# ASA 8.x/ASDM 6.x: Voeg nieuwe VPN-peer informatie toe in een bestaande site-to-site VPN met ASDM

# Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Achtergrondinformatie ASDM-configuratie Een nieuw verbindingsprofiel maken De bestaande VPN-configuratie bewerken Verifiëren Problemen oplossen IKE-initiator kan geen beleid vinden: Intf test\_ext, Src: 172.16.1.103, Dst: 10.1.4.251 Gerelateerde informatie

# Inleiding

Dit document bevat informatie over de configuratie van de wijzigen die moeten worden doorgevoerd wanneer een nieuwe VPN-peer wordt toegevoegd aan de bestaande site-to-site VPN-configuratie met Adaptieve Security Apparaatbeheer (ASDM). Dit is vereist in deze scenario's:

- De Internet Service Provider (ISP) is gewijzigd en er wordt een nieuwe reeks openbare IPtools gebruikt.
- Een compleet nieuw ontwerp van het netwerk op een site.
- Het apparaat dat als gateway van VPN op een plaats wordt gebruikt wordt gemigreerd naar een nieuw apparaat met een verschillend openbaar IP adres.

Dit document gaat ervan uit dat de site-to-site VPN al correct is geconfigureerd en goed werkt. Dit document bevat de te volgen stappen om een VPN-peer informatie in de L2L VPN-configuratie te wijzigen.

# **Voorwaarden**

#### **Vereisten**

Cisco raadt aan dat u kennis hebt van dit onderwerp:

ASA Site-to-Site VPN-configuratievoorbeeld

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco adaptieve security applicatie 5500 Series met softwareversie 8.2 en hoger
- Cisco Adapter Security apparaat Manager met softwareversie 6.3 en hoger

#### **Conventies**

Raadpleeg <u>Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor</u> meer informatie over documentconventies.

### **Achtergrondinformatie**

Het site-to-site VPN werkt prima tussen de HQASA en de BQASA. Stel dat de BQASA een compleet netwerk opnieuw ontworpen heeft en het IP-schema is aangepast op het niveau van de ISP, maar alle interne subnetwerk details blijven hetzelfde.

Deze voorbeeldconfiguratie gebruikt deze IP-adressen:

- Bestaande BQASA buiten IP-adres 20.20.200.200.200
- New BQASA Outside IP Address 209.165.201.2

**Opmerking:** Hier wordt alleen de peer informatie aangepast. Omdat er geen andere verandering is in interne vorm blijven de crypto toegangslijsten hetzelfde.

### **ASDM-configuratie**

Deze sectie verschaft informatie over de mogelijke methoden die worden gebruikt om VPN-peer informatie over HQASA te wijzigen met behulp van ASDM.

#### Een nieuw verbindingsprofiel maken

Dit kan de makkelijkste methode zijn omdat de bestaande VPN-configuratie niet wordt verstoord en u kunt een nieuw verbindingsprofiel maken met de nieuwe VPN peer-gerelateerde informatie.

 Ga naar Configuration > Site-to-Site VPN > Connection-profielen en klik op Add onder het gebied Connection Profile.

Interface	Allow Acces	55			
xutside Imz					
side					
nection Profiles					
mettion Profiles ionnection profile identi	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	raneters.
nection Profiles ionnection profile identi Add 2 Edt 1	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	ravelers.
nnection Profiles Connection profile identi Add 2 Edit 1 C Name	ies the peer of a site-to-site volcto	connection. It specifies what data traffic	is to be encrypted, how the data traffic Remote Network	is to be encrypted, and other pa	group Policy

Het venster Add IPSec Site-to-Site Connection Profile wordt geopend.

2. Typ onder het tabblad Basic de details voor *peer IP-adres*, *voorgedeelde sleutel* en *beschermde netwerken*. Gebruik alle dezelfde parameters als het bestaande VPN, behalve de peer informatie. Klik op *OK* 

and a second	Peer IP Address: [	🗹 Static	209.165.201.2	
vanceu	Connection Name: [	Same as IP Address	209.165.201.2	
	Interface:	outside	×	
	IKE Authentication			
	Pre-shared Key:	•••••		
	Identity Certificate:	None	<b>•</b>	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-MDS, ESP-DES-SHA, ESP-DES-MDS	Select

3. Klik onder het menu Geavanceerd op *Crypto Map*. Raadpleeg het tabblad *Prioriteit*. Deze prioriteit is gelijk aan het sequentienummer in zijn equivalente CLI-configuratie. Wanneer een kleiner aantal dan de bestaande crypto map entry is toegewezen, wordt dit nieuwe profiel eerst uitgevoerd. Hoe hoger het prioriteitsnummer, hoe lager de waarde. Dit wordt gebruikt om de volgorde van sequentie te veranderen dat een specifieke crypto kaart zal worden uitgevoerd. Klik op *OK* om het maken van het nieuwe verbindingsprofiel te voltooien.

asic	Priority:	20	
dvanced Crypto Map Entry	Perfect Forward Secrecy:	Disable     Disable	
Tunnel group		Diffie-Helmen Group:	~
	NAT-T:	C Enable	
	Reverse Route Injection:	Enable	
	Security Association Lifetime		
	Time:	8 ; 0 ; 0	hhimmis
	Traffic Volume:	4608000	KBytes
	Static Grypto Map Entry Par	ameters	
	Connection Type:	bidirectional	~
	CA Certificate:	None	~
		Send CA Certificate Chain	
	IKE Negotiation Mode:	Main O Aggresive	
		Diffie-Helmen Group:	~
(		ant Operations	

Dit creëert automatisch een nieuwe tunnelgroep samen met een gekoppelde crypto kaart. Zorg ervoor dat u de BQASA met het nieuwe IP-adres kunt bereiken voordat u dit nieuwe verbindingsprofiel gebruikt.

#### De bestaande VPN-configuratie bewerken

Een andere manier om een nieuw peer toe te voegen is de bestaande configuratie aan te passen. Het bestaande verbindingsprofiel kan niet voor de nieuwe peer informatie worden bewerkt omdat het aan een specifieke peer is gebonden. U moet de volgende stappen uitvoeren om de bestaande configuratie te bewerken:

- 1. Een nieuwe tunnelgroep maken
- 2. Bewerk de bestaande encryptie-kaart

#### Een nieuwe tunnelgroep maken

Ga naar *Configuratie > Site-to-Site VPN > Geavanceerd > Tunnelgroepen* en klik op *Add* om een nieuwe tunnelgroep te maken die de nieuwe VPN peer informatie bevat. Specificeer de velden *Naam* en *Voorgedeeld sleutel* en klik vervolgens op *OK*.

**Opmerking:** Controleer of de vooraf gedeelde sleutel overeenkomt met het andere uiteinde van VPN.

Name:	209.165.201.	2		
KE Authentication				
Pre-shared Key:	•••••			
Identity Certificate:	None		~	Manage
Send Certicate Chain:	Enable			3
IKE Peer ID Validation:	Required		~	
KE Keepalive	s			
Oisable keepalives				
O Monitor keepalives				
Confidence Interva	6 L	seconds		
Retry Interval		seconds		
O Headend will never	initiate keepali	ve monitoring		
Default Group Policy				
Group Policy:	DfltGrpPolicy		~	Manage.

**Opmerking:** In het veld Naam dient alleen het IP-adres van de externe peer te worden ingevoerd wanneer de verificatiemodus van tevoren gedeelde sleutels is. Elke naam kan alleen worden gebruikt wanneer de echtheidsmethode door middel van certificaten wordt gebruikt. Deze fout verschijnt wanneer een naam wordt toegevoegd in het veld Naam en de verificatiemethode wordt vooraf gedeeld:

🜃 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-525-VPN type ipsec-121 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-525-VPN ipsec-attributes tunnel-group New-525-VPN ipsec-attributes           [OK] pre-shared-key **********         [OK] isakmp keepalive threshold 10 retry 2
Close

#### Bewerk de bestaande encryptie-kaart

De bestaande crypto kaart kan worden bewerkt om de nieuwe peer informatie te koppelen.

Voer de volgende stappen uit:

1. Ga naar *Configuration > Site-to-Site VPN > Advanced > Crypto Maps*, selecteer de gewenste crypto-kaart en klik op

Bewerke	en.								
Configuration	> Site-to-Site VPN > Advance	d > Crypto Maps	പ്പെംപ						
Add +	Edt Delete T +	- 42 mil - ) Q, h	nd 🖽 Diagr	am					
Type:Prior	Edit Crypto Map	Destination	Service	Action	Transform Set	Peer	PFS	NAT-T Enabled	Reverse Route Enabled
🕞 interfac	Edit Traffic Selection							<u>. U</u>	
static: 1	i <u>De</u> inside-netwo.	. 192.168.25	. 😰 ip	Protect	ESP-AES-128-594	200.200.200.			

Het venster IPSec-regel bewerken verschijnt.

2. Onder het tabblad Tunnel beleid (Basis) specificeert u in het gebied Peer Instellingen de nieuwe peer in het veld IP Adres van peer die wordt toegevoegd. Klik vervolgens op *Add* (Toevoegen).

	ic Tunnel Policy (Crypto Map) - Advan	ced Traffic Selection	
Interface: outside	Policy Type: static	÷	Priority:
Transform Sets Transform Set to Be Adde	d:ESP-AES-1	28-SHA	
ESP-AES-128-MD5	Add >>		Move Up
The Connection Type is ap for LAN-to-LAN redundance	plicable to static tunnel policies only. Ur y. Tunnel policies of the 'Originate Only	hi-directional connection	n type policies are
redundant peers.	bidirectional		specify up to 10
redundant peers. Connection Type:	bidirectional	200.200	specify up to 10
redundant peers. Connection Type: IP Address of Peer to Be A 209.165.201.2	bidirectional dded: Add >> Remove	200.200	Move Up
redundant peers. Connection Type: IP Address of Peer to Be A 209.165.201.2	bidirectional	200.200	Move Up
redundant peers. Connection Type: IP Address of Peer to Be A 209.165.201.2 Enable Perfect Forward Diffie-Helman Group:	bidirectional	200.200	Move Up Move Down

3. Selecteer het bestaande peer IP-adres en klik op *Verwijderen* om alleen de nieuwe peerinformatie te behouden. Klik op *OK*.

inel Policy (Crypto Map) -	Basic Tunnel Policy (Crypto Map) - Advanc	ed Traffic Selection
Interface: outside	Policy Type: static	Priority: 1
Transform Set to Be A	ided: ESP-AES-12	28-SHA
ESP-AES-128-MD5	Remove	Move Down
Peer Settings - Optio	nal for Dynamic Crypto Map Entries	
The Connection Type i for LAN-to-LAN reduce	s applicable to static tunnel policies only. Un ancy. Tunnel policies of the 'Originate Only'	-directional connection type policies are us connection type may specify up to 10
The Connection Type i for LAN-to-LAN redund redundant peers. Connection Type:	s applicable to static tunnel policies only. Un ancy. Tunnel policies of the 'Originate Only' bidirectional	-directional connection type policies are us connection type may specify up to 10
The Connection Type i for LAN-to-LAN redund redundant peers. Connection Type: IP Address of Peer to I	e Added:	of the officient of the
The Connection Type i for LAN-to-LAN redund redundant peers. Connection Type: IP Address of Peer to I	is applicable to static tunnel policies only. Uni ancy. Tunnel policies of the 'Originate Only' bidirectional	onnection type may specify up to 10
The Connection Type i for LAN-to-LAN redund redundant peers. Connection Type: IP Address of Peer to I	ancy. Tunnel policies of the 'Originate Only' bidirectional	directional connection type policies are us connection type may specify up to 10 00.200 01.2 Move Up

**Opmerking:** Nadat u de peer informatie in de huidige crypto map hebt gewijzigd, wordt het verbindingsprofiel dat bij deze crypto map hoort direct verwijderd in het ASDM-venster.

4. De details van de versleutelde netwerken blijven hetzelfde. Als u deze instellingen wilt wijzigen, gaat u naar het tabblad *Verkeerselectie*.

unnel 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. Kies het venster Configuration > Site-to-Site VPN > Advanced > Crypto Maps om de aangepaste crypto-kaart te bekijken. Deze wijzigingen vinden echter niet plaats totdat u op Toepassen klikt. Nadat u op Toepassen klikt, gaat u naar de Configuration > Site-to-Site VPN > Advanced > Tunnel Groepen om te controleren of er een gekoppelde tunnelgroep al dan niet aanwezig is. Als ja, dan wordt een gekoppeld verbindingsprofiel gecreëerd

Toronia Palantha	Traffic Selection	n'					0	-	MAX X Frankland	Davis and Davids
Type:Priority	# Source		Destination	Service	Action	transform Sec	Peer	. 14-2	NAT-T Enabled	Reverse Houten
interface: outside	Page and				1000					
static: 1	1 10.10	0.10.0/24	192.168.25	20	Protect	ESP-AES-128-SHA	209.165.201.2		Image:	
¢ -			- 11				Ĵ.			

# Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het <u>Uitvoer Tolk</u> (<u>uitsluitend geregistreerde</u> klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

 Gebruik deze opdracht om de parameters van de veiligheidsassociatie die specifiek zijn voor één peer, te bekijken:<u>crypto-ipsec als peer <peer IP-adres> tonen</u>

### Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

IKE-initiator kan geen beleid vinden: Intf test\_ext, Src: 172.16.1.103, Dst: 10.1.4.251

Deze fout wordt in de logberichten weergegeven wanneer u de VPN-peer van een VPNconcentrator naar ASA probeert te wijzigen.

#### Oplossing:

Dit kan een gevolg zijn van ongeschikte configuratiestappen die tijdens de migratie zijn gevolgd. Zorg ervoor dat de crypto binding aan de interface wordt verwijderd voordat u een nieuw peer toevoegt. Zorg er ook voor dat u het IP-adres van de peer in de tunnel-groep gebruikte, maar niet de naam.

# **Gerelateerde informatie**

- Site to Site (L2L) VPN met ASA
- Populairste VPN-problemen
- ASA pagina voor technische ondersteuning
- Technische ondersteuning en documentatie Cisco Systems