为控制台和OPadmin门户配置ThreatGrid RADIUS over DTLS身份验证

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 配置 配置 验证 排除

简介

本文档介绍在ThreatGrid(TG)版本2.10中引入的远程身份验证拨入用户服务(RADIUS)身份验证功能 。它允许用户使用存储在身份验证、授权和记帐(AAA)服务器中的凭据登录管理员门户和控制台门 户。

在本文档中,您找到配置该功能所需的步骤。

先决条件

要求

- ThreatGrid 2.10版或更高版本
- 支持RADIUS over DTLS身份验证的AAA服务器(draft-ietf-radext-dtls-04)

使用的组件

- ThreatGrid设备2.10
- •身份服务引擎(ISE)2.7

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。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

配置

本节提供有关如何为RADIUS身份验证功能配置ThreatGrid设备和ISE的详细说明。

注意:要配置身份验证,请确保端口UDP 2083上的通信允许在ThreatGrid Clean接口和ISE策 略服务节点(PSN)之间进行。 步骤1.准备ThreatGrid证书以进行身份验证。

RADIUS over DTLS使用相互证书身份验证,这意味着需要来自ISE的证书颁发机构(CA)证书。首先 检查CA签名的RADIUS DTLS证书:

Identity Services Engine	Home	Context Visibility	Operations +	Policy Administration	● Work Centers			(9 0
▼System → Identity Management	 Network 	k Resources Device Po	rtal Management	pxGrid Services Fee	d Service + Threat Centri	c NAC			
Deployment Licensing - Certificate	es ⊧Lo	ogging Maintenance	Upgrade + Bac	kup & Restore + Admin	Access				
- Certificate Management	Syst	em Certificates 💧 For	disaster recovery	it is recommended to export	certificate and private key p	airs of all system certificates.			
System Certificates		Edit Generate Self Sig	ned Certificate	F Import Export	🗙 Delete 🔎 View				
Trusted Certificates		Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
OCSP Client Profile	▼ w	cecot-ise27-1							
Certificate Signing Requests	_	OU=Certificate Services System Certificate,CN=w cecot-ise26-1.lemon.com			wcecot-ise26-1.lemon.co	Certificate Services Endp			ao 🗖
Certificate Periodic Check Settings		#Certificate Services End point Sub CA - wcecot-ise	pxGrid		m	oint Sub CA - wcecot-ise2 6-1	Wed, 20 Feb 2019	vved, 21 Feb 202	19
Certificate Authority		26-1#00002	Adapta FAD						
		CN=wcecot-ise27-1.lemo n.com,C=PL#LEMON CA #00003	Admin, EAP Authentication, RADIUS DTLS, Portal	Default Portal Certificate Group (j)	wcecot-ise27-1.lemon.co m	LEMON CA	Tue, 19 Nov 2019	Thu, 19 Nov 202	0 🔽
		Default self-signed server certificate	Not in use		wcecot-ise27-1.lemon.co m	wcecot-ise27-1.lemon.co m	Mon, 18 Nov 2019	Sat, 16 Nov 2024	4 🔽
		Default self-signed saml s erver certificate - CN=SA ML_wcecot-ise26-1.lemo n.com	SAML		SAML_wcecot-ise26-1.le mon.com	SAML_wcecot-ise26-1.le mon.com	Thu, 21 Feb 2019	Fri, 21 Feb 2020	V
		OU=ISE Messaging Servi ce,CN=wcecot-ise26-1.le mon.com#Certificate Serv ices Endpoint Sub CA - w cecot-ise26-1#00001	ISE Messaging Service		wcecot-ise26-1.lemon.co m	Certificate Services Endp oint Sub CA - wcecot-ise2 6-1	Wed, 20 Feb 2019	Wed, 21 Feb 202	29 🔽

步骤2.从ISE导出CA证书。

导航至**管理>System >证书>证书管理>受信任证书**,找到CA,选择**导出**(如图所示),然后将证书 保存到磁盘,以备以后使用:

Identity Services Engine	Home Context Visibility Operations F	volicy - Administrat	ion					o 💿 o
* System + Identity Management	Network Resources Device Portal Management	pxGrid Services + F	eed Service + Threat	Centric NAC				
Deployment Licensing - Certificati	es + Logging + Maintenance Upgrade + Back	up & Restore + Admi	in Access					
0								
* Certificate Management	Trusted Certificates							
System Certificates	/Edit 🕂 Import 🔂 Export 🗙 Delete 🔎	New				Show	All	- 8
Trusted Certificates	Friendly Name	 Status 	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Dat
OCSP Client Profile	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Tue, 13 May 2
Certificate Signing Requests	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure AdminAuth	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Sat, 11 Jun 2005	Mon, 14 May
Certificate Periodic Check Settings	CISCO ECC Root CA	Enabled	Cisco Services	01	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Fri, 4 Apr 205
Certificate Authority	Cisco Licensing Root CA	Enabled	Cisco Services	01	Cisco Licensing Root CA	Cisco Licensing Root CA	Thu, 30 May 2013	Sun, 30 May 2
	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure AdminAuth	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2
	Cisco Root CA 2048	Disabled	Endpoints Infrastructure AdminAuth	5F F8 78 28 28 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May
	Cisco Root CA 2099	Enabled	Cisco Services	01 9A 33 58 78 CE	Cisco Root CA 2099	Cisco Root CA 2099	Tue, 9 Aug 2016	Mon, 10 Aug 2
	Cisco Root CA M1	Enabled	Cisco Services	2E D2 0E 73 47 D3	Cisco Root CA M1	Cisco Root CA M1	Tue, 18 Nov 2008	Fri, 18 Nov 20
	Cisco Root CA M2	Enabled	Endpoints Infrastructure AdminAuth	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2
	Gisco RXIC-R2	Enabled	Cisco Services	01	Cisco RXC-R2	Cisco RXIC-R2	Wed, 9 Jul 2014	Sun, 9 Jul 203
	Default self-signed server certificate	Enabled	Endpoints Infrastructure AdminAuth	SC 6E B6 16 00 00	wcecot-ise26-1.lemon.c	wcecot-ise26-1.lemon.c	Thu, 21 Feb 2019	Fri, 21 Feb 20
	DigiCert Global Root CA	Enabled	Cisco Services	08 38 E0 56 90 42	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov
	DigiCert root CA	Enabled	Endpoints Infrastructure AdminAuth	02 AC 5C 26 6A 08	DigiCert High Assurance	DigiCert High Assurance	Fri, 10 Nov 2006	Mon, 10 Nov 2
	DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure AdminAuth	04 E1 E7 A4 DC 5C	DigiCert SHA2 High Ass	DigiCert High Assurance	Tue, 22 Oct 2013	Sun, 22 Oct 2
	DoflamingoCA_ec.ort	Enabled	Infrastructure	01	DoflamingoCA	DoflamingoCA	Sun, 20 Mar 2016	Fri, 20 Mar 20
	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF 80 80 D6 A3	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2
	HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2
	LEMON CA	Enabled	Infrastructure Cisco Services Endpoints AdminAuth	12 34 56 78	LEMON CA	LEMON CA	Fri, 21 Jul 2017	Wed, 21 Jul 2

步骤3.将ThreatGrid添加为网络访问设备。

导航至**管理>网络资源>网络设备>添加**以为TG创建新条目,并输入Clean接口的**名称、IP地址**,然 后选择**DTLS Required**(如图所示)。单击**底部**的"保存":

cisco Identity Services Engine	Home	Context Visibility	 Operations 	Policy	▼Administrat	ion 🕨 V	/ork Centers		
System Identity Management	- Network Re	sources + Device	Portal Management	pxGrid S	ervices + Fe	ed Service	+ Threat Centric I	NAC	
* Network Devices Network Device O	Groups Net	work Device Profiles	External RADIUS	Servers F	RADIUS Server	Sequences	NAC Managers	External MDM	Location Services
0									
Network Devices	Network D	levices List > ksec-t	hreatgrid02-clean						
Default Device	Network	K Devices							
Device Security Settings				- N	ame ksec-thr	eatgrid02-cle	81		
				Descrip	ption				
		10 Address	10.62 14	2 1 71			/ 22		
		IP ADDRESS	· · · · · · · · · · · · · · · · · · ·	5.171			, 32		
				Device De		-			
				Device P1	Gisco	•			
				Model N	ame	Ŧ			
			S	oftware Ver	nion	Ŧ			
		* Network Device	Group						
			Oldab.						
		Location	Locations 😳	Set	To Default				
		IPSEC No	0	Set '	To Default				
		Device Type All	Device Types 🛛 🙄	Set	To Default				
	_								
		+ RADIUS Authent	ication Settings						
		RADIUS UD	P Settings						
				• •	Shared Secret	RADIUS		Chow	
				Pd 1	Change Count			Show	
			0	se second a	Shared Secret	L U		Chow	
					0.4.0.4	1799.0		Snow	1
					COA Port	1700		Set to Default	
		RADIUS DT	LS Settings (j)						
					Charad Correct	endus/de		T.	
					CoA Port	2083		Set To Default	
			Issuer CA /	of ISE Contrib	icates for CoA	LEMONICA			,] @
				A HOL OWNER	DNS Name	keesthread	nrid02.clean.cisco		1.0
					Dito Hallo	KSCC-UTED	gnove-creationsco		
		General Se	ttings						
				En	able KeyWrap				
				* Key E	incryption Key		Sho	244	
			* Messag	e Authentica	ator Code Key		Sho	2WV	
				Key	Input Format	ASCII	HEXADECIMAL		
		 TACACS Authen 	tication Settings						
		 SNMP Settings 							
		 Advanced Trusts 	ec Settings						
	Save	Reset							

步骤4.为授权策略创建授权配置文件。

导航至**策略>Policy元素>结果>授权>授权配置文件,**然后单**击添加**。输入**名称**并选**择高级属**性设置 (如图所示),然后单**击保存**:

cisco	Identity	y Service	s Engine	Home	→ Context \	/isibility	Operations	- Policy	 Administration 	Work Centers
Policy	Sets	Profiling	Posture	Client Provis	ioning - Po	olicy Eleme	nts			
Diction	naries	 Conditi 	ons v R	esults						
				0						
Auther	enticatio	on		Author	zation Profiles	s > TG opac rofile	imin			
- Autho	orizatio	n				* Name	ThreatGrid			
Auth	orizatior	Profiles			D	escription				
Dow	nloadab	le ACLs			* Acc	cess Type	ACCESS_ACCEPT	-	Ť	
▶ Profil	ing			N	etwork Device	Profile	📸 Cisco 👻 🕀)		
▶ Postu	ire				Service	Template	0			
Iclient	t Provis	ioning			Track M	lovement				
				P	assive Identity	/ Tracking				
				► Co	ommon Tasl	ks				
				▼ Ad	lvanced Att	ributes S	ettings			
				Ra	dius:Service-T	уре	📀 = Adı	ministrative	0	- +
				▼ At	tributes De	tails				
				Acce Servi	ss Type = ACO ice-Type = 6	CESS_ACCE	РТ			
				Save	Reset					

步骤5.创建身份验证策略。

导航至**策略>策略**集,然后单**击"+**"。 输入策略集**名称**,并将条件设置为NAD IP Address(分配给 TG的干净接口),单击保存,如图所示:

diale Ide	ntity Service	es Engine Home	Context Visibility Operations	✓ Policy	Administration	Work Centers			્ર	• • •
Policy Set	s Profiling	Posture Client Provisio	oning Policy Elements							
Policy S	ets						Reset Polic	yset Hitcoun	ts Rese	t Save
+	Status	Policy Set Name	Description	Co	nditions	Allowed Protocols / Serve	er Sequence	Hits	Actions	View
Search										
1	0	ThreatGrid		Ę	Network Access Dev Address EQUALS 10.62.148	Default Network Access	x • +		¢	>
	\odot	Default	Default policy set			Default Network Access	× * +	59	٥	>

步骤6.创建授权策略。

单击">"转到授权策略,展开授权策略,单击"+"并配置如图所示,然后单击"保**存"**:

✓ Authori	ization Polic	y (3)								
					Results					
•	Status	Rule Name	Cond	itions	Profiles		Security Groups		Hits	Actions
Search										
	Ø	ThreatGrid Admin	₽	Radius-NAS-Identifier EQUALS Threat Grid Admin	×ThreatGrid	+	Select from list	* +	1	\$
	Ø	ThreatGrid Console	₽	Radius-NAS-Identifier EQUALS Threat Grid UI	×ThreatGrid	+	Select from list	× +	1	٥
	Ø	Default			× DenyAccess	+	Select from list	• +	17	\$

提示:您可以为同时符合Admin和UI两种条件的所有用户创建一个授权规则。

步骤7.为ThreatGrid创建身份证书。

ThreatGrid的客户端证书必须基于椭圆曲线密钥:

openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem 它必须由ISE信任的CA签名。选中<u>将根证书导入受信任证书存储页</u>,了解有关如何将CA证书添加到 ISE受信任证书存储的详细信息。

步骤8.将ThreatGrid配置为使用RADIUS。

登录管理员门户,导航至**Configuration > RADIUS**。在RADIUS CA证书中,粘贴从ISE收集的 PEM文件的内容,在客户端证书中粘贴从CA接收的PEM格式的证书,在客户端密钥粘贴内容中粘 贴从上一步的private-ec-key.pem文件,如图所示。单击**Save**:

CISCO Threat Grid Appliance Administration Portal	Support ? Help
Configuration • Operations • Status • Support •	int -
RADIUS DTLS Configuration	
Authentication Mode	C Either System Or RADIUS Authentication
RADIUS Host	10.48.17.135
RADIUS DTLS Port	
RADIUS CA Certificate	rVOxvUhoHai7g+B END CERTIFICATE
RADIUS Client Certificate	QFrtRNBHrKaEND CERTIFICATE
RADIUS Client Key	A 2TOKEY4waktmOluw== END EC PRIVATE KEY
Initial Application Admin Username	a radek

注意:保存RADIUS设置后,必须重新配置TG设备。

步骤9.向控制台用户添加RADIUS用户名。

要登录到控制台门户,必须将RADIUS用户名属性添加到相应用户,如图所示:

D	eta	ai	ls
D	eta	aı	lS

	Login	radek		
	Name	radek 🖊		
	Title	Add 🖊		
	Email	rolszowy@c	sisco.com 🌶	/
	Integration 2	none	\sim	
	Role	admin		
	Status	Active	Inactive	1
	RADIUS Username @	radek		
	RADIUS Username Privacy	radek Private	Public	Unset
	RADIUS Username (2) Default UI Submission Privacy (2) FUI A Accepted (2)	radek Private	Public	Unset
CSA	RADIUS Username ? Default UI Submission Privacy ? EULA Accepted ? Auto-Submit Types ?	radek Private No Add	Public	Unset
CSA	RADIUS Username 3 Default UI Submission Privacy 3 EULA Accepted 3 Auto-Submit Types 3 Can Flag Entities 3	radek Private No Add / True	Public False	Unset

步骤10.仅启用RADIUS身份验证。

成功登录管理员门户后,将显示一个新选项,该选项将完全禁用本地系统身份验证并保留仅基于 RADIUS的身份验证。

CISCO Threat Grid Appliance Administration Portal		Support ? Help		
Configuration - Operations - Status - Support -			I	•
RADIUS DTLS Configuration				
Authentication Mode	04	RADIUS Authentication Not Enabled ✓ Either System Or RADIUS Authentication Permitted Only RADIUS Authentication Permitted		
RADIUS Host	0	10.48.17.135		

验证

重新配置TG后,注销,现在登录页面在映像、管理员和控制台门户中分别显示为:

Threat Grid





Threat Grid

Use your RADIUS username and password.
 RADIUS username
 RADIUS password
 Log In

Forgot password?

故障排除

有三个组件可能导致问题:ISE、网络连接和ThreatGrid。

• 在ISE中,确保它将ServiceType=Administrative返回到ThreatGrid的身份验证请求。导航至 Operations> RADIUS > Live Logs 并检查详细信息:

	Time	Status	Details	Repeat	Identity	Authentication Policy	У	Authorization Policy	Authorizati	Network Device
×		•			Identity	ThreatGrid	×	Authorization Policy	Authorization	Network Device
	Feb 20, 2020 09:40:38.753 AM	2	ò		radek	ThreatGrid >> Default		ThreatGrid >> ThreatGrid Admin	TG opadmin	ksec-threatgrid02-clean
	Feb 20, 2020 09:40:18.260 AM		0		radek	ThreatGrid >> Default		ThreatGrid >> ThreatGrid Console	TG console	ksec-threatgrid02-clean

Authentication Details

Source Timestamp	2020-02-20 09:40:38.753
Received Timestamp	2020-02-20 09:40:38.753
Policy Server	wcecot-ise27-1
Event	5200 Authentication succeeded
Username	radek
User Type	User
Authentication Identity Store	Internal Users
Authentication Method	PAP_ASCII
Authentication Method Authentication Protocol	PAP_ASCII PAP_ASCII
Authentication Method Authentication Protocol Service Type	PAP_ASCII PAP_ASCII Administrative
Authentication Method Authentication Protocol Service Type Network Device	PAP_ASCII PAP_ASCII Administrative ksec-threatgrid02-clean
Authentication Method Authentication Protocol Service Type Network Device Device Type	PAP_ASCII PAP_ASCII Administrative ksec-threatgrid02-clean All Device Types
Authentication Method Authentication Protocol Service Type Network Device Device Type Location	PAP_ASCII PAP_ASCII Administrative ksec-threatgrid02-clean All Device Types All Locations
Authentication MethodAuthentication ProtocolService TypeNetwork DeviceDevice TypeLocationAuthorization Profile	PAP_ASCII PAP_ASCII Administrative ksec-threatgrid02-clean All Device Types All Locations TG opadmin

 如果您没有看到这些请求,请在ISE上执行数据包捕获。导航至"操作">"故障排除">"诊断工具 ">"TCP转储",在TG的干净接口的"过滤器"字段中提供IP,然后单击"开始"并尝试登录 ThreatGrid:

TCP Dump

Status	Monitoring (approximate file size: 8192 bytes) Stop
Host Name	wcecot-ise27-1
Network Interface	GigabitEthernet 0
Promiscuous Mode	● On Off
Filter	ip host 10.62.148.171
	Example: 'ip host helios and not iceburg'
Format	Raw Packet Data
Dump File	
Download Delete	
您必须看到字节数增加。在Wireshark中打开pcap文件以了解详细信息。	
• 如果在您单击ThreatGrid中保存后看到错误"很抱歉,但出现了问题",页面如下所示:	
Threat Grid Appliance Administration Portal	

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

We're sorry, but something went wrong.

Operations *

The server experienced an error while processing your request. Please retry your request later.

Status *

Support *

If this problem persists, contact support.

Configuration -

*

这意味着您最可能将RSA密钥用于客户端证书。必须将ECC密钥与步骤7中指定的参数一起使用。

181 **•**