ASA 8.x/ASDM 6.x: Agregar nueva información de par VPN en una VPN de sitio a sitio existente mediante ASDM

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Información de backround Configuración de ASDM Crear un nuevo perfil de conexión Editar la configuración VPN existente Verificación Troubleshoot IKE Initiator unable to find policy: Intf test_ext, Src: 172.16.1.103, Dst: 10.1.4.251 Información Relacionada

Introducción

Este documento proporciona información sobre los cambios de configuración que se deben realizar cuando se agrega un nuevo peer VPN a la configuración VPN de sitio a sitio existente mediante Adaptive Security Device Manager (ASDM). Esto es necesario en estos escenarios:

- El proveedor de servicios de Internet (ISP) ha cambiado y se utiliza un nuevo conjunto de intervalos de IP públicos.
- Un rediseño completo de la red en un sitio.
- El dispositivo utilizado como gateway VPN en un sitio se migra a un nuevo dispositivo con una dirección IP pública diferente.

Este documento asume que la VPN de sitio a sitio ya está configurada correctamente y funciona bien. Este documento proporciona los pasos a seguir para cambiar la información de un peer VPN en la configuración VPN L2L.

Prerequisites

Requirements

Cisco le recomienda que tenga conocimiento acerca de este tema:

• Ejemplo de configuración de VPN de sitio a sitio ASA

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Adapative Security Appliance serie 5500 con versión de software 8.2 y posterior
- Cisco Adaptive Security Device Manager con versión de software 6.3 y posterior

Convenciones

Consulte <u>Convenciones de Consejos TécnicosCisco para obtener más información sobre las</u> <u>convenciones del documento.</u>

Información de backround

La VPN de sitio a sitio funciona bien entre la HQASA y la BQASA. Suponga que el BQASA ha obtenido un rediseño completo de la red y que el esquema IP se ha modificado en el nivel ISP, pero todos los detalles de la subred interna siguen siendo los mismos.

Esta configuración de ejemplo utiliza estas direcciones IP:

- Dirección IP externa BQASA existente 200.200.200.200
- Nueva dirección IP externa BQASA 209.165.201.2

Nota: Aquí sólo se modificará la información del par. Debido a que no hay otro cambio en la subred interna, las listas de acceso crypto siguen siendo las mismas.

Configuración de ASDM

Esta sección proporciona información sobre los posibles métodos usados para cambiar la información del peer VPN en HQASA usando el ASDM.

Crear un nuevo perfil de conexión

Este puede ser el método más fácil porque no perturba la configuración VPN existente y puede crear un nuevo perfil de conexión con la nueva información relacionada con el par VPN.

1. Vaya a *Configuration > Site-to-Site VPN > Connection Profiles* y haga clic en *Add* en el área Connection Profiles

1000 1000 1000 S					
Enable interfaces for IPsi	ec access.				
Interface	Allow Acces	55			
outside		¥			
dina					
inside					
	1				
nection Profiles					
nection Profiles	ies the new of a ste-to-stee	connection. It specifies what data traffic	is to be ecounted, how the data traffic	is to be encrypted, and other page	e avelers.
nnection Profiles	ies the peer of a site-to-site	connection. It specifies what data traffic	is to be encrypted, how the data traffic	is to be encrypted, and other pa	raveters.
nection Profiles Connection profile identif Add (2) Edit (1) D	ies the peer of a site-to-site	connection. It specifies what data traffic	is to be encrysted, how the data traffic	is to be encrypted, and other pa	wavelers.
nection Profiles onnection profile identif • Add 2 Edit 1 D	ies the peer of a site-to-site	connection. It specifies what data traffic	is to be encrypted, how the data traffic	is to be encrypted, and other pa	waweters.
nnection Profiles Connection profile identif & Add 2 Edit 1 0 Name	ies the peer of a site-to-site siste	connection. It specifies what data traffic	is to be encrypted, how the data traffic Remote Network	is to be encrypted, and other pa	arameters. Group Policy

Se abre la ventana Agregar perfil de conexión de sitio a sitio IPSec.

2. En la ficha Basic (Básica), proporcione los detalles de *Peer IP Address, Pre-shared Key* y *Protected Networks*. Utilice todos los mismos parámetros que la VPN existente, excepto la información del par. Click

twoored	Peer IP Address:	🗹 Static	209.165.201.2	
Wanceu -	Connection Name:	Same as 1P 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-MD5, ESP-3DE5	SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5	Select
		0.1ml		

3. En el menú Avanzado, haga clic en *Entrada de mapa criptográfico*. Consulte la pestaña *Prioridad*. Esta prioridad es igual al número de secuencia en su configuración CLI equivalente. Cuando se asigna un número menor que la entrada de mapa criptográfico existente, este nuevo perfil se ejecuta primero. Cuanto mayor sea el número de prioridad, menor será el valor. Esto se utiliza para cambiar el orden de secuencia en que se ejecutará un mapa crypto específico. Haga clic en *Aceptar* para completar la creación del nuevo perfil de

conexión.

Basic	Priority:	20	
Crypto Map Entry	Perfect Forward Secrecy:	⊙ Disable ○ Enable	
Tunnel group		Diffie-Helmen Group:	~
	NAT-T:	C Enable	
	Reverse Route Injection:	Enable	
	Security Association Lifetime		
	Time:	8 : 0 : 0	hhimmiss
	Traffic Volume:	4608000	KBytes
	Static Crypto Map Entry Para	ameters	
	Connection Type:	bidirectional	~
	CA Certificate:	None	~
		Send CA Certificate Chain	
	IKE Negotiation Mode:	Main Aggresive	
		Dffle-Helmen Group;	-

Esto crea automáticamente un nuevo grupo de túnel junto con un mapa criptográfico asociado. Asegúrese de que puede alcanzar el BQASA con la nueva dirección IP antes de utilizar este nuevo perfil de conexión.

Editar la configuración VPN existente

Otra forma de agregar un nuevo par es modificar la configuración existente. El perfil de conexión existente no se puede editar para la nueva información del par porque está enlazado a un par específico. Para editar la configuración existente, debe realizar estos pasos:

- 1. Crear un nuevo grupo de túnel
- 2. Editar el mapa criptográfico existente

Crear un nuevo grupo de túnel

Vaya a *Configuration > Site-to-Site VPN > Advanced > Tunnel groups* y haga clic en *Add* para crear un nuevo grupo de túnel que contenga la nueva información de peer VPN. Especifique los campos *Name* y *Pre-shared Key* y luego haga clic en *OK*.

Nota: Asegúrese de que la clave precompartida coincida con el otro extremo de la VPN.

Name:	209.165.201.2	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	6	seconds		
Retry Interval		seconds		
O Headend will never	initiate keepaliv	e monitoring		
Default Group Policy		-171		
Group Policy:	OfItGrpPolicy		~	Manage

Nota: En el campo Name (Nombre), sólo se debe ingresar la dirección IP del par remoto cuando el modo de autenticación es una clave previamente compartida. Cualquier nombre sólo se puede utilizar cuando el método de autenticación es a través de certificados. Este error aparece cuando se agrega un nombre en el campo Nombre y el método de autenticación se comparte previamente:

📽 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-S2S-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-S2S-VPN ipsec-attributes tunnel-group New-S2S-VPN ipsec-attributes [OK] pre-shared-key ********** [OK] isakmp keepalive threshold 10 retry 2
Close

Editar el mapa criptográfico existente

El mapa criptográfico existente se puede editar para asociar la nueva información de peer.

Complete estos pasos:

1. Vaya a *Configuration > Site-to-Site VPN > Advanced > Crypto Maps*, luego seleccione el mapa criptográfico necesario y haga clic en

Edit.									
Configuration	n > Site-to-Site VPN > Advance	d > Crypto Maps							
4 Add - 🖸	🖁 Edit 🔹 👔 Delete 🗇 🌾 🐰	- Q .	Find 🖭 Diago	am					
Transfer	2 Edt				Transform East	Date:	nec	MIT.T.Fashlad	Deursee Deute Stabilit
Typecanor	Z Edit Crypto Map	Destination	Service	Action	Trensrumi Sec	Peer	PFD	WAT-1 Enabled	Reverse Koule Enabled
🕞 interfac	Edit Traffic Selection	Mark Street	5. 7. Š					125	
static: 1	1 ge inside-netwo.	. 192.168.25.	😕 ip	Protect	ESP-AES-128-SHP	4 200.200.200		2 S	

Aparecerá la ventana Edit IPSec Rule.

2. En la ficha Tunnel Policy (Basic), en el área Peer Settings (Parámetros de par), especifique el nuevo par en el campo IP Address of Peer to be add (Dirección IP del par que se va a agregar). Luego, haga clic en Add (Agregar).

🗳 Edit IPsec Rule		
Tunnel Policy (Crypto Map) - Basic	Tunnel Policy (Crypto Map) - Advanced Traffic :	Selection
Interface: outside	Policy Type: static	Priority: 1
Transform Set to Be Added:	ESP-AES-128-SHA	Move Up
ESP-AES-128-MD5	Remove	Move Down
Peer Settings - Optional fo The Connection Type is app for LAN-to-LAN redundancy redundant peers.	r Dynamic Crypto Map Entries licable to static tunnel policies only. Uni-directional o . Tunnel policies of the 'Originate Only' connection t	connection type policies are used ype may specify up to 10
Connection Type:	idirectional 💌	
IP Address of Peer to Be Ad	Ided: 200.200.200 Add >>	Move Up
	Remove	Move Down
Diffie-Helman Group:	g Secrecy	
	OK Cancel Help	

 Seleccione la dirección IP de peer existente y haga clic en *Remove* para conservar la nueva información de peer solamente. Click OK.

unnel Policy (Crypto Map) - B	asic Tunnel Policy (Crypto Map) - Advanced Traffic Se	lection
Interface: outside	Policy Type: static	Priority: 1
Transform Set to Be Add	ded: ESP-AES-128-SHA	Move Up
Peer Settings - Option The Connection Type is for LAN-to-LAN redunda redundant peers.	al for Dynamic Crypto Map Entries applicable to static tunnel policies only. Uni-directional co ncy. Tunnel policies of the 'Originate Only' connection typ	nnection type policies are used pe may specify up to 10
Connection Type:	bidirectional	
IP Address of Peer to Be	Added: 200.200.200.200 Add >> 209.165.201.2	Move Down
	rding Secrety	

Nota: Después de modificar la información del par en el mapa criptográfico actual, el perfil de conexión asociado con este mapa criptográfico se elimina instantáneamente en la ventana ASDM.

4. Los detalles de las redes cifradas siguen siendo los mismos. Si necesita modificarlos, vaya a la ficha *Selección de*

Tunnel Policy	(Crypto Map) - Basic	Tunnel Policy (Crypto Map) - Advanced	Traffic Selection
Action: 💿	Protect 🔿 Do not Pr	rotect	
Source:	10.10.10.0/24		
Destination	192.168.25.0/24		
Service:	īp		

tráfico.

5. Vaya al panel Configuration > Site-to-Site VPN > Advanced > Crypto Maps para ver el mapa crypto modificado. Sin embargo, estos cambios no se producen hasta que haga clic en Aplicar. Después de hacer clic en Aplicar, vaya al menú Configuration > Site-to-Site VPN > Advanced > Tunnel groups para verificar si un túnel-group asociado está o no presente. Si la respuesta es afirmativa, se creará un perfil de conexión asociado

Tunic Drinelly	Traff	ic Selection				Transform Eat	Deer	DEC	MAT.T Foshied	Designing Design
rypermency	#	Source	Destination	Service	Action	mansionin sec	Peer	. 11-2	NATE ENADING	Preverse Produce E
interface: outside			- 61 7 4							
static: 1	1	10 10 10 02		The second s		the second s			a sine the first of the second se	
			- 176-100-20	0	rotect €	ESP-AES-128-SHA	209.165.201.2		2	
ŕ			1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	0	V Protect	ESP-AES-128-SHA	209.165.201.2		v	
¢			1994 196 100 LCO	D	Protect	ESP-AES-128-SHA	209.165.201.2			

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

 Utilice este comando para ver los parámetros de asociación de seguridad específicos de un solo par:<u>show crypto ipsec sa peer <Peer IP address></u>

Troubleshoot

Use esta sección para resolver problemas de configuración.

IKE Initiator unable to find policy: Intf test_ext, Src: 172.16.1.103, Dst: 10.1.4.251

Este error se muestra en los mensajes de registro cuando se intenta cambiar el par VPN de un concentrador VPN a ASA.

Solución:

Esto puede ser el resultado de los pasos de configuración inadecuados seguidos durante la migración. Asegúrese de que el enlace criptográfico a la interfaz se elimine antes de agregar un nuevo par. Además, asegúrese de que utilizó la dirección IP del par en el grupo de túnel, pero no el nombre.

Información Relacionada

- <u>VPN de sitio a sitio (L2L) con ASA</u>
- Problemas de VPN más comunes
- Página de soporte técnico de ASA
- Soporte Técnico y Documentación Cisco Systems