行 授权,因此,此结果中的dACL (ACL_USER1)也应用于用户。用户名USER2的配置也相同,对其使 用"9800-DOT1X-USER1"。

sco ISE							
			Policy - Policy Sets		📥 License Warring	9, 6	5 63
icy Sets→	Default				Reset Palicyset Hitcounts		Sav
Status P	folicy Set Name	escription Conditions			Allowed Protocols / Serve	r Segur	ence
Q Search							
•	Defeat	Default policy set			Default Network Access		~+
kathenticatio	on Palicy (2)						
Status	Rule Name	Conditions			Use	Hits	Acti
Q Search	h						
		Wined_883.1X			All_User_ID_Stores 00 V		
۰	Del1X	CR Windows MAB			> Options		4
		E Wired_MAS					
					All_User_ID_Stores 🛛 🖸 🗸		
•	Defexit				> Options	10	6
Authorization	n Pelicy - Local Exceptions						
kathorization	n Policy - Global Exceptions						
. factor	Bula Nama	And Marco		Results	faculty faces		
 Status 	Rule Name	Conditions		Results Profiles	Security Groups	Hits	Act
 Status Q Search 	Rule Name	Cenditions		Results Profiles	Security Groups	Hits	Act
 Status Q. Search 	Rule Name	Conditions		Results Profiles (B800-DOT1X-USER2 × v +	Security Groups Select from list ~ +	Hits	Aut
Status Q Search	Rule Name	Conditions InternetDate Flame EQUALS USER2 L InternetDate Flame EQUALS USER3		Results Profiles 9800-0011X-USER2 × >+ 9800-0011X-USER1 × >+	Select from list + Select from list +	Hits 0	Act E

有关将dACL与CWA SSID配合使用的说明

如<u>在Catalyst 9800 WLC和ISE上配置中央Web身份验证(CWA)</u>配置指南中所述,CWA依靠MAB和 特定结果对用户进行身份验证和授权。可下载的ACL可以从ISE端添加到CWA配置,与上文所述相 同。



警告:可下载ACL只能用作网络访问列表,不支持将其用作预身份验证ACL。因此,必须在WLC配置中定义CWA工作流程中使用的所有预身份验证ACL。

验证

要检验所做的配置,可以使用以下命令。

show run wlan
show run aaa
show aaa servers
show ap config general
show ap name <ap-name> config general
show ap tag summary
show ap tag summary
show wlan { summary | id | nme | all }
show wireless tag policy detailed <policy-tag-name>
show wireless profile policy detailed <policy-profile-name>
show access-lists { acl-name }

下面引用了与此示例相对应的WLC配置的相关部分。

```
aaa new-model
I
!
aaa group server radius authz-server-group
server name DACL-RADIUS
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authentication dot1x DOT1X group radius
aaa authorization exec default local
aaa authorization network default group radius
!
aaa server radius dynamic-author
client <ISE IP>
Т
aaa session-id common
I
[...]
vlan 1413
name VLAN 1413
T
[...]
radius server DACL-RADIUS
address ipv4 <ISE IP> auth-port 1812 acct-port 1813
key 6 aHaOSX[QbbEHURGW`cXiG^UE]CR]^PVANfcbROb
!
I
[...]
wireless profile policy DACL-8021X
 aaa-override
vlan VLAN 1413
no shutdown
[...]
wireless tag policy default-policy-tag
 description "default policy-tag"
wlan DACL_DOT1X_SSID policy DACL-8021X
[...]
wlan DACL_DOT1X_SSID 2 DACL_DOT1X_SSID
security dot1x authentication-list DOT1X
 no shutdown
```

将显示RADIUS服务器配置,使用show running-config all命令显示。

```
WLC#show running-config all | s radius-server
radius-server attribute 77 include-in-acct-req
radius-server attribute 77 include-in-access-req
radius-server attribute 11 default direction out
radius-server attribute nas-port format a
radius-server attribute wireless authentication call-station-id ap-macaddress-ssid
```

radius-server dead-criteria time 10 tries 10 radius-server cache expiry 24 enforce hours radius-server transaction max-tries 8 radius-server retransmit 3 radius-server timeout 5 radius-server ipc-limit in 10 radius-server ipc-limit done 10 radius-server vsa send accounting radius-server vsa send authentication

故障排除

核对清单

- 确保客户端可以正确连接到配置的802.1X SSID。
- 确保RADIUS access-request/accept包含适当的属性值对(AVP)。
- 确保客户端使用正确的WLAN/策略配置文件。

WLC一站式反射

要检查dACL是否已正确分配给特定无线客户端,可以使用show wireless client mac-address <H.H.H> detail命令,如下所示。从中可 以看到各种有用的故障排除信息,即:客户端用户名、状态、策略配置文件、WLAN,最重要的是这里是ACS-ACL。

<#root>

WLC#show wireless client mac-address 08be.ac14.137d detail Client MAC Address : 08be.ac14.137d Client MAC Type : Universally Administered Addreclient Username : USER1 AP MAC Address : f4db.e65e.7bc0 AP Name: AP4800-E Client State : Associated Policy Profile : DACL-8021X Wireless LAN Id: 2 WLAN Profile Name: DACL_DOTIX_SSID Wireless LAN Network Name (SSID): DACL_DOTIX_SSID BSSID : f4db.e65e.7bc0 Association Id : 1 Authentication Algorithm : Open System Client Active State : Client ACLs : None Policy Manager State: Run Last Policy Manager State : IP Learn Complete Client Entry Create Time : 35 seconds Policy Type : WPA2 | VLAN : VLAN_1413 [...] Session Manager: Point of Attachment : capwap_90000012 IIF ID : 0x90000012 Authorized : TRUE Sess SM State : AUTHENTICATED SM Bend State : IDLE Local Policies: Service Template : wlan_svc_DACL-8021x_local (priority 254) VLAN : VLAN_1413 Absolute-Timer : 28800 Server Policies: ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab Resultant Policies: ACS ACL : xACSACLx-IP-ACL_USER1-65e89aab VLAN Name : VLAN_1413 VLAN : 1413 Absolute-Timer : 28800 [...]

WLC Show命令

要查看当前作为Catalyst 9800 WLC配置一部分的所有ACL,可以使用**show access-lists**命令。此命令列出本地定义的所有ACL或WLC下载的dACL。WLC从ISE下载的所有dACL的格式为 xACSACLx-IP-<ACL_NAME>-<ACL_HASH>.



注意:只要客户端已关联并在无线基础设施中使用,可下载ACL就会保留在配置中。使用dACL的最后一个客户端离开基

础设施后,即会从配置中删除dACL。

```
WLC#show access-lists
Extended IP access list IP-Adm-V4-Int-ACL-global
[...]
Extended IP access list IP-Adm-V4-LOGOUT-ACL
[...]
Extended IP access list implicit_deny
[...]
Extended IP access list implicit_permit
[...]
Extended IP access list meraki-fqdn-dns
[...]
Extended IP access list preauth-ise
[...]
Extended IP access list preauth_v4
[...]
Extended IP access list xACSACLx-IP-ACL_USER1-65e89aab
   1 deny ip any host 10.48.39.13
   2 deny ip any host 10.48.39.15
    3 deny ip any host 10.48.39.186
    4 permit ip any any (56 matches)
IPv6 access list implicit_deny_v6
[...]
IPv6 access list implicit_permit_v6
[...]
IPv6 access list preauth_v6
[...]
```

条件调试和无线电主动跟踪

在排除配置故障时,您可以为假定已分配dACL的客户端收集<u>放射性跟踪</u>。这里突出显示的日志显示客户端08be.ac14.137d的客户端关 联过程中放射性踪迹的相关部分。

<#root>

```
24/03/28 10:43:04.321315612 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (note): MAC: 08be.ac14.137d Asso
```

2024/03/28 10:43:04.321414308 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d

[...]

```
2024/03/28 10:43:04.322185953 {wncd_x_R0-0}{1}: [dot11] [19620]: (note): MAC: 08be.ac14.137d Association
```

2024/03/28 10:43:04.322199665 {wncd_x_R0-0}{1}: [dot11] [19620]: (info): MAC: 08be.ac14.137d DOT11 state

[...]

2024/03/28 10:43:04.322860054 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d &

2024/03/28 10:43:04.322881795 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376

[...]

2024/03/28 10:43:04.323379781 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.330181613 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.353413199 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.13 2024/03/28 10:43:04.353414496 {wncd_x_R0-0}{1}: [auth-mgr-feat_wireless] [19620]: (info): [08be.ac14.13

2024/03/28 10:43:04.353438621 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 Au

2024/03/28 10:43:04.353443674 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

[...]

2024/03/28 10:43:04.381397739 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to

2024/03/28 10:43:04.381411901 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator e9 8b e

2024/03/28 10:43:04.381425481 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 7 "USERI

2024/03/28 10:43:04.381430559 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Service-Type [6] 6 Fr 2024/03/28 10:43:04.381433583 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 27 2024/03/28 10:43:04.381437476 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 21 " 2024/03/28 10:43:04.381440925 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Framed-MTU [12] 6 148 2024/03/28 10:43:04.381452676 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 12 . 2024/03/28 10:43:04.381466839 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator 2024/03/28 10:43:04.381482891 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Key-Name [102] 2 2024/03/28 10:43:04.381486879 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 49 2024/03/28 10:43:04.381489488 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 43 "2024/03/28 10:43:04.381491463 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381494016 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "r

2024/03/28 10:43:04.381495896 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32 2024/03/28 10:43:04.381498320 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 " 2024/03/28 10:43:04.381500186 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 20

2024/03/28 10:43:04.381502409 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 14 "

2024/03/28 10:43:04.381506029 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6

2024/03/28 10:43:04.381509052 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port-Type [61] 6 2024/03/28 10:43:04.381511493 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-Port [5] 6 3913 2024/03/28 10:43:04.381513163 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 39

2024/03/28 10:43:04.381515481 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 33 "d

2024/03/28 10:43:04.381517373 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 41

2024/03/28 10:43:04.381519675 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 35 "v

2024/03/28 10:43:04.381522158 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Called-Station-Id [30]

2024/03/28 10:43:04.381524583 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Calling-Station-Id [3 2024/03/28 10:43:04.381532045 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Airespace [26 2024/03/28 10:43:04.381534716 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Airespace-WLAN-ID [1]

2024/03/28 10:43:04.381537215 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Nas-Identifier [32] 1

2024/03/28 10:43:04.381539951 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-group-cipher [18 2024/03/28 10:43:04.381542233 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-pairwise-cipher[2024/03/28 10:43:04.381544465 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: wlan-akm-suite [188] 2024/03/28 10:43:04.381619890 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout [...]

2024/03/28 10:43:04.392544173 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812,

2024/03/28 10:43:04.392557998 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 08 6d for 2024/03/28 10:43:04.392564273 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: State [24] 71 ... 2024/03/28 10:43:04.392615218 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: EAP-Message [79] 8 .. 2024/03/28 10:43:04.392628179 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator 2024/03/28 10:43:04.392738554 {wncd_x_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t 2024/03/28 10:43:04.726798622 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001.

2024/03/28 10:43:04.726801212 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

2024/03/28 10:43:04.726896276 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_9000001

2024/03/28 10:43:04.726905248 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

[...]

2024/03/28 10:43:04.727148212 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727164223 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000 2024/03/28 10:43:04.727169069 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727223736 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : use

2024/03/28 10:43:04.727233018 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : cl 2024/03/28 10:43:04.727234046 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA 2024/03/28 10:43:04.727234996 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Me 2024/03/28 10:43:04.727236141 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : EA M\$®vf9∫Ø◊«? %ÿ0?ã@≤™ÇÑbWï6\Ë&\q·1U+QB-2®"≠∫JÑv?"

2024/03/28 10:43:04.727246409 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applying Attribute : Cis

[...]

2024/03/28 10:43:04.727509267 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727513133 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.727607738 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: SVM Apply user profile 2024/03/28 10:43:04.728003638 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: Activating EPM feature

2024/03/28 10:43:04.728144450 {wncd_x_R0-0}{1}: [epm-misc] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.728161361 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012] 2024/03/28 10:43:04.728177773 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012] 2024/03/28 10:43:04.728184975 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012]

2024/03/28 10:43:04.728218783 {wncd_x_R0-0}{1}: [epm-acl] [19620]: (info): [08be.ac14.137d:capwap_90000

2024/03/28 10:43:04.729005675 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [08be.ac14.137d:capwap_90000012] 2024/03/28 10:43:04.729019215 {wncd_x_R0-0}{1}: [svm] [19620]: (info): SVM_INFO: Response of epm is ASY [...]

2024/03/28 10:43:04.729422929 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Send Access-Request to

2024/03/28 10:43:04.729428175 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 20 06 3

2024/03/28 10:43:04.729432771 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: NAS-IP-Address [4] 6

2024/03/28 10:43:04.729435487 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.729437912 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 32

2024/03/28 10:43:04.729440782 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 26 "a

2024/03/28 10:43:04.729442854 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 30

2024/03/28 10:43:04.729445280 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 24 "a

2024/03/28 10:43:04.729447530 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator 2024/03/28 10:43:04.729529806 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Started 5 sec timeout

2024/03/28 10:43:04.731972466 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Received from id 1812/

2024/03/28 10:43:04.731979444 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: authenticator 2a 24 8

2024/03/28 10:43:04.731983966 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: User-Name [1] 32 "#ACS

2024/03/28 10:43:04.731986470 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Class [25] 75 ... 2024/03/28 10:43:04.732032438 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Message-Authenticator

2024/03/28 10:43:04.732048785 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732051657 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 "i

2024/03/28 10:43:04.732053782 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 47

2024/03/28 10:43:04.732056351 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 41 ":

2024/03/28 10:43:04.732058379 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 48

2024/03/28 10:43:04.732060673 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Cisco AVpair [1] 42 "i

2024/03/28 10:43:04.732062574 {wncd_x_R0-0}{1}: [radius] [19620]: (info): RADIUS: Vendor, Cisco [26] 36

2024/03/28 10:43:04.732114294 {wncd_x_R0-0}{1}: [radius] [19620]: (info): Valid Response Packet, Free t

2024/03/28 10:43:04.733046258 {wncd_x_R0-0}{1}: [svm] [19620]: (info): [08be.ac14.137d] Applied User Pro

2024/03/28 10:43:04.733058380 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M 2024/03/28 10:43:04.733064555 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: M 2024/03/28 10:43:04.733065483 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e 2024/03/28 10:43:04.733066816 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: m 2024/03/28 10:43:04.733068704 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c 2024/03/28 10:43:04.73306947 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c 2024/03/28 10:43:04.733069947 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: i

2024/03/28 10:43:04.733070971 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: us

2024/03/28 10:43:04.733079208 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: c 2024/03/28 10:43:04.733080328 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: E M\$®vf9∫Ø◊«? %ÿ0?ã@≤™ÇÑbWï6\Ë&\q·lU+QB-º®"≠∫JÑv?" 2024/03/28 10:43:04.733091441 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile: e

2024/03/28 10:43:04.733092470 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): Applied User Profile:Cis

[...]

2024/03/28 10:43:04.733396045 {wncd_x_R0-0}{1}: [auth-mgr] [19620]: (info): [08be.ac14.137d:capwap_9000

2024/03/28 10:43:04.733486604 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d L2 A

2024/03/28 10:43:04.734665244 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.734894043 {wncd_x_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d E 2024/03/28 10:43:04.734904452 {wncd_x_R0-0}{1}: [client-keymgmt] [19620]: (info): MAC: 08be.ac14.137d C

2024/03/28 10:43:04.734915743 {wncd_x_R0-0}{1}: [dot1x] [19620]: (info): [08be.ac14.137d:capwap_90000012

2024/03/28 10:43:04.740499944 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= of the set of the

2024/03/28 10:43:04.742238941 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: #

2024/03/28 10:43:04.744387633 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= of the set of the

[...]

2024/03/28 10:43:04.745245318 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.745294050 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Allocate

2024/03/28 10:43:04.745326416 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.751291844 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= of the set of the

2024/03/28 10:43:04.751943577 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.752686055 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Clier

2024/03/28 10:43:04.755505991 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= 0

2024/03/28 10:43:04.756746153 {wncd_x_R0-0}{1}: [mm-transition] [19620]: (info): MAC: 08be.ac14.137d MM 2024/03/28 10:43:04.757801556 {wncd_x_R0-0}{1}: [client-auth] [19620]: (note): MAC: 08be.ac14.137d ADD

2024/03/28 10:43:04.758843625 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1376

2024/03/28 10:43:04.759064834 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d II

2024/03/28 10:43:04.761186727 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.761241972 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.763131516 {wncd_x_R0-0}{1}: [client-auth] [19620]: (info): MAC: 08be.ac14.137d Client-auth]

2024/03/28 10:43:04.764575895 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= o

2024/03/28 10:43:04.764755847 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.769965195 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.770727027 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= o

2024/03/28 10:43:04.772314586 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.772362837 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.773070456 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= o

2024/03/28 10:43:04.773661861 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

2024/03/28 10:43:04.775537766 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= o

2024/03/28 10:43:04.777154567 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= o

2024/03/28 10:43:04.778756670 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: epm acl]

2024/03/28 10:43:04.778807076 {iosrp_R0-0}{1}: [buginf] [26311]: (debug): AUTH-FEAT-IAL-EVENT: Index in

2024/03/28 10:43:04.778856100 {iosrp_R0-0}{1}: [mpls_ldp] [26311]: (info): LDP LLAF: Registry notificat:

2024/03/28 10:43:04.779401863 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= c

2024/03/28 10:43:04.779879864 {iosrp_R0-0}{1}: [og] [26311]: (info): OG_PI_ACL_INFO: ogacl_configured: A

```
2024/03/28 10:43:04.780510740 {iosrp_R0-0}{1}: [parser_cmd] [26311]: (note): id= console@console:user= of the set of the
```

2024/03/28 10:43:04.786433419 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interface 2024/03/28 10:43:04.786523172 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interface 2024/03/28 10:43:04.787787313 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): RX: DHCPv4 from interface 2024/03/28 10:43:04.788160929 {wncd_x_R0-0}{1}: [sisf-packet] [19620]: (info): TX: DHCPv4 from interface 2024/03/28 10:43:04.788491833 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): TX: DHCPv4 from interface 2024/03/28 10:43:04.788576063 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): [08be.ac14.137d:capwap_9000 2024/03/28 10:43:04.788741337 {wncd_x_R0-0}{1}: [webauth-sess] [19620]: (info): Change address update, 0 2024/03/28 10:43:04.788761575 {wncd_x_R0-0}{1}: [auth-mgr-feat_acct] [19620]: (info): [08be.ac14.137d:c2 2024/03/28 10:43:04.78877999 {wncd_x_R0-0}{1}: [epm] [19620]: (info): [0000.0000.0000:unknown] HDL = 0

2024/03/28 10:43:04.789333126 {wncd_x_R0-0}{1}: [client-iplearn] [19620]: (info): MAC: 08be.ac14.137d II

2024/03/28 10:43:04.789410101 {wncd_x_R0-0}{1}: [client-orch-sm] [19620]: (debug): MAC: 08be.ac14.137d

2024/03/28 10:43:04.789622587 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : us

2024/03/28 10:43:04.789632684 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : c

2024/03/28 10:43:04.789642576 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute :Cis

2024/03/28 10:43:04.789651931 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute :bs

2024/03/28 10:43:04.789653490 {wncd_x_R0-0}{1}: [aaa-attr-inf] [19620]: (info): [Applied attribute : t 2024/03/28 10:43:04.789735556 {wncd_x_R0-0}{1}: [ew]c-qos-client] [19620]: (info): MAC: 08be.ac14.137d 2024/03/28 10:43:04.789800998 {wncd_x_R0-0}{1}: [rog-proxy-capwap] [19620]: (debug): Managed client RUN

2024/03/28 10:43:04.789886011 {wncd_x_R0-0}{1}: [client-orch-state] [19620]: (note): MAC: 08be.ac14.1370

数据包捕获

另一个有趣的反射是获取和分析客户端关联的RADIUS流的数据包捕获。可下载ACL依赖于RADIUS,不仅要分配给无线客户端,还 要由WLC下载。因此,在进行数据包捕获以排除dACL配置故障时,必须在控制器与RADIUS服务器通信所使用的接口上进行捕获。 <u>本文档</u>介绍如何在Catalyst 9800上配置轻松嵌入的数据包捕获,该数据包捕获已用于收集本文所分析的捕获。

RADIUS客户端身份验证

您可以看到从WLC发送到RADIUS服务器的客户端RADIUS访问请求,以对DACL_DOT1X_SSID SSID (AVP NAS-Identifier)上的用户 USER1 (AVP User-Name)进行身份验证。

- 480 6	517 39 10.48.39.130	10.48.39.134	Access-Request id=92, Duplicate Request	RADIUS
- 480 3	39 10.48.39.134	10.48.39.130	Access-Accept 10=92	KAUTUS
> Frame 48	035: 617 bytes on wire (4936 bits), 617 bytes c	aptured (4936 bits)	
Ethernet	II, Src: Cisco_b2:fe:ff	(00:1e:f6:b2:fe:ff), D	t: VMware_8d:01:ec (00:50:56:8d:01:ec)	
> 802.10 V	/irtual LAN, PRI: 0, DEI:	0, ID: 39		
> Internet	Protocol Version 4, Src	:: 10.48.39.130, Dst: 10	48.39.134	
	agram Protocol, Src Port	:: 63/72, DSt Port: 1812		
Code:	Access-Request (1)			
Packet	identifier: 0x5c (92)			
Length	: 571			
Authen	ticator: 3642d8733b9fb2a	c198d89e9f4f0ff71		
[Dupli	cate Request Frame Numbe	r: 48034]		
Line r	esponse to this request	15 1n Trame 48039]		
AVP:	t=User-Name(1) l=7 val=	USER1		
> AVP:	t=Service-Type(6) l=6 v	al=Framed(2)		
> AVP:	t=Vendor-Specific(26) l	=27 vnd=ciscoSystems(9)		
> AVP:	t=Framed-MTU(12) l=6 va	l=1485		
> AVP:	t=EAP-Message(79) l=48	Last Segment[1]	1-47-00 J-01LL000 J-0000	
> AVP:	t=Message-Authenticator +=EAD_Kov_Name(102) 1-2	(80) l=18 val=cdc/61262	104/6900631000693098329	
	t=Vendor-Specific(26)]	=49 vnd=ciscoSvstems(9)		
> AVP:	t=Vendor-Specific(26) l	=20 vnd=ciscoSystems(9)		
> AVP:	t=Framed-IP-Address(8)	l=6 val=10.14.13.240		
> AVP:	t=Vendor-Specific(26) l	=40 vnd=ciscoSystems(9)		
> AVP:	t=Vendor-Specific(26) l	=32 vnd=ciscoSystems(9)		
> AVP:	t=Vendor-Specific(26) l	=20 vnd=c1scoSystems(9)		
	t=NAS-IP-Autress(4) (=0 t=NAS-Port-Type(61)]=6	val=10.48.39.130		
> AVP:	t=NAS-Port(5) l=6 val=3	913		
> AVP:	t=State(24) l=71 val=33	3743504d53657373696f6e4	9443d383232373330304130303030303039463834393335	
> AVP:	t=Vendor-Specific(26) l	=39 vnd=ciscoSystems(9)		
> AVP:	t=Vendor-Specific(26) l	=41 vnd=ciscoSystems(9)		
> AVP:	t=Called-Station-Id(30)	l=35 val=f4-db-e6-5e-7	C0: DACL_DOT1X_SSID	
	t=Vendor-Specific(26)]	=12 vnd=Airespace. Inc()	4179)	
> AVP:	t=NAS-Identifier(32) l=	17 val=DACL DOT1X SSID	(41)5)	
> AVP:	t=Unknown-Attribute(187) l=6 val=000fac04		
> AVP:	t=Unknown-Attribute(186) l=6 val=000fac04		
😑 🖉 🛛 AVP (n	edius.avp), 48 bytes			 Packets: 55012 - Displayed: 2 (0.0%) - Ignored: 1 (0.0%) Profile: Defau

当身份验证成功时,RADIUS服务器会回复一个access-accept,仍然针对用户USER1 (AVP User-Name)并应用AAA属性,尤其是供应商特定AVP ACS: CiscoSecure-Defined-ACL在此为"#ACSACL#-IP-ACL_USER1-65e89aab"。



DACL下载

如果dACL已是WLC配置的一部分,则它仅分配给用户,RADIUS会话结束。否则,WLC将下载ACL,同时仍使用RADIUS。为此 ,WLC发出RADIUS访问请求,这次使用AVP用户名的dACL名称("#ACSACL#-IP-ACL_USER1-65e89aab")。此外,WLC通知 RADIUS服务器此access-accept使用Cisco AV对aaa: event=acl-download启动ACL下载。



发回控制器的RADIUS access-accept包含请求的dACL,如下所示。每个ACL规则都包含在"ip:inacl#<X>=<ACL_RULE>"的不同Cisco AVP中,<X>是规则编号。

					Packet:	Go to packet Cancel
No.	Length ID	Source	Destination	linfo		Protocol
8037	184 3	9 10.48.39.130	10.48.39.134	Access-Request id=81, Duplicate Request		RADIUS
+ 8038	369 3	9 10.48.39.134	10.48.39.130	Access-Accept id=81		RADIUS
> Frame > Ethern 000, 10	8038: 369 et II, Sr	bytes on wire (2952 c: VMware_8d:01:ec (0	bits), 369 bytes captured (7 0:50:56:8d:01:ec), Dst: Cise	2952 bits) co_b2:fe:ff (00:1e:f6:b2:fe:ff)		
> Intern	et Proto	col Version 4, Src: 10	.48.39.134, Dst: 10.48.39.13	30		
User D ~ RADIUS	atagram F Protocol	rotocol, Src Port: 18	12, Dst Port: 63772			
Code	: Access-	Accept (2)				
Leng	th: 323	(1161: 0X51 (81)				
Auth	enticator s is a re	: 61342164ce39be06eed	828b3ce566ef5 n frame 80361			
[Tim	e from re	quest: 0.007995000 se	conds]			
> AV	P: t=User	-Name(1) l=32 val=#AC	SACL#-IP-ACL_USER1-65e89aab			
> AV > AV	P: t=Clas P: t=Mess	s(25) l=75 val=434143 age-Authenticator(80)	533a30613330323738366d624251 l=18 val=a3c4b20cd1e64785d9	L7239445259673447765f436554692f48737050 De0232511cd8b72		
~ AV	P: t=Vend	lor-Specific(26) l=47	vnd=ciscoSystems(9)			
	Length: 4	7				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l=41 va	l=ip:inacl#1=denv ip anv hos	st 10.48.39.13		
~ AV	P: t=Vend	lor-Specific(26) l=47	vnd=ciscoSystems(9)			
	Length: 4	7				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l=41 va	l=ip:inacl#2=denv ip anv hos	st 10.48.39.15		
~ AV	P: t=Vend	or-Specific(26) l=48	vnd=ciscoSystems(9)			
	Length: 4	8				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l=42 va	l=ip:inacl#3=denv ip anv hos	t 10.48.39.186		
~ AV	P: t=Vend	lor-Specific(26) l=36	vnd=ciscoSystems(9)			
	Length: 3	6				
	Vendor ID VSA: t=Ci	: ciscoSystems (9) .sco-AVPair(1) l= <u>30 va</u>	l=ip:inacl#4=permit ip any a	any		
• 2 •	DILIS Protocol (re	dus). 323 bytes		- Parkar	ts: 43372 - Displayed: 2 (0.0%)	Profile: Default
	the second s				and the second sec	Provide: Delagan



注意:如果下载ACL的内容在WLC上下载后被修改,则使用此ACL的用户重新进行身份验证(并且WLC再次对此类用户 执行RADIUS身份验证)后,此ACL的更改才会反映出来。实际上,ACL名称的散列部分变化反映了ACL的变化。因此 ,下次将此ACL分配给用户时,其名称必须不同,因此ACL不能是WLC配置的一部分,应该下载。但是,在ACL更改之前 进行身份验证的客户端将继续使用上一个客户端,直到它们完全重新进行身份验证。

ISE操作日志

RADIUS客户端身份验证

操作日志显示应用了可下载ACL "ACL_USER1"的用户"USER1"的成功身份验证。故障排除的兴趣部分以红色标出。

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	USER1
Endpoint Id	08:BE:AC:14:13:7D ⊕
Endpoint Profile	Unknown
Authentication Policy	Default >> Dot1X
Authorization Policy	Default >> 802.1x User 1 dACL
Authorization Result	9800-DOT1X-USER1

Authentication Details	
Source Timestamp	2024-03-28 05:11:11.035
Received Timestamp	2024-03-28 05:11:11.035
Policy Server	ise
Event	5200 Authentication succeeded
Username	USER1
User Type	User
Endpoint Id	08:BE:AC:14:13:7D
Calling Station Id	08-be-ac-14-13-7d
Endpoint Profile	Unknown
Authentication Identity Store	Internal Users
Identity Group	Unknown
Identity Group Audit Session Id	Unknown 8227300A0000000B848ABE3F
Identity Group Audit Session Id Authentication Method	Unknown 8227300A0000000D848ABE3F dot1x
Identity Group Audit Session Id Authentication Method Authentication Protocol	Unknown 8227300A000000D848ABE3F dol1x PEAP (EAP-MSCHAPv2)
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type	Unknown 8227300A000000D848ABE3F dol1x PEAP (EAP-MSCHAPv2) Framed
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device	Unknown 8227300A000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type	Unknown 8227300A0000000D848ABE3F det1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location	Unknown 8227300A000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address	Unknown 8227300A000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type	Unknown 822730040000000D848ABE3F dot1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130 Wireless - IEEE 802.11
Identity Group Audit Session Id Authentication Method Authentication Protocol Service Type Network Device Device Type Location NAS IPv4 Address NAS Port Type Authorization Profile	Unknown 8227300A0000000B48ABE3F dol1x PEAP (EAP-MSCHAPv2) Framed gdefland-9800 All Device Types All Locations 10.48.39.130 Wireless - IEEE 802.11 9800-DOT1X-USER1

S

Steps	
11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12301	Extracted EAP-Response/NAK requesting to use PEAP instead
12300	Prepared EAP-Request proposing PEAP with challenge
12625	Valid EAP-Key-Name attribute received
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated
12318	Successfully negotiated PEAP version 0
12800	Extracted first TLS record; TLS handshake started
12805	Extracted TLS ClientHello message
12806	Prepared TLS ServerHello message
12807	Prepared TLS Certificate message
12808	Prepared TLS ServerKeyExchange message
12810	Prepared TLS ServerDone message
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
12305	Prepared EAP-Request with another PEAP challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12304	Extracted EAP-Response containing PEAP challenge- response
12305	Prepared EAP-Request with another PEAP challenge

12305 Prepared EAP-Request with another PEAP challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS ir re-using an existing session 12304 Extracted EAP-Response containing PEAP challenge-response

12318 Successfully negotiated PEAP version 0

Other Attributes	
ConfigVersionId	73
DestinationPort	1812
Protocol	Radius
NAS-Port	3913
Framed-MTU	1485
State	37CPMSessionID=8227300A000000D848ABE3F;26SessionI D=ise/499610885/35;
undefined-186	00:0f:ac:04
undefined-187	00:0f:ac:04
undefined-188	00:0f:ac:01
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	ise/499610885/35
SelectedAuthenticationIden	Internal Users
SelectedAuthenticationIden	All_AD_Join_Points
SelectedAuthenticationIden	Guest Users
AuthenticationStatus	AuthenticationPassed
AuthenticationStatus IdentityPolicyMatchedRule	AuthenticationPassed Dot1X
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched	AuthenticationPassed Dot1X 802.1x User 1 dACL
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X \$15
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency	AuthenticationPassed Det1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Det1X 515 147
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECOHE-RSA-AES256-GCM-SHA384
AuthenticationStatus IdentityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSCipher TLSVersion	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSSversion DTLSSupport	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-BE-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSSversion DTLSSupport HostIdentityGroup	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown Cisco
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName IdentitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile Location	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Unknown Endpoint Identity Groups:Unknown Cisco LocationttAll Locations
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName identitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostidentityGroup Network Device Profile Location Device Type	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSV1.2 Unknown Endpoint Identity Groups:Unknown Cisco Locationt#All Locations Device Types/All Device Types
AuthenticationStatus identityPolicyMatchedRule AuthorizationPolicyMatched EndPointMACAddress ISEPolicySetName identitySelectionMatchedRule TotalAuthenLatency ClientLatency TLSCipher TLSVersion DTLSSupport HostIdentityGroup Network Device Profile Location Device Type IPSEC	AuthenticationPassed Dot1X 802.1x User 1 dACL 08-8E-AC-14-13-7D Default Dot1X 515 147 ECDHE-RSA-AES256-GCM-SHA384 TLSV1.2 Unknown Endpoint Identity Groups:Unknown Cisco LocationHAll Locations Device TypesHAII Device Types IPSECHIS IPSEC DeviceIINo

EnableFlag	Enabled
RADIUS Username	USER1
NAS-Identifier	DACL_DOT1X_SSID
Device IP Address	10.48.39.130
CPMSessionID	8227300A000000D848ABE3F
Called-Station-ID	10-b3-c6-22-99-c0:DACL_DOT1X_SSID
CiscoAVPair	service-type=Framed, audit-session-id=8227300A000000000848ABE3F, method=dot1x, client-iif-id=2113931001, vian-id=1431, clisco-wian-ssid=DACL_DOT1X_SSID, wian-profile-name=DACL_DOT1X_SSID, AuthenticationidentityStore=Internal Users, FQSubjectName=9273480-8601-1165-996c- 525400b48521Huser1, UniqueSubjectID=94b3604f5b49b88ccfafe2f3a86c80d1979b 5c43

	Result	
	Class	CACS:8227300A000000D848ABE3F:ise/499610885/35
	EAP-Key-Name	19:66:05:40:45:8d:a0:0b:35:b3:a4:1b:ab:87:b8:72:94:16:e3:b 9:93:72:37:29:6b:c5:88:e3:b1:40:23:0a:b3:96:6f:85:82:04:0a:c 5:c5:05:d5:75:bf:12:d62:d3:6b:e0:19:cf:46:a4:29:f0:ba:65:0 6:9c:ef:3e:9f:f6
	cisco-av-pair	ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-ACL_USER1- 65e89aab
	MS-MPPE-Send-Key	
	MS-MPPE-Recv-Key	
	LicenseTypes	Essential license consumed.
	Session Events	
Г	2024-03-28 05:11:11.035	Authentication succeeded

12810	Prepared TLS ServerDone message		
12812	Extracted TLS ClientKeyExchange message		
12803	Extracted TLS ChangeCipherSpec message		
12804	Extracted TLS Finished message		
12801	Prepared TLS ChangeCipherSpec message		
12802	Prepared TLS Finished message		
12816	TLS handshake succeeded		
12310	PEAP full handshake finished successfully		
12305	Prepared EAP-Request with another PEAP challenge		
11006	Returned RADIUS Access-Challenge		
11001	Received RADIUS Access-Request		
11018	RADIUS is re-using an existing session		
12304	Extracted EAP-Response containing PEAP challenge- response		
12313	PEAP inner method started		
11521	Prepared EAP-Request/Identity for inner EAP method		
12305	Prepared EAP-Request with another PEAP challenge		
11006	Returned RADIUS Access-Challenge		
11001	Received RADIUS Access-Request		
11018	RADIUS is re-using an existing session		
12304	Extracted EAP-Response containing PEAP challenge- response		
11522	Extracted EAP-Response/Identity for inner EAP method		
11806	Prepared EAP-Request for inner method proposing EAP- MSCHAP with challenge		
12305	Prepared EAP-Request with another PEAP challenge		
11006	Returned RADIUS Access-Challenge		
11001	Received RADIUS Access-Request		
11018	RADIUS is re-using an existing session		
12304	Extracted EAP-Response containing PEAP challenge- response		
11808	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negotiated		
11808 15041	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negotiated Evaluating Identity Policy		
11808 15041 15048	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negoliated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusRiowType		
11808 15041 15048 22072	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negotiated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity source sequence - All_User_ID_Stores		
11808 15041 15048 22072 15013	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negotiated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users		
11808 15041 15048 22072 15013 24210	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negotiated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1		
11808 15041 15048 22072 15013 24210 24212	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as regolated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore		
11808 15041 15048 22072 15013 24210 24212 22037	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as required Evaluating Identity Policy Queried PIP - Normalised Radius.Radius.FlowType Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed		
11808 15041 15048 22072 15013 24210 24212 22037 11824	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as regolated Evaluating Identity Policy Queried PIP - Normalised Radius:Radius:FlowType Selected Identity source or All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as regolated Evaluating Identity Policy Queried PIP - Normalised Radius:Radius:FlowType Selected Identity source exquence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User In Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negolitated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity Source - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negoliated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity Source - Internal Users_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Request		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as required Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Received RADIUS Access-Request RADIUS is re-using an existing session		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018 12304	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negoliated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity Source - Internal Users ID Solected Identity Source - Internal Users ID Solected Identity Source - Internal Users Looking up User in Internal Users ID Store - USER1 Found User in Internal Users ID Prepared EAP-Request with another PEAP challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response containing PEAP challenge- response		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018 12304	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as regolated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Received RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response containing PEAP challenge- response		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018 12304	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as regolated Evaluating Identity Policy Queried PIP - Normalised Radius:Radius:FlowType Selected Identity source or Latter and Lyser_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge Received RADIUS Access-Challenge RADIUS is re-using an existing session Extracted EAP-Response containing PEAP challenge- response		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018 12304 11810 11814	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negoliated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity Source - Internal Users IDStore Selected Identity Source - Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge Retracted EAP-Response containing PEAP challenge- response Extracted EAP-Response for inner method containing MSCHAP challenge-response Inner EAP-MSCHAP authentication succeeded		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018 12304 11810 11814 11519	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as response for inner method and accepting EAP- MSCHAP as response for inner method software Selected Identity Policy Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Received RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response for inner method containing MSCHAP challenge-response Inner EAP-MSCHAP authentication succeeded Inner EAP-MSCHAP authentication succeeded		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018 12304 11810 11814 11519 12314	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as response for inner method and accepting EAP- MSCHAP as response for inner method software Selected identity Policy Queried PIP - Normalised Radius: Radius/IbwType Selected identity source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response for inner method containing MSCHAP challenge-response Inner EAP-MSCHAP authentication succeeded Prepared EAP-Success for inner EAP method PEAP inner method finished successfully		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11018 12304 11810 11814 11519 12314	Extracted EAP-Response for inner method and accepting EAP- MSCHAP as required Evaluating Identity Policy Queried PIP - Normalised Radius:RadiusFlowType Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Received RAD: Racess-Challenge Received RAD: Racess-Challenge Extracted EAP-Request with another PEAP challenge Received RAD: Racess-Challenge Extracted EAP-Response containing PEAP challenge- response Extracted EAP-Response for inner method containing MSCHAP challenge-response Inner EAP-MSCHAP authentication succeeded Prepared EAP-Success for inner EAP method PEAP inner method [Inished successfully Prepared EAP-Request with another PEAP challenge		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11810 11810 11814 11519 12314	Extracted EAP-Response containing EAP-MSCHAP challenge-response for inner method and accepting EAP- MSCHAP as negoliated Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Authentication Passed EAP-MSCHAP authentication attempt passed Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge Returned RADIUS Access-Challenge Extracted EAP-Response for inner method containing MSCHAP challenge-response Inner EAP-MSCHAP authentication succeeded Prepared EAP-Success for inner EAP method PEAP inner method finiahed successfully Prepared EAP-Request with another PEAP challenge returned RADIUS Access-Challenge		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11814 11519 12314 12305 11205 11206 11201	Extracted EAP-Response for inner method and accepting EAP- MSCHAP as required Evaluating Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity Source - Internal Users IDStore - All_User_ID_Stores Selected Identity Source - Internal Users IDStore - USER1 Found User In Internal Users IDStore - USER1 Found User In Internal Users IDStore - USER1 Found User In Internal Users IDStore Authentication Passed Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge Retracted EAP-Response for inner method containing MSCHAP challenge-response Iner EAP-MSCHAP authentication succeeded Prepared EAP-Success for inner EAP method PEAP inner method Initiahed successfully Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge Returned RADIUS Access-Challenge Reteried EAP-Request with another PEAP challenge Reteried EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11001 11814 11519 12314 12305 11006 11001	Extracted EAP-Response for inner method and accepting EAP- MSCHAP as required and accepting EAP- MSCHAP as required Radius.RadiusFlowType Selected Identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected Identity source sequence - All_User_ID_Stores Selected Identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore Authentication Passed Prepared EAP-Request with another PEAP challenge Received RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response for inner method containing MSCHAP challenge-response Inner EAP-MSCHAP authentication succeeded Prepared EAP-Success for inner EAP method PEAP inner method finished successfully Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge Returned RADIUS Access-Challenge Returned RADIUS Access-Challenge		
11808 15041 15048 22072 15013 24210 24212 22037 11824 12305 11006 11810 11814 11519 12314 12305 11006 11001 11018	Extracted EAP-Response for inner method and accepting EAP- MSCHAP as negoliated Evaluating identity Policy Queried PIP - Normalised Radius.RadiusFlowType Selected identity source sequence - All_User_ID_Stores Selected identity Source - Internal Users Looking up User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Found User in Internal Users IDStore - USER1 Prepared EAP-Request with another PEAP challenge Returned RADIUS Access-Challenge Retracted EAP-Response for inner method containing MSCHAP authentication succeeded Prepared EAP-Response for inner method containing MSCHAP Authentication succeeded Prepared EAP-Success for inner EAP method PEAP inner method finished successfully Prepared EAP-Success - Request Returned RADIUS Access-Request Returned RADIUS Access-Request Returned RADIUS Access-Challenge Returned RADIUS Access-Challenge Returned RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Request with another PEAP challenge Returned RADIUS Access-Request RADIUS Access-Request RADIUS ACCESS-Request RADIUS is re-using an existing session Extracted EAP-Response containing PEAP challenge- response		

15036 Evaluating Authorization Policy

22081 Max sessions policy passed 22080 New accounting session created in Session cache 12306 PEAP authentication succeeded 11503 Prepared EAP-Success 11002 Returned RADIUS Access-Accept

 24209
 Looking up Endpoint in Internal Endpoints IDStore -USER1

 24211
 Found Endpoint in Internal Endpoints IDStore

 15048
 Queried PIP - Network Access.UserName

 15048
 Queried PIP - InternalUser.Name

 15016
 Selected Authorization Profile - 9800-DOTIX-USER1

 11022
 Added the dACL specified in the Authorization Profile

DACL下载

操作日志显示ACL "ACL_USER1"成功下载。故障排除的兴趣部分以红色标出。

Cisco ISE

Overview					
Event	5232 DACL Download Succeeded				
Username	#ACSACL#-IP-ACL_USER1-65e89aab				
Endpoint Id					
Endpoint Profile					
Authorization Result					
Authentication Details					
Source Timestamp	2024-03-28 05:43:04.755				
Received Timestamp	2024-03-28 05:43:04.755				
Policy Server	ise				
Event	5232 DACL Download Succeeded				
Username	#ACSACL#-IP-ACL_USER1-65e89aab				
Network Device	gdefland-9800				
Device Type	All Device Types				
Location	All Locations				
NAS IPv4 Address	10.48.39.130				
Response Time	1 milliseconds				
Other Attributes					
ConfigVersionId	73				
DestinationPort	1812				
Protocol	Radius				
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c				
IsThirdPartyDeviceFlow	false				
AcsSessionID	ise/499610885/48				
TotalAuthenLatency	1				
ClientLatency	0				
DTLSSupport	Unknown				
Network Device Profile	Cisco				
Location	Location#All Locations				
Device Type	Device Type#All Device Types				
IPSEC	IPSECIIIs IPSEC Device#No				
RADIUS Username	#ACSACL#-IP-ACL_USER1-65e89aab				
Device IP Address	10.48.39.130				
CPMSessionID	0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfdFbcs eM				
CiscoAVPair	aaa:service=ip_admission, aaa:event=acl-download				
Result					
Class	CACS:0a302786pW4sgAjhERVzOW2a4lizHKqV4k4gukE1upAfd FbcseM:ise/499610885/48				
cisco-av-pair	ip:inacl#1=deny ip any host 10.48.39.13				
cisco-av-pair	ip:inacl#2+deny ip any host 10.48.39.15				
cisco-av-pair	ip:inacl#3=deny ip any host 10.48.39.186				
cisco-av-pair	ip:inacl#4+permit ip any any				

Steps

11001	Received	RADIUS	Access-Request

- 11017 RADIUS created a new session 11117 Generated a new session ID 11102 Returned RADIUS Access-Accept

1

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)。