在ISE中配置使用OCSP的EAP-TLS身份验证

 _
~

<u>先决条件</u>
· · · · · · · · · · · · · · · · · · ·
<u>使用的组件</u>
网络图
<u>C1000中的配直</u>
Windows PC中的配置
<u> </u>
<u>Windows Server屮的配直</u> 生要1·汤加田白
<u>27秋山水加市)</u> 第二步:确认OCSP服务
<u>10日中的配置</u> 步骤1:添加设备
第二步:添加Active Directory
<u>第四步:添加身份源隔离</u>
<u>第五步:在ISE中配置证书</u>
<u>第六步:添加允许的协议</u>
<u>步骤 7.添加策略集</u>
<u>步骤 8添加身份验证策略</u>
<u>步骤 9添加授权策略</u>
<u>验证</u>
步骤1:确认身份验证会话
<u>第二步:确认Radius实时日志</u>
<u>故障排除</u>
<u>1. 调试日志</u>
<u>2. TCP转储</u>
<u>相关信息</u>

简介

本文档介绍设置使用OCSP的EAP-TLS身份验证以进行实时客户端证书撤销检查所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题:

- 思科身份服务引擎的配置
- Cisco Catalyst的配置
- 在线证书状态协议

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 身份服务引擎虚拟3.2补丁6
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2016
- Windows 10

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。

网络图

下图显示本文档示例中使用的拓扑。



网络图

背景信息

在EAP-TLS中,客户端在身份验证过程中向服务器提供其数字证书。本文档介绍ISE如何验证客户

端证书,方法是针对AD服务器检查证书公用名(CN),并使用OCSP(在线证书状态协议)确认证书 是否已吊销,OCSP提供实时协议状态。

在Windows Server 2016上配置的域名是ad.rem-xxx.com,本文档中将其用作示例。

本文档中引用的OCSP (在线证书状态协议)和AD (Active Directory)服务器用于证书验证。

- · Active Directory FQDN : winserver.ad.rem-xxx.com
- CRL分布URL: <u>http://winserver.ad.rem-xxx.com/ocsp-ca.crl</u>
- 颁发机构URL: <u>http://winserver.ad.rem-xxx.com/ocsp</u>

这是证书链,带有文档中使用的每个证书的公用名称。

- CA : ocsp-ca-common-name
- 客户端证书:clientcertCN
- 服务器证书:ise32-01.ad.rem-xxx.com
- OCSP签名证书: ocspSignCommonName

配置

C1000中的配置

这是C1000 CLI中的最低配置。

aaa new-model

radius server ISE32 address ipv4 1.x.x.181 key cisco123

aaa group server radius AAASERVER server name ISE32

aaa authentication dot1x default group AAASERVER aaa authorization network default group AAASERVER aaa accounting dot1x default start-stop group AAASERVER dot1x system-auth-control

interface Vlan12 ip address 192.168.10.254 255.255.255.0

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

interface GigabitEthernet1/0/3
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto

dot1x pae authenticator
spanning-tree portfast edge

Windows PC中的配置

步骤1:配置用户身份验证

导航到身份验证,选中启用IEEE 802.1X身份验证,然后选择Microsoft:智能卡或其他证书。 单击"设置"按钮,选中"在此计算机上使用证书",然后选择"Windows PC的受信任CA"。

pciPassthru0 Properties	× Smart Card or other Certificate Properties ×
Networking Authentication Select this option to provide authenticated network access for this Ethemet adapter. Enable IEEE 802.1X authentication Choose a network authentication method:	When connecting:
Microsoft: Smart Card or other certificate <	Trusted Boot Certification Authorities:
	View Certificate
	Don't grompt user to authorize new servers or trusted certification authorities.
OK Cancel	Use a different user name for the connection

启用证书身份验证

导航到身份验证,选择其他设置。选择User or computer authenticationfrom下拉列表。

pciPassthru0 Properties ×	Advanced settings ×
Networking Authentication	802. 1X settings
Select this option to provide authenticated network access for this Ethemet adapter.	Specify authentication mode User or computer authentication Save credentials Delete credentials for all users
Microsoft: Smart Card or other certificate Remember my credentials for this connection each time I'm logged on	Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): Allow additional dialogs to be displayed during single
Eallback to unauthorized network access	sign on This network uses separate virtual LANs for machine and user authentication
OK Cancel	OK Cancel

指定身份验证模式

第二步:确认客户端证书

导航到证书-当前用户>个人>证书,并检查用于身份验证的客户端证书。

Console1 - [Console Root\Certificates - Current User\Personal\Certificates]								-	
hile Action View Favorites Window Help									- @ ×
← → 2 🔟 4 % 🗙 🖾 🖦 🖬 📷									
Console Root ^ Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te	Action	s	
Certificates - Current User	inter-	0/14/2024	C	10.71.170.10			Certifi	cates	
Certificates	ocsp-ca-common-name	6/4/2025	Client Authentication	ocsp-client			M	ore Actions	•
Trusted Root Certification Authorities Certificates							cliento	ertCN	-
> 🛅 Enterprise Trust							M	ore Actions	,

确认客户端证书

双击客户端证书,导航到详细信息,检查主题、CRL分发点和授权信息访问的详细信息。

- 主题:CN = clientcertCN
- CRL分发点:<u>http://winserver.ad.rem-xxx.com/ocsp-ca.crl</u>
- 授权信息访问:<u>http://winserver.ad.rem-xxx.com/ocsp</u>



客户端证书的详细信息

Windows Server中的配置

步骤1:添加用户

导航到Active Directory用户和计算机,然后单击用户。添加clientcertCN作为用户登录名。

clientcert CN Properties	? X	clientcert CN Propertie	25			?	\times
Member Of Dial-in Environment Remote control Remote Desktop Services Profile General Address Account Profile Telephones User logon name: @ad rem-s, : sm.com User logon name (pre-Windows 2000): AD\ Log On To Log On To Uplock account Account gptions:	Sessions COM+ Organization	Remote control General Address Member Of Member of: Name Domain Admins Domain Users	Remote I Account Dial-in Active Direct ad.rem-s	Desktop Se Profile Envi ory Domain m.com/Use m.com/Use	arvices Profile Telephones ironment	COI Organiz Session	M+ ation ns
User must change password at next logon User cannot change password Password never expires Store password using reversible encryption Account expires	~	Add E	emove omain Users There is r	no need to o	change Primary o	roup unle	55
Never End of: Friday , July 5, 2024 OK Cancel Apply	Help	Set Primary Group	you have applicatio	Macintosh ns.	Clients or POSIX	complian	lp

用户登录名

第二步:确认OCSP服务

导航到Windows,点击Online Responder Management。确认OCSP服务器的状态。



OCSP服务器的状态

单击winserver.ad.rem-xxx.com,检查OCSP签名证书的状态。

Pocsp - [Online Responder: winserver.ad.rem-system.com\Array Configuration\winserver.ad.rem-system.com]

💠 🔿 🖄			
 Online Responder: winserver.ad.rem-s,::h.m.com Revocation Configuration Array Configuration Winserver.ad.rem-t_sie.n.com 	Revocation Configuration Name ocsp-revocation	Certificate Certification Path Certification gath Certification gath Certification gath Certificate gatus: This certificate is OK.	ew Certificate
	Revocation Configuration Status	us provider	OK

OCSP签名证书的状态

ISE中的配置

步骤1:添加设备

导航到管理>网络设备,点击添加按钮以添加C1000设备。

				Ac	Iministration - Netw	ork Resources		
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors	Location Services
Network Devices Default Device Device Security Settings	Network Devices Lis	x > C1000 CeS						
	Namo	C1000						
	Description							
	IP Address	 *™: 1.1 %, %101 	/					
	Device Profile	# Cisco	× 0					
	Model Name		~					
	Software Versio	n	~					
	Network Device	e Group						
	Location	All Locations	✓ Set To	Default				
	IPSEC	No	✓ Set To	Default				
	Device Type	All Device Types	✓ Set To	Default				
	RAL	DIUS Authentication Setti	ngs					
	RADIU	JS UDP Settings						
	Protoc	ol RADIUS						
	Shared	d Secret cisco123	Hid	e				
	- u	se Second Shared Secret 🕕						

添加设备

第二步:添加Active Directory

导航到管理>外部身份源> Active Directory,点击连接选项卡,将Active Directory添加到ISE。

- 加入点名称: AD_Join_Point
- Active Directory域: ad.rem-xxx.com

≡ Cisco ISE	Administration - Identity Management
Identities Groups External Ide	Intity Sources Identity Source Sequences Settings
External Identity Sources	Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
< Tel Certificate Authentication F < Tel Active Directory	* Join Point Name AD_Join_Point ① * Active Directory ad.rem-s_t*'(n.com ①
AD_Join_Point LDAP ODBC	+ Join + Leave A Test User 🕺 Diagnostic Tool 💋 Refresh Table
RADIUS Token	□ ISE Node ∧ ISE Node R Status Domain Controller Site
RSA SecurID	ise32-01.ad.rem-sy .sm.c STANDALONE 🗹 Operational winserver.ad.rem-s, ste Default-First-Site-Na
 SAML Id Providers Social Login 	

添加Active Directory

导航到组选项卡,从下拉列表中选择选择目录中的组。

≡ Cisco ISE					Administration - Identity Management				
lde	entities	Groups	External Ide	entity Sources	Identity Source Sequences	Settings			
	External Id	entity Sources	s	Connection	Allowed Domains PassivelD	Groups	Attributes	Advanced Settings	
		Certificate Auth	entication (🖉 Edit 🕇	Add 🔿 📋 Delete Group Update S	SID Values			
	~ •	Active Directory	y		Select Groups From Directory	~ 1	SID		

从目录中选择组

单击Retrieve Groupsfrom下拉列表。Checkad.rem-xxx.com/Users/Cert Publishers,然后单击 OK。

E Cisco ISE		Administration - Identity Management	
Identifies Groups External Identify Sources	Connection Allowed Dom	Select Directory Groups This diatog is used to select groups from the Directory. Domain adverse; 1 s.com Name, SID, Type au	×
Active Directory	Name	Fiber Fiber Fiber	
AD_Join_Point	ad.rem-system.com	Review Groups	
C LOAP		Name Group SID Group Type	
COBC		ad rem-rs; / m.com/Ukers/Moved R000 Pass 5-1-5-21-4193743415-4133520008-20482399 DOMAIN LOCAL	^
E RADIUS Taken		atiremite it incom/Users/Cert Publishers 5-1-5-21-4193743415-4133520026-20462399 DOMAIN LOCAL	1
C SAME to Providers		adven-ey'r m.com/Ukers/Cloneste Domin C 5-1-5-21-4193743415-4133520026-30462399 GLOBAL	
Social Login		adven-sym.com/Users/Deried R000 Passe. 5-1-5-21-4193743415-413352020-20462399 DOMAN LOCAL	
		ad rem-sy im.com/bars/0xaAdmins 5-1-5-21-4193742415-4133520205-20482399 DOMAIN LOCAL	
		ad rem-s + sm.com/likers/DmillodeteProxy 5-1-5-21-4193743415-413352028-20462399 GL084L	
	×	ad rem-s), 2, 3m.com/Ukers/Domain Admins 5-1-5-21-4193742415-4133520028-20482399 GL08AL	i - 1
		ad rem-er 11 m.com/Ukers/Domein Computers 5-1-5-21-4193742415-4133520026-20442299 GLOBAL	
		adven-sys + Lion/Users/Donain Controllers 5-1-5-21-4193743415-4133520026-20462399 GL084L	1 I
		ad rem-ey, n. n. con/Users/Domain Guests 5-1-5-21-4193743415-4133520026-30462399. GL0BAL	
		adven-e-1 m.com/Users/Domain Users 5-1-5-21-4193782415-4133520208-20482399 GLOBAL	~
		Cancel	

检查证书发布者

第三步:添加证书身份验证配置文件

导航到Administration > External Identity Sources > Certificate Authentication Profile,点击Add按 钮以添加新的证书身份验证配置文件。

- 名称 : cert_authen_profile_test
- 身份库: AD_Join_Point
- 使用来自证书属性的身份:主题-公用名。
- Match Client Certificate Against Certificate In Identity Store:仅用于解决身份模糊问题。

Cisco ISE	Administration - Identity Management
Identities Groups External Id	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profiles List > cert_authen_profile_test Certificate Authentication Profile
<pre>ect_authen_profile_test</pre>	* Name cert_authen_profile_test
Preloaded_Certificate_Prof Active Directory AD_Join_Point LDAP	Description
C ODBC	Identity Store AD_Join_Point V
RADIUS Token	
RSA SecurID SAML Id Providers Social Login	Use Identity From Certificate Attribute Subject - Common Name
	Match Client Certificate Against Certificate In Identity Store () Only to resolve identity ambiguity Always perform binary comparison

添加证书身份验证配置文件

第四步:添加身份源隔离

导航到管理>身份源序列,添加身份源序列。

- 名称 : Identity_AD
- 选择Certificate Authentication Profile: cert_authen_profile_test
- 身份验证搜索列表: AD_Join_Point

Cisco ISE

Identities	Groups	External Identity Sources	Identity Source Sequences	Settings
Identity Source	Sequences Lis	t > Identity_AD		
~ Identity	/ Source S	equence		
Description	Ident	ity_AD		
✓ Certifi	cate Base	d Authentication		_A.
🔽 Se	lect Certificate	Authentication Profile cert_at	uthen_profil~	

✓ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected	
Internal Endpoints	^	AD_Join_Point	^
Internal Users			
Guest Users			
All_AD_Join_Points	\geq		
	>>		
			

添加身份源序列

第五步:在ISE中配置证书

导航到管理>证书>系统证书,确认服务器证书由受信任CA签署。

E Cisco ISE	Administration - System	🛦 Evaluation Mode 1 : Days Q 🕥 🗔 🔅
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings	
Certificate Management ~ System Certificates	Dufauft self-signed samt server cer SAML tificate - CN-SAML_ise32-01.ad.rem-sy m.co Thu, 2 May 2024 m-sy am.com m-sy am.com	Tue, 1 May 2029 Z
Trusted Certificates OCSP Client Profile Certificate Signing Requests	CN+16e32-01.ad.rem-#_ em.com, ISE Messaging Service lae32-01.ad.rem-#j, I m.com Certificate Services Endpoint Sub C. Wed, 1 May 2024 OU+ISE Messaging Service#Certific ass Services Endpoint Sub CA - Ise 32-01800001	Wed, 2 May 2029
Certificate Periodic Check Se	CN+16e32-01.ad.rem-s), 1 m.com, Not In use Ise32-01.ad.rem-s), em.com Centificate Services Endpoint Sub C. Wed, 1 May 2024 OU-Cartificate Services Endpoint Sub C. Wed, 1 May 2024 Interactive Company Company Services Endpoint Sub C. Wed, 1 May 2024	Wed, 2 May 2029 Scrive
Geruficate Authority	CN4-ise32-01.ad.rem-s, i m.com# Portal Default Portal Certificate Group () ise32-01.ad.rem-sy im.com rootCACommonName Tue, 4 Jun 2024 rootCACommonName#00004	Wed, 4 Jun 2025
	Ise-server-cert-friendly-name Admin, CAP () Ise32-01.ad.rem-s xt m.com ocsp-ca-common-name Administration, Administration, Administration, BANets OTLS, pedint, Portst	Wed, 4 Jun 2025

服务器证书

导航到管理>证书> OCSP客户端配置文件,单击"添加"按钮以添加新的OCSP客户端配置文件。

- 名称:ocsp_test_profile
- 配置OCSP响应程序URL: <u>http://winserver.ad.rem-xxx.com/ocsp</u>

≡ Cisco ISE	Administration - System
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings
Certificate Management ~ System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Se	Edit OCSP Profile * Name ocsp_test_profile Description
Certificate Authority	 Server Connection Enable Secondary Server Always Access Primary Server First Failback to Primary Server After Interval 5 Minutes 0
	✓ Primary Server * URL http:// r.ad.rem-t_ts'sm.com/ocspl ① URL http:// ① Image: Server URL http:// 0 0 Image: Server URL http:// 0 Image: Server URL http:// 0 Image: Validate Response Signature Image: Server
	Use OCSP URLs specified in Authority Information Access (AIA) Enable Nonce Extension Support Validate Response Signature
OCSP客户端配置文件	Kesponse Cache Clear Cache Clear Cache

导航到管理>证书>受信任证书,确认受信任CA已导入到ISE。

Cisco ISE				Administra	tion - System				A Evaluation Mode Days Q 🛞 🧔
Deployment Licensing	Certificate	s Logging Maintenance	Upgrade Health	Checks Bac	kup & Restore Admin A	ccess Settings			
		Cisco Manufacturing CA SHA2	Infrastructure	02	Cisco Manufacturing CA SH	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2	Enabled
Certificate Management \sim		Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2	Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Tue, 15 May 2	Disabled
System Certificates		Cisco Root CA 2099	Cisco Services	01 9A 33 58 7	Cisco Root CA 2099	Cisco Root CA 2099	Wed, 10 Aug 2016	Mon, 10 Aug	Enabled
Trusted Certificates OCSP Client Profile		Cisco Root CA M1	Cisco Services	2E D2 0E 73 4	Cisco Root CA M1	Cisco Root CA M1	Wed, 19 Nov 2008	Sat, 19 Nov 2	Enabled
Certificate Signing Requests		Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2	Enabled
Certificate Periodic Check Se		Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Mon, 10 Jul 2	Enabled
Certificate Authority		CN=root_ca_common_name, OU=cisc	Infrastructure Cisco Services Endpoints AdminAuth	20 BF 12 86 F	root_ca_common_name	root_ca_common_name	Thu, 16 May 2024	Tue, 16 May 2	Enabled
		CN=rootCACommonName#rootCACom	Infrastructure Cisco Services Endpoints AdminAuth	21 31 D3 DE	rootCACommonName	rootCACommonName	Tue, 4 Jun 2024	Sun, 4 Jun 20	Enabled
		Default self-signed server certificate	Endpoints Infrastructure	37 66 FC 29	ise32-01.ad.rem-system.com	ise32-01.ad.rem-system.com	Thu, 2 May 2024	Sat, 2 May 20	Enabled
		DigiCert Global Root CA	Cisco Services	08 38 E0 56 9	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov	Enabled
		DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6	DigiCert Global Root G2	DigiCert Global Root G2	Thu, 1 Aug 2013	Fri, 15 Jan 20	Enabled
		DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26	DigiCert High Assurance EV	DigiCert High Assurance EV	Fri, 10 Nov 2006	Mon, 10 Nov	Enabled
		DigiCert SHA2 High Assurance Server	Endpoints Infrastructure	04 E1 E7 A4	DigiCert SHA2 High Assuran	DigiCert High Assurance EV	Tue, 22 Oct 2013	Sun, 22 Oct 2	Enabled
		IdenTrust Commercial Root CA 1	Cisco Services	0A 01 42 80 0	IdenTrust Commercial Root	IdenTrust Commercial Root	Fri, 17 Jan 2014	Tue, 17 Jan 2	Enabled
		ocsp-ca-friendly-name	Cisco Services Endpoints	1A 12 1D 58	ocsp-ca-common-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Sun, 4 Jun 20	Enabled

受信任的CA

选中CA并单击Edit按钮,输入用于证书状态验证的OCSP配置详细信息。

- 根据OCSP服务进行验证:ocsp_test_profile
- 如果OCSP返回UNKNOWN状态,则拒绝请求:检查
- 如果OCSP响应器无法访问,则拒绝请求:检查

Cisco ISE		Administration - System
Deployment Licensing	Certificates Logging Ma	aintenance Upgrade Health Checks Backup & Restore Admin Access Settings
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Se	* Friendly Name Status Description Subject	e ocsp-ca-friendly-name Enabled \checkmark t CN=ocsp-ca-common-name
Certificate Authority >	Issuer Valid From Valid To (Expiration) Serial Number Signature Algorithm Key Length Usage	 CN=ocsp-ca-common-name Tue, 4 Jun 2024 13:52:00 JST Sun, 4 Jun 2034 13:52:00 JST r 1A 12 1D 58 59 6C 75 18 SHA256withRSA 2048
	Certificate Status Validation	Trusted For: () Image: Trust for authentication and Syslog Image: Trust for certificate based admin authentication Trust for authentication of Cisco Services
		To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first. OCSP Configuration Validate against OCSP Service ocsp_test_profile Reject the request if OCSP returns UNKNOWN status Reject the request if OCSP Responder is unreachable Certificate Revocation List Configuration Download CRL
		CRI, Distribution URI, Retrieve CRI. O Every 1 Minutes V before expiration. Hours V
证书状态验证		If download failed, wait 10 Minutes Sefere retry.

第六步:添加允许的协议

导航到策略>结果>身份验证>允许的协议,编辑默认网络访问服务列表,然后选中允许EAP-TLS。

Cisco ISE

Policy · Policy Elements

Dictionaries	Conditions	Results
Authentication Allowed Protocols	Ť	Allowed Protocols Services List > Default Network Access Allowed Protocols
Authorization	>	Name: Default Network Access
Profiling	>	Description Default Allowed Protocol Service
Posture	>	
Client Provisioning	>	 Allowed Protocols
		Authentication Bypass
		C Process Host Lookup 🕡
		Authentication Protocols
		Allow PAP/ASCII
		Allow CHAP
		Allow MS-CHAPVI
		Allow MS-CHAPV2
		A Rev EAP-MDS
		Allow EAP-ILS
		Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ()
		Enable Stateless Session Resume
		Session ticket time to live 2 Mours >>
		so the to the last spire
		Allow LEAP
		V Allow PEAP
		PEAP Inner Methods
		Allow EAP-MS-CHAPv2
		Allow Password Change Retries 1 (Valid Range 0 to 3)
		Allow EAP-GTC
		Allow Password Change Retries 1 (Valid Range 0 to 3)
		Allow EAP-TLS
		Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy
		0
		Require cryptobinding TLV ()
		Allow PEAPv0 only for legacy clients



步骤 7.添加策略集

导航到策略>策略集,点击+添加策略集。

- 策略集名称: EAP-TLS-Test
- 条件:网络访问协议等于RADIUS
- 允许的协议/服务器序列:默认网络访问

≡ Cisco ISE	Policy - Policy Sets	🛕 Evaluation Mode :) Days Q 💿 🖼 🚳
Policy Sets		Reset Policyset Hitcounts Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
Edillizion	2 Network Access Protocol EQUALS RADIUS	Default Network Access 🥒 + 25 🚳 🕨

添加策略集

步骤 8添加身份验证策略

导航到策略集,点击EAP-TLS-Tests以添加身份验证策略。

- 规则名称: EAP-TLS-Authentication
- 条件:网络访问EapAuthentication 等于EAP-TLS 和Wired_802.1 X
- 使用:Identity_AD

\sim Authentication Policy (2)					
(Status Rule Name	Co	nditions	Use	Hits	Actions
Q Search					
	C	Network Access EspAuthentication EQUALS EAP-TLS	Identity_AD	1	
CAP-TLS-Author	ntication AND	0 [] Wired_802.1X	> Options	26	츟

添加身份验证策略

步骤 9添加授权策略

导航到策略集,点击EAP-TLS-Test添加授权策略。

- 规则名称: EAP-TLS-Authorization
- 条件:证书使用者-公用名等于clientcertCN
- 结果:PermitAccess

\sim Authorization P	olicy (2)					
			Results			
• Status	Rule Name	Conditions	Profiles	Security Groups	Hit	s Actions
Q Search						
٥	EAP+TLS+Authorization	L CERTIFICATE Subject - Common Name EQUALS clientcenCN	PermitAccess	Select from list	2 + 11	\$

添加授权策略

验证

步骤1:确认身份验证会话

运行show authentication sessions interface GigabitEthernet1/0/3 details命令,确认C1000中的身份验证会话。

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/3 details

Interface: GigabitEthernet1/0/3 MAC Address: b496.9114.398c IPv6 Address: Unknown IPv4 Address: 192.168.10.10 User-Name: clientcertCN Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Restart timeout: N/A Periodic Acct timeout: N/A Session Uptime: 111s Common Session ID: 01C20065000000933E4E87D9 Acct Session ID: 0x00000078 Handle: 0xB6000043 Current Policy: POLICY_Gi1/0/3 Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list: Method State

dot1x Authc Success

第二步:确认Radius实时日志

在ISE GUI中导航到操作> RADIUS >实时日志,确认身份验证的实时日志。

=	Cisco ISE						Operations - RADIUS				Q () (,a ø
Live I	.ogs Live Sessions											
Misco	onfigured Supplicants 🕕			Misconfig	ured Network Devices 🕕		RADIUS	S Drops 🕕	Client Stopped Responding ①		Repeat Cou	inter 🕕
	0				0			0	0		0	
ø	Seset Repeat Counts	₫ Export To ∨							Refresh Never	Show Latest 50 recov	Within Last 24 h Filter V	ours 🗸
	Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorizatio	IP Address	
\times			~	-	Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Pr	IP Address	~
	Jun 05, 2024 09:43:36.3	•	à	0	clientcentCN	B4:96:91:14:3	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authoria	tation PermitAccess	192.168.10.1	10
	Jun 05, 2024 09:43:33.2	•	à		clientcertCN	B4:96:91:14:3	Intel-Device	EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authoriz	ation PermitAccess		

Radius实时日志

确认身份验证的详细实时日志。

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C ①
Endpoint Profile	Intel-Device
Authentication Policy	EAP-TLS-Test >> EAP-TLS-Authentication
Authorization Policy	EAP-TLS-Test >> EAP-TLS-Authorization
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-06-05 09:43:33.268
Received Timestamp	2024-06-05 09:43:33.268
Policy Server	ise32-01
Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C
Calling Station Id	B4-96-91-14-39-8C
Endpoint Profile	Intel-Device
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C20065000000933E4E87D9
Other Attributes	
ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C2006500000933E4E87D9;31SessionI D=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s;=:em.com
AD-User-Candidate- Identities	clientcertCN@ad.rem-sy:.tem.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN,CN=Users,DC=ad,DC=rem- st-ctem,DC=com
AD-User-DNS-Domain	ad.rem-st : tem.com
AD-User-NetBios-Name	AD
IsMachineldentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy:::+m.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy*t;.m.com
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
Subject	CN=clientcertCN

CN+ocsp-ca-common-name

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 12502 Extracted EAP-Response containing EAP-TLS challengeresponse and accepting EAP-TLS as negotiated 12800 Extracted first TLS record; TLS handshake started 12545 Client requested EAP-TLS session ticket The EAP-TLS session ticket received from supplicant 12542 while the stateless session resume is disabled. Performing full authentication 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12809 Prepared TLS CertificateRequest message 12810 Prepared TLS ServerDone message 12505 Prepared EAP-Request with another EAP-TLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12504 Extracted EAP-Response containing EAP-TLS challengeresponse 12988 Take OCSP servers list from OCSP service configuration - certificate for clientcertCN 12550 Sent an OCSP request to the primary OCSP server for the CA - External OCSP Server 12553 Received OCSP response - certificate for clientcertCN 12554 OCSP status of user certificate is good - certificate for clientcertCN 12811 Extracted TLS Certificate message containing client certificate 12812 Extracted TLS ClientKevExchange message 12813 Extracted TLS CertificateVerify message 12803 Extracted TLS ChangeCipherSpec message 24432 Looking up user in Active Directory - AD_Join_Point 24325 Resolving identity - clientcertCN 24313 Search for matching accounts at join point - ad.rems' em.com 24319 Single matching account found in forest - ad.rem-s,. :-m.com 24323 Identity resolution detected single matching account 24700 Identity resolution by certificate succeeded -AD_Join_Point 22037 Authentication Passed 12506 EAP-TLS authentication succeeded 24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore clientcertCN 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore clientcertCN 24211 Found Endpoint in Internal Endpoints IDStore 15016 Selected Authorization Profile - PermitAccess 22081 Max sessions policy passed 22080 New accounting session created in Session cache 11503 Prepared EAP-Success

11002 Returned RADIUS Access-Accept

Issuer

Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP Callback -

starting OCSP request to primary

,SSL.cpp:1444 Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Start processing OCSP request

,

URL=<u>http://winserver.ad.rem-xxx.com/ocsp</u>

, use nonce=1,0cspClient.cpp:144

Crypto, 2024-06-05 09:43:33, 104, DEBUG, 0x7f9822961700, NIL-CONTEXT, Crypto::Result=0, Crypto.0cspClient::pe

Received OCSP server response

,0cspClient.cpp:411 Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.0cspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

User certificate status: Good

,OcspClient.cpp:598
Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP C

perform OCSP request succeeded

, status: Good,SSL.cpp:1684

// Radius session
Radius,2024-06-05 09:43:33,120,DEBUG,0x7f982d7b9700,cntx=0000017387,sesn=ise32-01/506864164/73,CPMSessi

Code=1(AccessRequest)

Identifier=238 Length=324 [1] User-Name - value: [

clientcertCN

] [4] NAS-IP-Address - value: [1.x.x.101] [5] NAS-Port - value: [50103] [24] State - value: [37CPMSessionID=01C20065000000933E4E87D9;31SessionID=ise32-01/506864164/73;] [87] NAS-Port-Id - value: [GigabitEthernet1/0/3]

Radius, 2024-06-05 09:43:33, 270, DEBUG, 0x7f982d9ba700, cntx=0000017387, sesn=ise32-01/506864164/73, CPMSessi

Code=2(AccessAccept)

Identifier=238 Length=294
[1] User-Name - value: [clientcertCN]

Radius, 2024-06-05 09:43:33, 342, DEBUG, 0x7f982d1b6700, cntx=0000017401, sesn=ise32-01/506864164/74, CPMSessie

Code=4(AccountingRequest)

```
Identifier=10 Length=286
[1] User-Name - value: [clientcertCN]
[4] NAS-IP-Address - value: [1.x.x.101]
[5] NAS-Port - value: [50103]
[40] Acct-Status-Type - value: [Interim-Update]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/3]
[26] cisco-av-pair - value: [audit-session-id=01C2006500000933E4E87D9]
[26] cisco-av-pair - value: [method=dot1x] ,RADIUSHandler.cpp:2455
```

Radius, 2024-06-05 09:43:33, 350, DEBUG, 0x7f982e1be700, cntx=0000017401, sesn=ise32-01/506864164/74, CPMSessi

Code=5(AccountingResponse)

Identifier=10 Length=20,RADIUSHandler.cpp:2455

2. TCP转储

在ISE中的TCP转储中,您希望查找有关OCSP响应和Radius会话的信息。

OCSP请求和响应:

No.	Time	Identification	Source	S.Port Destination	D.Port Time to L	ve Protocol	Length TC	P.Se Next se 1	CP.Ac Info
+	140 2024-06-05 00:43:33.093523	0x0295 (661)	1.1181	25844 1.: 1	80	64 OCSP	262	1 197	1 Request
•	141 2024-06-05 00:43:33.104108	0x0117 (279)	1.1 ? 0.57	80 1.1 181	25844	128 OCSP	1671	1 1607	197 Response

OCSP请求和响应的数据包捕获

>	Frame 141: 1671 bytes on wire (13368 bits), 1671 bytes captured (13368 bits)						
>	Ethernet II, Src: VMware_98:c9:91 (00:50:56:98:c9:91), Dst: VMware_98:57:1c (00:50:56:98:57:1c)						
>	Internet Protocol Version 4, Src: 1.1 . 1.57, Dst: 1.131.1.181						
>	Transmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605						
>	Hypertext Transfer Protocol						
v	Online Certificate Status Protocol						
	responseStatus: successful (0)						
	✓ responseBytes						
	ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)						
	✓ BasicOCSPResponse						
	✓ tbsResponseData						
	> responderID: byKey (2)						
producedAt: Jun 5, 2024 09:43:33.000000000							
✓ responses: 1 item							
	✓ SingleResponse						
	> certStatus: good (0)						
	cmisopdate: Jun 4, 2024 16:05:00.000000000						
	nextUpdate: Jul 4, 2024 16:05:00.000000000						
	responseExtensions: 1 item						

捕获OCSP响应的详细信息

Radius会话:

146 2024-06-05 00:43:33.118175	0x9bc6 (39878)	1.100.101	67181 1.1 7	1645	255 RADIUS	366	Access-Request id=238
185 2024-06-05 00:43:33.270244	0x033d (829)	1.1	67181 1	1645	64 RADIUS	336	Access-Accept id=238
187 2024-06-05 00:43:33.341233	0x9bc7 (39879)	1.1.1.1.1.101	1646 1	1646	255 RADIUS	328	Accounting-Request id=10
188 2024-06-05 00:43:33.350936	0x037a (890)	1.17181	1646 1.:)101	1646	64 RADIUS	62	Accounting-Response id=10
267 2024-06-05 00:43:36.359621	0x9bc8 (39880)	1.104.0.101	1646 1.1.4	1646	255 RADIUS	334	Accounting-Request id=11
268 2024-06-05 00:43:36.369035	0x0489 (1161)	1.1 1.1.181	1646 1.174 1.101	1646	64 RADIUS	62	Accounting-Response id=11

Radius会话的数据包捕获

相关信息

使用ISE配置EAP-TLS身份验证

在ISE中配置TLS/SSL证书

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)。