# ASA 8.x/ASDM 6.x: Aggiunta di nuove informazioni peer VPN in una VPN da sito a sito esistente tramite ASDM

### Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Informazioni di background Configurazione ASDM Crea un nuovo profilo di connessione Modifica la configurazione VPN esistente Verifica Risoluzione dei problemi Iniziatore IKE: impossibile trovare il criterio: Testo\_test, Src: 172.16.1.103, Dst: 10.1.4.251 Informazioni correlate

# **Introduzione**

In questo documento vengono fornite informazioni sulle modifiche di configurazione da apportare quando un nuovo peer VPN viene aggiunto alla configurazione VPN da sito a sito esistente utilizzando Adaptive Security Device Manager (ASDM). Questa operazione è necessaria nei seguenti scenari:

- Il provider di servizi Internet (ISP) è stato modificato e viene utilizzato un nuovo insieme di indirizzi IP pubblici.
- Una riprogettazione completa della rete in un sito.
- Il dispositivo utilizzato come gateway VPN in un sito viene migrato in un nuovo dispositivo con un indirizzo IP pubblico diverso.

In questo documento si presume che la VPN da sito a sito sia già configurata correttamente e funzioni correttamente. In questo documento viene descritto come modificare le informazioni su un peer VPN nella configurazione della VPN L2L.

# **Prerequisiti**

### **Requisiti**

Cisco raccomanda la conoscenza di questo argomento:

• Esempio di configurazione della VPN da sito a sito ASA

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Adapative Security Appliance serie 5500 con software versione 8.2 e successive
- Cisco Adapative Security Device Manager con software versione 6.3 e successive

#### **Convenzioni**

Per ulteriori informazioni sulle convenzioni usate, consultare il documento <u>Cisco sulle convenzioni</u> <u>nei suggerimenti tecnici.</u>

### Informazioni di background

La VPN da sito a sito funziona correttamente tra HQASA e BQASA. Si supponga che BQASA abbia completato una riprogettazione della rete e che lo schema IP sia stato modificato a livello di ISP, ma che tutti i dettagli della sottorete interna rimangano invariati.

In questa configurazione di esempio vengono utilizzati i seguenti indirizzi IP:

- Indirizzo BQASA esterno IP esistente 200.200.200.200
- Nuovo indirizzo IP esterno BQASA 209.165.201.2

**Nota:** in questo caso verranno modificate solo le informazioni sul peer. Poiché non vi sono altre modifiche nella subnet interna, gli elenchi degli accessi crittografici rimangono invariati.

# **Configurazione ASDM**

In questa sezione vengono fornite informazioni sui possibili metodi utilizzati per modificare le informazioni peer VPN su HQASA tramite ASDM.

#### Crea un nuovo profilo di connessione

Questo può essere il metodo più semplice perché non disturba la configurazione VPN esistente e può creare un nuovo profilo di connessione con le nuove informazioni correlate al peer VPN.

 Selezionare Configurazione > VPN da sito a sito > Profili di connessione e fare clic su Aggiungi nell'area Profili di connessione.

1055 1100 1 0005					
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

Verrà visualizzata la finestra Aggiungi profilo di connessione da sito a sito IPSec.

2. Nella scheda Basic (Base), specificare i dettagli per *Peer IP Address* (Indirizzo IP peer), *Pre-shared Key* (Chiave già condivisa) e *Protected Networks* (Reti protette). Utilizzare tutti gli stessi parametri della VPN esistente, ad eccezione delle informazioni sul peer. Fare clic su *OK*.

ac teanced	Peer IP Address:	Static 🗸	209.165.201.2	
svances	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:	1.	Next Previous	1	

3. Nel menu Avanzate, fare clic su *Voce mappa crittografica*. Fare riferimento alla scheda *Priorità*. Questa priorità è uguale al numero di sequenza nella configurazione CLI equivalente. Quando viene assegnato un numero inferiore alla voce della mappa crittografica esistente, il nuovo profilo viene eseguito per primo. Maggiore è il livello di priorità, minore sarà il valore. Questa opzione viene usata per modificare l'ordine di sequenza con cui verrà eseguita una mappa crittografica specifica. Fare clic su *OK* per completare la creazione del nuovo profilo di connessione.

Basic	Priority:	20	
dvanced Crypto Map Entry	Perfect Forward Secrecy:	Disable      Enable	
Tunnel group		Diffie-Helman Group:	~
	NAT-T:	Enable	
	Reverse Route Injection:	Enable	
	Security Association Lifetime		
	Time:	8 : 0 : 0	hhimmiss
	Traffic Volume:	4608000	KBytes
	Static Crypto Map Entry Par	ameters	
	Connection Type:	bidirectional	~
	CA Certificate:	None	~
		Send CA Certificate Chain	
	IKE Negotiation Mode:	Main      Aggresive	
		Diffis-Helman Group:	~
1		evt 🙆 Previous	

In questo modo viene creato automaticamente un nuovo gruppo di tunnel con una mappa crittografica associata. Accertarsi di poter raggiungere BQASA con il nuovo indirizzo IP prima di usare questo nuovo profilo di connessione.

#### Modifica la configurazione VPN esistente

Un altro modo per aggiungere un nuovo peer consiste nel modificare la configurazione esistente. Impossibile modificare il profilo di connessione esistente per le nuove informazioni peer perché è associato a un peer specifico. Per modificare la configurazione esistente, effettuare le seguenti operazioni:

- 1. Crea nuovo gruppo di tunnel
- 2. Modifica la mappa crittografica esistente

#### Crea nuovo gruppo di tunnel

Selezionare *Configurazione > VPN da sito a sito > Avanzate > Gruppi di tunnel* e fare clic su *Aggiungi* per creare un nuovo gruppo di tunnel contenente le nuove informazioni peer della VPN. Specificare i campi *Nome* e *Chiave già condivisa*, quindi fare clic su *OK*.

Nota: verificare che la chiave già condivisa corrisponda all'altra estremità della VPN.

Name:	209.165.201.2	2	f	
KE Authentication				
Pre-shared Key:	•••••			
Identity Certificate:	None		~	Manage
Send Certicate Chain:	Enable			
IKE Peer ID Validation:	Required		*	
KE Keepalive				
<ul> <li>Disable keepalives</li> </ul>				
O Monitor keepalives				
Confidence Interva	¢	seconds		
Retry Interval		seconds		
O Headend will never	initiate keepaliv	re monitoring		
Default Group Policy				
Group Policy:	DfltGrpPolicy		~	Manage.

**Nota:** se la modalità di autenticazione è chiavi già condivise, nel campo Nome deve essere immesso solo l'indirizzo IP del peer remoto. È possibile utilizzare qualsiasi nome solo quando il metodo di autenticazione è basato sui certificati. Questo errore viene visualizzato quando si aggiunge un nome nel campo Nome e il metodo di autenticazione è già condiviso:

📽 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

#### Modifica la mappa crittografica esistente

La mappa crittografica esistente può essere modificata per associare le nuove informazioni peer.

Attenersi alla seguente procedura:

1. Selezionare *Configurazione > VPN da sito a sito > Avanzate > Mappe crittografiche*, quindi selezionare la mappa crittografica richiesta e fare clic su

Woditic	ca.								
Configurat	ion > Site-to-Site VPN > Advance	ed > Crypto Maps							
💠 Add 🔹	🕑 Edt - 👔 Delete 🛧 🎸	6 m m - Q F	ind 🖭 Diag	ram					
Transferre	🖉 Edk				Transform Eat	Deer	nec	MAT. T. Fashlad	Desurera Desuta Enablad
Typecento	Edit Crypto Map	Destination	Service	Action	Trensrumi Sec	Peer	PES	WAT-1 Enabled	Reverse Route chaplet
🕞 interfac	Edit Traffic Selection	- Here					-	115	
static: 1	I <u>nside-netwo</u>	🛃 192.168.25	. 😕 ip	Protect	ESP-AES-128-SH	200.200.200		2	

Viene visualizzata la finestra Modifica regola IPSec.

2. Nella scheda Criteri tunnel (di base), nell'area Impostazioni peer, specificare il nuovo peer nel campo Indirizzo IP del peer da aggiungere. Quindi fare clic su *Add*.

🖆 Edit IPsec Rule		
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (	(Crypto Map) - Advanced Traf	ic Selection
Interface: outside	Policy Type: static	Priority: 1
Transform Set to Be Added:	ESP-AES-128-SHA	Move Up
ESP-AES-128-MD5	ve	Move Down:
Peer Settings - Optional for Dynamic Crypt The Connection Type is applicable to static t for LAN-to-LAN redundancy. Tunnel policies redundant peers.	o Map Entries unnel policies only. Uni-direction of the 'Originate Only' connectio	al connection type policies are used on type may specify up to 10
Connection Type: bidirectional	~	
IP Address of Peer to Be Added:	200.200.200.200	Move In
209.165.201.2	ove	Move Down
Diffie-Helman Group:		
ОК	Cancel Help	

3. Selezionare l'indirizzo IP peer esistente e fare clic su *Rimuovi* per mantenere solo le nuove informazioni peer. Fare clic su *OK*.

	IC   Tunnel Policy (Crypto Map) - Advanced   Traffic	Selection
Interface: outside	Policy Type: static	Priority: 1
Transform Set to Be Adde	d: ESP-AES-128-SHA	Move Up
ESP-AES-128-MD5	Remove	Move Down
The Connection Type is ap for LAN-to-LAN redundant	plicable to static tunnel policies only. Uni-directional cy. Tunnel policies of the 'Originate Only' connection	connection type policies are us type may specify up to 10
redundant peers.		
Connection Type:	bidirectional 💌	
redundant peers. Connection Type: IP Address of Peer to Be A	bidirectional	Move Up
redundant peers. Connection Type: IP Address of Peer to Be A	bidirectional	Move Up
Connection Type: IP Address of Peer to Be A	bidirectional	Move Up
Connection Type: IP Address of Peer to Be A	bidirectional	Move Up

**Nota:** dopo aver modificato le informazioni sul peer nella mappa crittografica corrente, il profilo della connessione associato a questa mappa crittografica viene eliminato istantaneamente nella finestra ASDM.

4. I dettagli delle reti crittografate rimangono invariati. Se è necessario modificarli, andare alla scheda *Selezione* 

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

traffico.

\_ \_ \_ \_ \_ \_ \_ \_ \_ \_

5. Per visualizzare la mappa crittografica modificata, andare al riquadro *Configurazione > VPN da sito* a sito > Avanzate > Mappe crittografiche. Tuttavia, queste modifiche non vengono applicate finché non si fa clic su *Applica*. Dopo aver fatto clic su *Applica*, andare al menu *Configurazione > VPN da sito a sito > Avanzate > Gruppi di tunnel* per verificare se è presente un gruppo di tunnel associato. In caso affermativo, verrà creato un *profilo di connessione* 

Turnin Dringiba	Traf	fic Selection				Transform Cab	Dear	PES	MAT.T Fooblad	Davance Doute
(Sherringer)	#	Source	Destination	Service	Action	Transform Sec	Peer		Part of Enabled	Preverse Produce
🖃 interface: outside	0.2									
static: 1	1	10.10.10.0/24	192.168.25	12 io	Protect	ESP-AES-128-SHA	209.165.201.2			
6										

### **Verifica**

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

 Utilizzare questo comando per visualizzare i parametri dell'associazione di sicurezza specifici di un singolo peer:<u>show crypto ipsec sa peer <indirizzo IP peer></u>

# Risoluzione dei problemi

Utilizzare questa sezione per risolvere i problemi relativi alla configurazione.

Iniziatore IKE: impossibile trovare il criterio: Testo\_test, Src: 172.16.1.103, Dst:

### 10.1.4.251

Questo errore viene visualizzato nei messaggi di log quando si cerca di modificare il peer VPN da un concentratore VPN ad ASA.

#### Soluzione:

Ciò può essere dovuto a una procedura di configurazione non corretta eseguita durante la migrazione. Verificare che il binding crittografico all'interfaccia venga rimosso prima di aggiungere un nuovo peer. Verificare inoltre di aver utilizzato l'indirizzo IP del peer nel gruppo di tunnel, ma non il nome.

### Informazioni correlate

- <u>VPN da sito a sito (L2L) con ASA</u>
- Problemi VPN più comuni
- Pagina di supporto tecnico ASA
- Documentazione e supporto tecnico Cisco Systems