ASA 8.x/ASDM 6.x:使用ASDM在现有站点到站点 VPN中添加新的VPN对等体信息

目录

简介 先决条件 要求 使用的组件 规则 回退信息 ASDM 配置 创建新连接配置文件 编辑现有VPN配置 验证 故障排除 IKE Initiator unable to find policy:Intf test_ext,源:172.16.1.103,目的:10.1.4.251 相关信息

<u>简介</u>

本文档提供有关使用自适应安全设备管理器(ASDM)将新VPN对等体添加到现有站点到站点VPN配 置时要进行的配置更改的信息。 在以下场景中,需要执行以下操作:

- Internet服务提供商(ISP)已更改,并使用了一组新的公共IP范围。
- •现场网络的完整重新设计。
- 站点上用作VPN网关的设备将迁移到具有不同公有IP地址的新设备。

本文档假设站点到站点VPN已正确配置且工作正常。本文档提供在L2L VPN配置中更改VPN对等体 信息的步骤。

<u>先决条件</u>

<u>要求</u>

Cisco 建议您了解以下主题:

• ASA站点到站点VPN配置示例

<u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

- •思科自适应安全设备5500系列,带软件版本8.2及更高版本
- •思科自适应安全设备管理器,软件版本6.3及更高版本

<u>规则</u>

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。

回退信息

站点到站点VPN在HQASA和BQASA之间工作正常。假设BQASA已完成网络重新设计,ISP级别的 IP方案已修改,但所有内部子网详细信息保持不变。

此示例配置使用以下IP地址:

- •现有BQASA外部IP地址 200.200.200.200
- •新的BQASA外部IP地址 209.165.201.2

注意:此处仅修改对等体信息。由于内部子网没有其他更改,因此加密访问列表保持不变。

<u>ASDM 配置</u>

本节提供有关使用ASDM更改HQASA上VPN对等体信息的可能方法的信息。

创建新连接配置文件

这可以是更简单的方法,因为它不会干扰现有VPN配置,并且可以使用新的VPN对等体相关信息创 建新连接配置文件。

1. 转到*Configuration > Site-to-Site VPN > Connection Profiles,然后*在Connection Profiles区域 下点击Add。

erface	Allow Acces	55			
tside iz ide					
		· · · · · · · · · · · · · · · · · · ·			
nection Profiles onnection profile identi Add 2 Edit 1	fies the peer of a site-to-site boloto	e connection. It specifies what data traffic	is to be encrypted, how the data traff	it is to be encrypted, and other	parameters.

将打开"添加IPSec站点到站点连接配置文件"窗口。

 在"基本"选项卡下,提供对等IP地址、预共享密钥和受保护网络的详细信息。使用与现有 VPN相同的所有参数,但对等体信息除外。Click OK.

asic duanced	Peer IP Address: [🗹 Static	209.165.201.2	
ovanceo	Connection Name: [Same as IP Address	209.165.201.2	
	Interface:	outside	×	
	IKE Authentication			
	Pre-shared Key:	•••••		
	Identity Certificate:	None	×	Manage
	Protected Networks -			
	Local Network:	inside-network/24		
	Remote Network:	192.168.25.0/24		
	Encryption Algorithms			
	IKE Proposal:	pre-share-des-sha, pre	-share-3des-sha	Manage
	IPsec Proposal:	S-256-MDS, ESP-3DES	SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5	Select
d:		Next Previou	ç	

3. 在"高级"菜单下,单击"加*密映射条目"*。请参阅"优先级*"选*项卡。此优先级等于其等效CLI配置 中的序列号。如果分配的数字小于现有加密映射条目,则首先执行此新配置文件。优先级数值 越高,值越小。这用于更改将执行特定加密映射的顺序。单击*OK*完成新连接配置文件的创建

sic	Priority:	20	
anced Crypto Map Entry	Perfect Forward Secrecy:	Disable Disable	
Tunnel group		Diffie-Helmen Group:	
	NAT-T:	🗹 Enable	
	Reverse Route Injection:	🗌 Enable	
	Security Association Lifetime		
	Time:	8 : 0 : 0	hhimmise
	Traffic Volume:	4608000	KBytes
	Static Crypto Map Entry Par	meters	
	Connection Type:	bidirectional	~
	CA Certificate:	None	×
		Send CA Certificate Chain	
	IKE Negotiation Mode:	Main Aggresive	
		Diffie-Helmen Group:	~
		xt 🙆 Previous	

这会自动创建新隧道组以及关联的加密映射。在使用此新连接配置文件之前,请确保可以使用新 IP地址到达BQASA。 添加新对等体的另一种方法是修改现有配置。无法为新对等体信息编辑现有连接配置文件,因为它 已绑定到特定对等体。要编辑现有配置,需要执行以下步骤:

- 1. 创建新隧道组
- 2. 编辑现有加密映射

创建新隧道组

转到*Configuration > Site-to-Site VPN > Advanced > Tunnel groups*,然后单击*Add*以创建包含新 VPN对等体信息的新隧道组。指定"*名称*"和"预共享密钥"字段,然*后单击OK*。

注意:确保预共享密钥与VPN的另一端匹配。

🖆 Add IPsec Site-to-	site Tunnel G	roup		
Name:	209.165.201.2	-		
IKE Authentication				
Pre-shared Key:	•••••			
Identity Certificate:	None		~	Manage
Send Certicate Chain:	Enable			×
IKE Peer ID Validation:	Required		~	
IKE Keepalive				
Oisable keepalives				
O Monitor keepalives				
Confidence Interva	(; [seconds		
Retry Interval		seconds		
O Headend will never	initiate keepalive	monitoring		
Default Group Policy		121		
Group Policy:	OfltGrpPolicy		~	Manage
IPsec Protocol:	Enabled			
			1	
	OK	Cancel Help		

注意:在"名称"字段中,当身份验证模式为预共享密钥时,应仅输入远程对等体的IP地址。只有身 份验证方法通过证书时,才能使用任何名称。在名称字段中添加名称且预共享身份验证方法时,会 出现此错误:

📽 Warning
ASDM received messages below when one or more of the commands below were sent to the ASA. [OK] means success, [ERROR] means failure, [INFO] means information and [WARNING] means warning
[WARNING] tunnel-group New-S25-VPN type ipsec-I2I L2L tunnel-groups that have names which are not an IP address may only be used if the tunnel authentication method is Digital Certificates and/or The peer is configured to use Aggressive Mode [OK] tunnel-group New-S25-VPN ipsec-attributes tunnel-group New-S25-VPN ipsec-attributes [OK] pre-shared-key ********** [OK] isakmp keepalive threshold 10 retry 2
Close

<u>编辑现有加密映射</u>

可以编辑现有加密映射以关联新的对等体信息。

请完成以下步骤:

1. 转到*Configuration > Site-to-Site VPN > Advanced > Crypto Maps,然后选*择所需的加密映射 并单击*Edit*。

Configura	tion 3	Site-to-Site VPN > Advanced	d > Crypto Maps							
🗣 Add 🔹	3	Edit • 👔 Delete 🗇 🗸 👗	10 m - Q.F	ind 🖭 Diag	ram					
Timethe	đ	Edt				Transform Eat	Ener.	nec	MAT. T. Fashlad	Designer Doute Fashlard
Typecyn	13	Edit Crypto Map	Destination	Service	Action	Transi umi per	Peer	PES	INAL-1 EUROPO	Reverse Kouce Enabled
🕞 interfa	• 3	Edit Traffic Selection		×.7. 5		<u></u>		-	425	and the second
static:	1	1 nside-netwo	192.168.25	. 💌 ip	Protect	ESP-AES-128-SHP	4 200.200.200		2	

系统将显示Edit IPSec Rule窗口。

2. 在Tunnel Policy(Basic)选项卡的Peer Settings(对等体设置)区域中,在Peer of Peer to Added(要添加的对等体的IP地址)字段中指定新对等体。然后点击*添加*。

	 Tunnel Policy (Crypto Map) 	- Advanced 1	rame selection	
Interface: outside	Policy Type:	static		Priority: 1
Transform Sets				
Transform Set to Be Added	l:ES	P-AES-128-SHA	¥	
	Add >>			Move Up
ESP-AES-128-MD5	Remove			Move Down
Door Sottings - Onting of F	or Dunamic Crucks Man Enhiles			
The Connection Type is app	plicable to static tunnel policies	only. Uni-direct	tional connection	type policies ar
for LAN-to-LAN redundancy redundant peers	y. Tunnel policies of the 'Origina	ate Only' conne	ction type may	specify up to 10
redundant peers.				
Connection Type:	bidirectional 💌			
IP Address of Peer to Be A	dded:	0.200.200.200		
	Add >>			Move Up
209.165.201.2				
	Remove			Move Down
🗆 Ea abla Darfact Eannada	- Comment			
Enable Perfect Forwardi	ng Secrecy			
Diffie-Helman Group:	ng Secrecy			

3. 选择现有对等IP地址,然后单击*删除*仅保留新的对等信息。Click *OK*.

iai Policy (crypto Piap) - basi	Tunnel Policy (Crypto Map) - A	ovanced Trame	selection
Interface: outside	Policy Type:	static	Priority: 1
Transform Sets			
Transform Set to Be Addec	ESP-4	ES-128-5HA	Move Up
ESP-AES-128-MD5	Remove		Move Down
Peer Settings - Optional f	or Dynamic Crypto Map Entries		
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance	or Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate	y. Uni-directional (Only' connection (connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers.	or Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate	y, Uni-directional Only' connection (connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers.	or Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate pidirectional	y. Uni-directional (Only' connection)	connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	or Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate didirectional	y. Uni-directional Only' connection (connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	br Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate bidirectional	y. Uni-directional Only' connection (200.200.200 (65.201.2	connection type policies are u type may specify up to 10 Move Up
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	br Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate bidirectional	y. Uni-directional Only' connection (200.200.200 (65.201.2	connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	br Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate bidirectional Ided: Add >> Remove	y. Uni-directional Only' connection (200.200.200 (65.201.2	connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	br Dynamic Crypto Map Entries licable to static tunnel policies onl . Tunnel policies of the 'Originate bidirectional	y. Uni-directional Only' connection (200.200.200 (65.201.2	connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	br Dynamic Crypto Map Entries licable to static tunnel policies only . Tunnel policies of the 'Originate bidirectional	y. Uni-directional Only' connection (200.200.200 (65.201.2	connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	pr Dynamic Crypto Map Entries licable to static tunnel policies only . Tunnel policies of the 'Originate pidirectional Ided: Add >> Remove g Secrecy	y. Uni-directional Only' connection (200.200.200 (65.201.2	connection type policies are u type may specify up to 10
Peer Settings - Optional f The Connection Type is ap for LAN-to-LAN redundance redundant peers. Connection Type:	g Secrecy	y. Uni-directional Only' connection (200.200.200 (65.201.2	connection type policies are u type may specify up to 10

注意:修改当前加密映射中的对等体信息后,与此加密映射关联的连接配置文件会立即在 ASDM窗口中删除。

4. 加密网络的详细信息保持不变。如果需要修改这些,请转至"流量选择"选项卡。

innel Policy	(Crypto Map) - Basic	Tunnel Policy (Crypto Map) - Advanced Traffic Selection
Action: 💿 I	Protect 🔘 Do not P	rotect
Source:	10.10.10.0/24	-
Destination	192.168.25.0/24	-
Service:	ip	

5. 转到Configuration > Site-to-Site VPN > Advanced > Crypto Maps窗格以查看修改的加密映射。但是,在单击"应用"之前,这些更改不会发生。单击Apply后,转到Configuration > Site-to-Site VPN > Advanced > Tunnel groups菜单,以验证是否存在关联的隧道组。如果是,则将创建相关的连接配置文件

Tupic Priority	Traff	ic Selection				Transform Set	Peer	pes	MAT-T Epobled	Reverse Route I
(ppermitty)	#	Source	Destination	Service	Action	in an ar of the ass	1.001		Territoria Chabled	Provide and Produce a
interface: outside	9. 4-14		- 61 T 4			-	ang para ang ang ang ang		1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	
static: 1	1	10.10.10.0/24	192.168.25	1 in	- A Distant	CO ACC 100 CHA	200 145 201 2			
					- Protoci	EPACATOR A	1209/100/201-2			
					10000	Credo I Color	120512012	1		
¢			- <u>-</u>			Crecologica	120512012			

<u>验证</u>

使用本部分可确认配置能否正常运行。

<u>命令输出解释程序(仅限注册用户)(OIT) 支持某些 show 命令。</u>使用 OIT 可查看对 show 命令输 出的分析。

 使用此命令可查看特定于单个对等体的安全关联参数:<u>show crypto ipsec sa peer <peer IP</u> <u>address></u>

<u>故障排除</u>

使用本部分可排除配置故障。

IKE Initiator unable to find policy:Intf test_ext,源: 172.16.1.103,目的: 10.1.4.251

尝试将VPN对等体从VPN集中器更改为ASA时,日志消息中会显示此错误。

解决方案:

这可能是迁移期间执行的配置步骤不正确的结果。在添加新对等体之前,请确保删除接口的加密绑 定。另外,请确保您使用隧道组中对等体的IP地址,而不是名称。

相关信息

- <u>采用ASA的站点到站点(L2L)VPN</u>
- <mark>最常见的VPN问题</mark>
- <u>ASA技术支持页</u>
- <u>技术支持和文档 Cisco Systems</u>