通过IKEv2将Anyconnect VPN配置为FTD与ISE

目录	
<u>简介</u>	
<u>先决条件</u>	
<u>要求</u>	
<u>使用的组件</u>	
<u>背景信息</u>	
<u>配置</u>	
<u>1. 导入SSL证书</u>	
<u>2. 配置RADIUS服务器</u>	
<u>2.1.在FMC上管理FTD</u>	
<u>2.2.在ISE上管理FTD</u>	
<u>3. 在FMC上为VPN用户创建地址池</u>	
<u>4. 上传AnyConnect映像</u>	
<u>5. 创建XML配置文件</u>	
<u>5.1.在配置文件编辑器上</u>	
<u>5.2.在FWU上</u> 2. 和 異に知道	
<u>0. </u>	
<u>7. Anyconnect配直又仵配直</u>	
<u> </u>	
<u> </u>	

简介

本文档介绍在FMC管理的FTD上使用IKEv2和ISE身份验证的远程访问VPN的基本配置。

先决条件

要求

Cisco 建议您了解以下主题:

- 基本VPN、TLS和互联网密钥交换版本2 (IKEv2)
- 基本身份验证、授权和记帐(AAA)以及RADIUS
- 使用Firepower管理中心(FMC)的经验

使用的组件

本文档中的信息基于以下软件版本:

- 思科Firepower威胁防御(FTD) 7.2.0
- 思科FMC 7.2.0

- AnyConnect 4.10.07073
- 思科ISE 3.1

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。

背景信息

IKEv2和安全套接字层(SSL)都是用于建立安全连接的协议,特别是在VPN环境中。IKEv2提供强大 的加密和身份验证方法,为VPN连接提供高级别的安全性。

本文档提供了FTD版本7.2.0及更高版本的配置示例,它允许远程访问VPN使用传输层安全(TLS)和 IKEv2。作为客户端,可以使用Cisco AnyConnect,它受多个平台支持。

配置

1. 导入SSL证书

配置AnyConnect时,证书至关重要。

手动注册证书有以下限制:

- 1. 在FTD上,生成证书签名请求(CSR)之前需要证书颁发机构(CA)证书。
- 2. 如果从外部生成CSR,则使用PKCS12的其他方法。

在FTD设备上获取证书有多种方法,但安全简单的方法是创建CSR并由CA签署。具体操作如下:

1. 定位至Objects > Object Management > PKI > Cert Enrollment, 然后单击Add Cert Enrollment。
 2. 输入信任点名称RAVPN-SSL-cert。

3. 在CA Information选项卡下,选择Manual"注册类型",然后粘贴CA证书,如图所示。

Add Cert Enrollme	nt			?
Name* RAVPN-SSL-cert				
CA Information	ertificate Parameters	Key Revor	ation	
Enrollment Type:	Manual CA Only Check this option if you de from this CA	• not require a	n identity certificate t	to be created
CA Certificate:	BEGIN CERTIFICA MIIG1jCCBL6gAwIBAgIO wogXPrr4Y9x1zq7eDAN G9w0BAQsFADBK MQswCQYDVQQGEwJV AGA1UEChMJSWRIbIRy cwJQYDVQQDEx5JZGV VHJ1c3QgQ29tbWVyY2 290IENBIDEwHhcNMTkx Y1NjE1WhcNMjkx MiEvMTY1NiE1WiBvMO	FE QAFu+ IBgkqhki UzESMB vdXN0MS u !IhbCBSb kMjEyMT swCQYD		

FMC - CA证书

4. 在Certificate Parameters下,输入主题名称。例如:

Name*		
RAVPN-SSL-cert		
Description		
CA Information Certificate	Parameters Key Revocation	
Include FQDN:	Don't use FQDN in certificate 🔹	
Include Device's IP Address:		
Common Name (CN):	ftd.cisco.com	
Organization Unit (OU):	TAC	
Organization (O):	cisco	
Locality (L):		
State (ST):		
Country Code (C):		
Email (E):		
Include Device's Serial Number		
		Cancel

FMC -证书参数

5. 在Key 选项卡下,选择密钥类型,然后提供名称和位大小。对于RSA,最少2048位。

6. 单击Save。

Add Cert Enrollment

Name*	
RAVPN-SSL-cert	
Description	
CA Information Certificate Parameters Key Revocation	
Кеу Туре:	
RSA CECDSA EdDSA	
Key Name:*	
RSA-key	
Key Size:	
2048 🔻	I
▼ Advanced Settings	2
Ignore IPsec Key Usage Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client certificates.	Ŧ
Cancel]

FMC -证书密钥

- 7. 定位至Devices > Certificates > Add > New Certificate。
- 8. 选择Device。在Cert Enrollment下,选择创建的信任点,然后单击Add(如图所示)。

?

Add New Certif	icate		0
Add a new certificat generate CA and ide	te to the device using entify certificate.	cert enrollment object which is used t	0
Device*:			
ftd		•	
Cert Enrollment*:			
RAVPN-SSL-cert		• +	
Cert Enrollment Det	ails:		
Name: Enrollment Type: Enrollment URL:	RAVPN-SSL-cert Manual (CA & ID) N/A		
		Cancel Ad	d
FMC -向FTD注册证书			

9. 单击ID,屏幕上将显示生成CSR的提示,请选择Yes。

Firewall Management Center Devices / Certificates	Overview Anal	ysis Policies	Devices Objects Integration	Deploy Q 🚱 🔅 I	admin • dealer SECURE
					Add
Name	Domain	Enrollment Type	Status		
√ 🚥 ftd					≙ ^
Root-CA	Global	Manual (CA Only)	GLO A OID		±₽CT
RAVPN-SSL-cert	Global	Manual (CA & ID)	CA A ID A Identity certificate import required		± 🖉 C 🗑

FMC -已注册证书CA



This operation will generate Certificate Signing Request do you want to continue?



FMC -生成CSR

10. 会生成一个可与CA共享的CSR,以便获取身份证书。

11. 从CA收到base64格式的身份证书后,请从磁盘上选择,方法是单击Browse Identity Certificate和Import,如图所示。

Step 1

Send Certificate Signing Request (CSR) to the Certificate Authority.

Certificate Signing Request (Copy the CSR below and send to the Certificate Authority):

BEGIN CERTIFICATE REQUEST
MIICqjCCAZICAQAwNjEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDaXNjbzEWMBQG
A1UEAwwNRIRELmNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAPLLwTQ6BkGjER2FfyofT+RMcCT5FQTrrMnFYok7drSKmdaKlycKM8Ljn+2m
8BeVcfHsCpUybxn/ZrlsDMxSHo4E0oJEUgutsk++p1jlWcdVROn0vtahe+BRxC3q
jo1FsLcp5zQru5goloRQRoiFwn5syAqOztgl0aUrFSSWF/Kdh3GeDE1XHPP1zzl4
Step 2
Once certificate authority responds back with identity certificate file, import it to device.

Identity Certificate File:	Browse Identity Certificate		
	Cancel Import		

FMC -导入身份证书

12. 导入成功后,信任点RAVPN-SSL-cert将显示为:

Namo	Domain	Enrollment Type	Status	
∼ == ftd				a
RAVPN-SSL-cert	Global	Manual (CA & ID)		± ₽ C ∎

FMC -信任点注册成功

2. 配置RADIUS服务器

2.1.在FMC上管理FTD

1. 导航至Objects > Object Management > RADIUS Server Group > Add RADIUS Server Group。

2. 输入名称ISE,并单击+添加RADIUS服务器。

7

Name:*		
ISE		
Description:		
Group Accountin	ig Mode:	
Single	▼	
Retry Interval:*	(1-10) Seconds	
10		
Realms:		
	▼	
Enable autho	orize only	
Enable interi	m account update	
Interval:*	(1-120) hours	
24		
Enable dyna	mic authorization	
Port:*	(1024-65535)	
1700		
RADIUS Servers	(Maximum 16 servers)	
IP Address/Hos	tname	
10.197.224.173		

FMC - Radius服务器配置

3. 提及ISE Radius服务器的IP地址以及与ISE服务器相同的共享密钥(密钥)。

4. 选择FTD与ISE服务器通信时使用的Routing 或Specific Interface。

Edit RADIUS Server	?
IP Address/Hostname:*	
Confirme DNS at Threat Defense Diatform Settings to recolve bestneme	
Authentication Port* (1-65535)	
1812	
Key:*	
••••••	
Confirm Key:*	
•••••	
Accounting Port: (1-65535)	
1813	
Timeout: (1-300) Seconds	
10	
Connect using:	
Routing O Specific Interface	
outside 💌 🕂	
Redirect ACL:	
▼ +	
Cancel	Save

6. 保存后,服务器即会添加到RADIUS Server Group 下,如图所示。

RADIUS Server Group	Add RADIUS Server Group	Q, Filter			
RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.					
Name	Value				
ISE	1 Server		11		

FMC - RADIUS服务器组

2.2.在ISE上管理FTD

1. 导航至Network Devices ,然后单击Add。

2. 输入服务器和FTD通信接口IP Address的RADIUS客户端的名称"Cisco-Radius"。

3. 在Radius Authentication Settings下,添加Shared Secret。

4. 单击Save。

	Network Devices	Network Dev	vice Groups	Network Device Profiles	External RADI	JS Servers	RADIUS Server Sequences	NAC Managers	External MDM	Location Services	
N	Network Devices		Network Devices Li	st > Cisco-Radius							
	Network Devices		Network Devices								
	Default Device										
(Device Security Settings		Name	Cisco-Radius							
			Description								
			IP Address	✓ * IP: 10.197.167.5	/ 25 🧔	6					
			Device Profile	🗰 Cisco-Radius	× 0						
			Model Name		~						
			Software Version		~						
			Network Devi	ce Group							
			Device Type	All Device Types	~	Set To De	ault				
			IPSEC	No		Set To Det	ault				
			Location	All Locations	~	Set To De	ault				
			🗹 🗸 RAI	DIUS Authentication Settin	igs						
			DADIU	C UDD Sottions							
			KADIU	S ODP Settings							
			Protocol	RADIUS							
			Shared S	iecret		Show					
			Use	Second Shared Secret 🕕							
			networkD	evices.secondSharedSecret			Show				
				CoA Port 1700		Se	t To Default				

ISE -网络设备

5. 要创建用户,请导航至Network Access > Identities > Network Access Users,然后单击 Add。

6.根据需要创建UsernameandLogin Password。

Overview Identitie	${f s}$ Id Groups Ext Id Sources Network Resources Policy Elements Policy Sets Troubleshoot Reports More $arphi$
Endpoints	Network Access Users List > ikev2-user
Network Access Users	
Identity Source Sequences	✓ Network Access User
	* Username ikev2-user
	Status 💟 Enabled 🗸
	Email
	✓ Passwords
	Password Type: Internal Users V
	Password Re-Enter Password
	* Login Password Generate Password ①
	Enable Password ()

ISE - 用户

7. 要设置基本策略,请定位至Policy > Policy Sets > Default > Authentication Policy > Default,选择All_User_ID_Stores。

8. 定位至Policy > Policy Sets > Default > Authorization Policy > Basic_Authenticated_Access, 并选择,如PermitAccess图所示。

	0	Default					All_User_ID_Stores	∞ ∨	4	ŝ
ISE	-身份验	立证策略								
	0	Basic_Authenticated_Acces s	=	Network_Access_Authentication_Passed	$\text{PermitAccess} \times$	~+	Select from list	~+	4	ŝ

ISE -授权策略

3. 在FMC上为VPN用户创建地址池

1. 定位至Objects > Object Management > Address Pools > Add IPv4 Pools。

- 2. 输入名称RAVPN-Pool和地址范围,掩码是可选的。
- 3. 单击Save。

Edit IPv4 Pool

Name*

RAVPN-Pool

IPv4 Address Range*

10.1.1.0-10.1.1.255

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask

255.255.255.0

Description

Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

Override (0)

FMC -地址池

4. 上传AnyConnect映像

1. 定位至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。

2. 输入名称anyconnect-win-4.10.07073-webdeploy,然后单击Browse 从磁盘中选择Anyconnect文件,然后单击Save (如图所示)。

0

Cancel

Save

Edit AnyConnect File

Name:*

anyconnect-win-4.10.07073-webdeploy

FMC - Anyconnect客户端映像

5. 创建XML配置文件

5.1.在配置文件编辑器上

1. 从software.cisco.com下载配置文件编辑器并打开它。

2. 定位至Server List > Add...

3. 输入"显示名称"RAVPN-IKEV2和FQDN以及"用户组"(别名)。

4. 选择主要协议 IPsec, 单击Ok 如图所示。

Server	List Entry					×
Server	Load Balancing Servers	SCEP Mo	bile Certificate Pinning			
Pri	mary Server isplay Name (required)	RAVPN-IK	EV2	Connection Information Primary Protocol IPs	sec 🗸 🗸	
F	QDN or IP Address ftd.cisco.com		User Group	ASA gateway	g IKE Negotiation	EAP-AnyConnect 🗸
G	Group URL		IKE Identity (IOS ga	ateway only)		
f	ftd.cisco.com/RAVPN-IKEV	/2				



5. 添加服务器列表。另存为ClientProfile.xml。

AnyConnect Profile Editor -	VPN						-		×	
File Help										
VPN	Server List Profile: C:\Users\Amrutha\Documents\ClientProfile.xml									
Backup Servers										
Certificate Pinning	Hostname	Host Address	User Group	Backup Server List	SCEP	Mobile Settings		Certificate	Pins	
Certificate Enrollment	RAVPN-IKEV2	ftd.cisco.com	RAVPN-IKEV2	Inherited						
Mobile Policy										
Server List										
	Note: it is highly recommended that at least one server be defined in a profile. Add					D	Delete			
						Edit	D	etails		

配置文件编辑器-ClientProfile.xml

5.2. FMC上

- 1. 定位至Objects > Object Management > VPN > AnyConnect File > Add AnyConnect File。
- 2. 输入名称ClientProfile,然后单击Browse以选择ClientProfile.xml磁盘文件。
- 3. 单击Save。

Edit AnyConnect File		?
Name:*		
ClientProfile]	
File Name:*		
ClientProfile.xml	Browse	
File Type:*		
AnyConnect VPN Profile]	
Description:		
	Cancel	Save
C - Anyconnect VPN配置文件		

6. 配置远程访问

1. 导航到Devices > VPN > Remote Access并单击+以添加连接配置文件(如图所示)。

RAVPN-IKEV2						
Connection Profile Access Interfaces Advanced Dyna						
			+			
Name	АЛА	Group Policy				
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfttGrpPolicy	/1			

FMC -远程访问连接配置文件

2. 输入连接配置文件名称RAVPN-IKEV2+,并单击Group Policy中的创建组策略(如图所示)。

Add Connection Profile	e	0
Connection Profile:*	RAVPN-IKEV2	
Group Policy:*	▼ +	
E	Edit Group Policy	
Client Address Assignment	AAA Aliases	
IP Address for the remote clie Servers. Configure the ' <i>Client</i> assignment criteria. Address Pools:	ents can be assigned from local IP Address pools/DHCP Servers/AAA Address Assignment Policy' in the Advanced tab to define the	+
Name	IP Address Range	
DHCP Servers:		÷
Name	DHCP Server IP Address	. 1
	Cancel	2

FMC -组策略

3. 输入名称RAVPN-group-policy,选择VPN协议, SSL and IPsec-IKEv2 如图所示。

Edit Group Policy

Name:*						
RAVPN-group-policy						
Description:						
Description.						
General AnyCon	nect Advanced					
VPN Protocols	VPN Tunnel Protocol:					
IP Address Pools	must be configured for users to connect over a VPN tunnel.					
Banner	SSL SSL					
DNS/WINS	V IPsec-IKEv2					
Split Tunneling						

?

Cancel	Save

FMC - VPN协议

4. 在AnyConnect > Profile下,从下拉列表中选择XML配置文件ClientProfile,然后单击Save(如图所示)。

Edit Group Policy		?
Name:* RAVPN-group-policy Description:		
Profile Management Profile Client Modules SSL Settings Connection Settings Custom Attributes	AnyConnect profiles contains settings for the VPN client functionality and optional features. Firewall Threat Defense deploys the profiles during AnyConnect client connection.	
	Cancel	ave

FMC - Anyconnect配置文件

5.单击+ as shown in the image添加地址池RAVPN-Pool。

Edit Connection Profile	>	0
Connection Profile:*	RAVPN-IKEV2 RAVPN-group-policy +	
Client Address Assignment	AAA Aliases	
IP Address for the remote clie Servers. Configure the ' <i>Client</i> assignment criteria. Address Pools:	ents can be assigned from local IP Address pools/DHCP Servers/AAA Address Assignment Policy' in the Advanced tab to define the	+
Name	IP Address Range	
RAVPN-Pool	10.1.1.0-10.1.1.255	1
DHCP Servers:		+
Name	DHCP Server IP Address	
		_
	Cancel	e

FMC -客户端地址分配

6. 定位至AAA > Authentication Method, 然后选择AAA Only。

7. 选择Authentication Server作为ISE (RADIUS)。

Edit Connection Profile	?
Connection Profile:* RAVPN-IKEV2 Group Policy:* RAVPN-group-policy + Edit Group Policy Client Address Assignment AAA Aliases	
Authentication	
Authentication Method: AAA Only 🔹	
Authentication Server: ISE (RADIUS)	
 Fallback to LOCAL Authentication Use secondary authentication Authorization Authorization Server: Use same authentication server Allow connection only if user exists in authorization database 	
Accounting	
Accounting Server:	
► Advanced Settings	
Cancel	e
FMC - AAA身份验证	

8. 导航到Aliases ,输入RAVPN-IKEV2别名,在ClientProfile.xml中将其用作用户组。

9. 单击Save。

Edit Connection Profile	e		
Connection Profile:*	RAVPN-IKEV2]
Group Policy:*	RAVPN-group-	-policy 🔻) +
Client Address Assignmen	t AAA A	Aliases	

0

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name	Status	
RAVPN-IKEV2	Enabled	/1

URL Alias:

Configure the list of URL alias which your endpoints can select on web access. If users choose the following URLs, system will automatically log them in via this connection profile.

URL	Status			
				Ŧ
		Cancel	Save	

FMC -别名

10. 导航到Access Interfaces(IKEv2),然后选择必须启用RAVPN IKEv2的接口。

11. 选择SSL和IKEv2的身份证书。

12. 单击Save。

Connection Profile Access Interfaces Advanced

Interfaces of the targeted device wi	erfaces of the targeted device which belong to below specified interface groups will support incoming Remote Access VPN connections							
Name		Interface Trustpoir	nt	DTLS	SSL	IPsec-IKEv2		
outside				•	0	0	/1	
Access Settings								
Allow Users to select connection	n profile while logg	ging in						
SSL Settings								
Web Access Port Number:*	443]					
DTLS Port Number:*	443							
SSL Global Identity Certificate:	RAVPN-SSL-cer	t v]+					
Note: Ensure the port used in VPN con	figuration is not used	d in other services						
IPsec-IKEv2 Settings								
IKEv2 Identity Certificate:	RAVPN-SSL-cer	t 🔻]+					
Access Control for VPN Tra	ffic							
Bypass Access Control policy fi Decrypted traffic is subjected to A bypasses the inspection, but VPN AAA server are still applied to VPM	or decrypted traffic ccess Control Policy Filter ACL and autho I traffic.	(sysopt permit-vpn by default. This optic rization ACL downloa	i) an adied from					

FMC - 接入接口

13. 导航至Advanced。

14. 单击+添加Anyconnect客户端映像。

RAVPN-IKEV2				Save Cancel
Connection Profile Access In	erfaces Advanced		Local Realm: None	Policy Assignments.(1) Dynamic Access Policy: None
AnyConnect Client Images Address Assignment Policy Certificate Maps Group Policies	AnyConnect Client Images The VPN gateway can automatically download the latest AnyConnect package Download AnyConnect Client packages from Clicco Software Download Cente	to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appro r.	priate OS for the selected package.	Show Re-order buttons +
LDAP Attribute Mapping	AnyConnect File Object Name	AnyConnect Client Package Name	Operating System	
Load Balancing V IPsec Crypto Maps IKE Policy IPsec/IKEv2 Parameters	anyconnect-win-4.10.07073-webdisploy-k9 pkg AnyConnect External Browser Package A package that enables SAML based authentication using external web brows Download AnyConnect External Browser Package from Cisco Software Download Package File: Default-External-Browser-Package +	anyconnect-win-4.10.07073-webdeploy-k9 pkg er instead of the browser that is embedded in the AnyConnect Client. Enable the external browser option in one o and Center.	Windows •	û

FMC - Anyconnect客户端软件包

15. 在IPsec下,添加如图所示的Crypto Maps。

RAVPN-IKEV2				Save Cancel
				Policy Assignments (1)
			Local Realm: None	Dynamic Access Policy: None
Connection Profile Access Inte	rfaces Advanced			
AnyConnect Client Images	Crypto Maps			
Address Assignment Policy	Crypto Maps are auto generated for the interfaces on which IPsec-IKEv2 protocol is enabled.			
Certificate Maps	Following are the list of the interface group on which IPsec-IKEv2 protocol is enabled. You can add,	remove interface group to this VPN configuration in 'Access Interface' tab.		
Group Policies	Interface Group	IKEv2 IPsec Proposals	RRI	
LDAP Attribute Mapping	outside	AES-GCM	true	/
Load Balancing				
✓ IPsec				
Crypto Maps				
IKE Policy				
IPsec/IKEv2 Parameters				

FMC -加密映射

16. 在IPsec 下,单击+添加IKE Policy 命令。

RAVPN-IKEV2						Save Cancel
Connection Profile Access Inte	erfaces Advanced			Loc	al Realm: None	Policy Assignments (1) Dynamic Access Policy: None
AnyConnect Client Images Address Assignment Policy Certificate Maps	IKE Policy This list specifies all of the IKEv2 po	olicy objects applicable for this VPN policy when AnyCon	nect endpoints connect via IPsec-IKEv2 protocol.			+
Group Policies	Name	Integrity	Encryption	PRF Hash	DH Group	
LDAP Attribute Mapping Load Balancing	AES-SHA-SHA-LATEST	SHA, SHA256, SHA384, SHA512	AES, AES-192, AES-256	SHA, SHA256, SHA384, SHA512	14, 15, 16, 19, 20, 21	Ŷ
✓ IPsec						
Crypto Maps						
IKE Policy						
IPsec/IKEv2 Parameters						

FMC - IKE策略

17. 在IPsec 下,添加IPsec/IKEv2 Parameters。

Connection Profile Access Inte	erfaces Advanced			
AnyConnect Client Images Address Assignment Policy	IKEv2 Session Settings			
Certificate Maps	Identity Sent to Peers:	Auto 🔻		
Group Policies	Enable Notification on Tunnel Disconnect			
LDAP Attribute Mapping	Do not allow device reboot until all session	ons are terminated		
Load Balancing	IKEv2 Security Association (SA) Set	ttings		
∨ IPsec	Cookie Challenge:	Custom v		
Crypto Maps	Threshold to Challenge Incoming Cookies:	50) %	
IKE Policy		50	70	
IPsec/IKEv2 Parameters	Number of SAs Allowed in Negotiation:	100	%	
	Maximum number of SAs Allowed:	Device maximum		
	IPsec Settings			
	Enable Fragmentation Before Encryption			
	Path Maximum Transmission Unit Aging			
	Value Reset Interval:		Minutes	(Range 10 - 30)
	NAT Transparency Settings			
	Enable IPsec over NAT-T			
	Note: NAT-Traversal will use port 4500. Ensure to	hat this port number is not used in other s	services, e.g.	NAT Policy.
	NAT Keepalive Interval:	20	Seconds	(Range 10 - 3600)

FMC - IPsec/IKEv2参数

18. 在Connection Profile下,创建新的配置文件RAVPN-IKEV2。

19.Save单击图中所示。

RAVPN-IKEV2			You have unsaved change Save Cancel
Connection Profile Access Interfaces Advanced		Local Realm: /	Policy Assignments (1) None Dynamic Access Policy: None
			+
Name	AAA	Group Policy	
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	E DftGrpPolicy	/1
RAVPN-IKEV2	Authentication: ISE (RADIUS) Authorization: ISE (RADIUS) Accounting: None	RAVPN-group-policy	/1

FMC -

连接配置文件RAVPN-IKEV2

20. 部署配置。

	Deploy Q 💕 🌣 🕜 admin 🕶 🖞 SEC
Q	Advanced Deploy Deploy All
ftd	Ready for Deployment

FMC - FTD部署

7. Anyconnect配置文件配置

PC上的配置文件,保存在 C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile.

<#root>

<?xml version="1.0" encoding="UTF-8"?> <AnyConnectProfile xmlns="http://schemas[dot]xmlsoap<dot>org/encoding/" xmlns:xsi="http://www[dot]w3 <HostName>RAVPN-IKEV2</HostName> <HostAddress>ftd.cisco.com</HostAddress> <UserGroup>RAVPN-IKEV2</UserGenerational contents and the standard s



注意:建议在将客户端配置文件下载到所有用户的PC后,在组策略下禁用SSL客户端作为隧道协议。这可确保用户可以使用IKEv2/IPsec隧道协议以独占方式连接。

验证

您可以使用此部分来确认您的配置是否正常工作。

1. 对于第一个连接,使用FQDN/IP通过Anyconnect从用户的PC建立SSL连接。

2. 如果已禁用SSL协议且无法执行之前步骤,请确保客户端配置文件ClientProfile.xml存在于PC上的路径C:\ProgramData\Cisco\Cisco Anyconnect Secure Mobility Client\Profile下。

3. 系统提示后,输入用于身份验证的用户名和密码。

4. 身份验证成功后,客户端配置文件会下载到用户的PC上。

5. 断开与Anyconnect的连接。

6. 下载配置文件后,请使用下拉列表选择客户端配置文件中提及的主机名,RAVPN-IKEV2 以便使用IKEv2/IPsec连接到

Anyconnect.

7. 单击Connect。

🚳 Cisco AnyC	onnect Secure Mobility Client		-		×
	VPN: Ready to connect. RAVPN-IKEV2	~		Connect	

Anyconnect下拉列表

8. 输入在ISE服务器上创建的身份验证的用户名和密码。

S Cisco AnyConnect RAVPN-IKEV2										
		Username:	ikev2-user							
		Password:	*******							
						_				
				ОК	Cance	el				
🕙 Ci	sco AnyCo	onnect Secur	e Mobility Cl	ient	-	• ×				
		VPN: Contacting R.	AVPN-IKEV2.							
	_	RAVPN-IKEV	/2	Connect						

Anyconnect连接

9. 验证连接后使用的配置文件和协议(IKEv2/IPsec)。



已连接 AnyConnect

FTD CLI输出:

<#root>

firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect

Username : ikev2-user Index : 9 Assigned IP : 10.1.1.1 Public IP : 10.106.55.22 Protocol : IKEv2 IPsecOverNatT AnyConnect-Parent License : AnyConnect Premium Encryption : IKEv2: (1)AES256 IPsecOverNatT: (1)AES-GCM-256 AnyConnect-Parent: (1)none

Hashing : IKEv2: (1)SHA512 IPsecOverNatT: (1)none AnyConnect-Parent: (1)none Bytes Tx : 450 Bytes Rx : 656 Pkts Tx : 6 Pkts Rx : 8 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : RAVPN-group-policy Tunnel Group : RAVPN-IKEV2 Login Time : 07:14:08 UTC Thu Jan 4 2024 Duration : 0h:00m:08s Inactivity : 0h:00m:00s VLAN : none VLAN Mapping : N/A Audt Sess ID : 0ac5e205000090006596618c Security Grp : none Tunnel Zone : 0 IKEv2 Tunnels: 1 IPsecOverNatT Tunnels: 1 AnyConnect-Parent Tunnels: 1 AnyConnect-Parent: Tunnel ID : 9.1 Public IP : 10.106.55.22 Encryption. : none. Hashing : none Auth Mode : userPassword Idle Time out: 30 Minutes Idle TO Left : 29 Minutes Client OS : win Client OS Ver: 10.0.15063 Client Type : AnyConnect Client Ver : 4.10.07073 IKEv2: Tunnel ID : 9.2 UDP Src Port : 65220 UDP Dst Port : 4500 Rem Auth Mode: userPassword Loc Auth Mode: rsaCertificate Encryption : AES256 Hashing : SHA512 Rekey Int (T): 86400 Seconds Rekey Left(T): 86391 Seconds PRF : SHA512 D/H Group : 19 Filter Name : Client OS : Windows Client : AnyConnect Type IPsecOverNatT: Tunnel ID : 9.3 Local Addr : 0.0.0.0/0.0.0/0/0 Remote Addr : 10.1.1.1/255.255.255.255/0/0 Encryption : AES-GCM-256 Hashing : none Encapsulation: Tunnel Rekey Left(T) : 28791 Seconds Rekey Int (T): 28800 Seconds Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Bytes Tx : 450 Bytes : 656 Rx Pkts Tx : 6 Pkts Rx : 8

firepower# show crypto ikev2 sa

IKEv2 SAs:

Session-id:6, Status:UP-ACTIVE, IKE count:1, CHILD count:1

 Tunnel-id Local
 Remote
 fvrf/ivrf

 16530741
 10.197.167.5/4500
 10.106.55.22/65220
 Encr:

 Encr:
 AES-CBC, keysize:
 256, Hash:
 SHA512, DH Grp:19, Auth sign: RSA, Auth verify: EAP
 Life/Active Time:
 86400/17 sec

 Child sa:
 local selector
 0.0.0.0/0 - 255.255.255/65535
 remote selector
 10.11.1.1/65535

 ESP spi
 in/out:
 0x6f7efd61/0xded2cbc8
 535

firepower# show crypto ipsec sa

interface: Outside Crypto map tag: CSM_Outside_map_dynamic, seq num: 30000, local addr: 10.197.167.5 Protected vrf: local ident (addr/mask/prot/port): (0.0.0.0/0.0.0/0/0) remote ident (addr/mask/prot/port): (10.1.1.1/255.255.255.255/0/0) current_peer: 10.106.55.22, username: ikev2-user dynamic allocated peer ip: 10.1.1.1 dynamic allocated peer ip(ipv6): 0.0.0.0 #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6 #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.197.167.5/4500, remote crypto endpt.: 10.106.55.22/65220 path mtu 1468, ipsec overhead 62(44), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: DED2CBC8 current inbound spi : 6F7EFD61 inbound esp sas: spi: 0x6F7EFD61 (1870593377) SA State: active transform: esp-aes-gcm-256 esp-null-hmac no compression in use settings ={RA, Tunnel, NAT-T-Encaps, IKEv2, } slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic sa timing: remaining key lifetime (sec): 28723 IV size: 8 bytes replay detection support: Y Anti replay bitmap:

0x0000000 0x00001FF

```
outbound esp sas:
  spi: 0xDED2CBC8 (3738356680)
  SA State: active
  transform: esp-aes-gcm-256 esp-null-hmac no compression
  in use settings ={RA, Tunnel, NAT-T-Encaps, IKEv2, }
  slot: 0, conn_id: 9, crypto-map: CSM_Outside_map_dynamic
  sa timing: remaining key lifetime (sec): 28723
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
  0x00000000 0x00000001
```

ISE日志:

1	Time	Status	Details	Repea	Identity	Endpoint ID	Endpoint	Authenti	Authoriz	Authoriz	IP Address	Network De	Device Port	Identity Group	Posture	Server	Mdm Ser
×			. ×		Identity	Endpoint ID	Endpoint Pr	Authenticati	Authorizatio	Authorizatio	IP Address	Network Device	Device Port	Identity Group	Posture Star	Server	Mdm Server
	Jan 04, 2024 07:14:10.4	•	0	1	lkev2-user	00:50:56:8D:68:	Windows1	Default >>	Default >>	PermitAcc					1	ise	
J	Jan 04, 2024 07:14:10.4		0		lkev2-user	00:50:56:8D:68:	Windows1	Default >>	Default >>	PermitAcc		Cisco-Radius		Workstation	1	ise	

ISE -实时日志

故障排除

本部分提供了可用于对配置进行故障排除的信息。

debug radius all debug crypto ikev2 platform 255 debug crypto ikev2 protocol 255 debug crypto ipsec 255

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)。