ASA 8.x/ASDM 6.x : Ajouter de nouvelles informations d'homologue VPN dans un VPN site à site existant à l'aide d'ASDM

Contenu

Introduction Conditions préalables Conditions requises Components Used Conventions Informations générales Configuration ASDM Créer un profil de connexion Modifier la configuration VPN existante Vérification Dépannage IKE Initiator unable to find policy: Intf test_ext, Src : 172.16.1.103, Dst : 10.1.4.251 Informations connexes

Introduction

Ce document fournit des informations sur les modifications de configuration à apporter lorsqu'un nouvel homologue VPN est ajouté à la configuration VPN site à site existante à l'aide d'Adaptive Security Device Manager (ASDM). Ceci est nécessaire dans ces scénarios :

- Le fournisseur d'accès à Internet (FAI) a été modifié et un nouvel ensemble de plages d'adresses IP publiques est utilisé.
- Refonte complète du réseau sur un site.
- Le périphérique utilisé comme passerelle VPN sur un site est migré vers un nouveau périphérique avec une adresse IP publique différente.

Ce document suppose que le VPN site à site est déjà configuré correctement et fonctionne correctement. Ce document fournit les étapes à suivre afin de modifier les informations d'homologue VPN dans la configuration VPN L2L.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez une connaissance de ce sujet :

• Exemple de configuration de VPN site à site ASA

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme Cisco Adaptive Security Appliance 5500 avec logiciel version 8.2 et ultérieure
- Cisco Adaptive Security Device Manager avec logiciel version 6.3 et ultérieure

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

Informations générales

Le VPN de site à site fonctionne correctement entre HQASA et BQASA. Supposons que le BQASA a fait l'objet d'une reconception complète du réseau et que le schéma IP a été modifié au niveau du FAI, mais que tous les détails du sous-réseau interne restent les mêmes.

Cet exemple de configuration utilise les adresses IP suivantes :

- Adresse IP externe BQASA existante 200.200.200.200.200
- Nouvelle adresse IP externe BQASA 209.165.201.2

Note : Ici, seules les informations d'homologue seront modifiées. Comme il n'y a pas d'autre changement dans le sous-réseau interne, les listes d'accès de chiffrement restent les mêmes.

Configuration ASDM

Cette section fournit des informations sur les méthodes possibles utilisées pour modifier les informations d'homologue VPN sur HQASA à l'aide de l'ASDM.

Créer un profil de connexion

Cette méthode peut être plus simple car elle ne perturbe pas la configuration VPN existante et peut créer un nouveau profil de connexion avec les nouvelles informations relatives aux homologues VPN.

 Accédez à Configuration > Site-to-Site VPN > Connection Profiles et cliquez sur Add sous la zone Connection Profiles.

inable interfaces for IPs	ec access.				
Interface	Allow Acce	56			
autside		×			
dira					
nside					
nection Profiles					
nection Profiles	ies the peer of a ste-to-sta	e connection. It specifies what data traffic	is to be encrysted, how the data traffic	is to be encrypted, and other pa	ravelers.
metton Profiles	ies the peer of a site-to-site	e connection. It specifies what data traffic	is to be encrypted, how the data traffic	is to be encrypted, and other par	ravelers.
nnection Profiles Connection profile identi & Add 🕼 Edt 📋 C	ies the peer of a site-to-site	e connection. It specifies what data traffic	is to be encrypited, how the data traffic	is to be encrypted, and other par	rameters.
nnection Profiles Connection profile identi	ies the peer of a site-to-site voloto	e connection. It specifies what data traffic	is to be encrypted, how the data traffic	is to be encrypted, and other par	rameters.
nnection Profiles Connection profile identi Add 2 Edt 1 0 Name	ies the peer of a site-to-site voioto	e connection. It specifies what data traffic Local Network	is to be encrypted, how the data traffic Remote Network	is to be encrypted, and other pa	rameters. Group Policy

La fenêtre Ajouter un profil de connexion de site à site IPSec s'ouvre.

 Sous l'onglet Basic, indiquez les détails de l'adresse IP de l'homologue, de la clé prépartagée et des réseaux protégés. Utilisez tous les mêmes paramètres que le VPN existant, à l'exception des informations d'homologue. Click OK.

asic duanced	Peer IP Address:	🗹 Static	209.165.201.2	
www.anceu	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-MD5, ESP-3DE5	SHA, ESP-3DES-MD5, ESP-DES-SHA, ESP-DES-MD5	Select
d:		Rest Previous	1	

3. Sous le menu Avancé, cliquez sur Entrée de crypto-carte. Reportez-vous à l'onglet Priorité. Cette priorité est égale au numéro de séquence dans sa configuration CLI équivalente. Lorsqu'un nombre inférieur à l'entrée de crypto-carte existante est attribué, ce nouveau profil est exécuté en premier. Plus le numéro de priorité est élevé, plus la valeur est faible. Ceci est utilisé pour modifier l'ordre de séquence d'une crypto-carte spécifique qui sera exécutée. Cliquez sur *OK* pour terminer la création du nouveau profil de connexion.

sic	Priority:	20	
anced Crypto Map Entry	Perfect Forward Secrecy:	Disable DEnable	
Tunnel group		Diffie-Helman Group:	2
	NAT-T:	🗹 Enable	
	Reverse Route Injection:	Enable	
	Security Association Lifetime	1 	8.4
	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	
		Diffie-Helman Group:	-
		and Charles	

Cela crée automatiquement un nouveau groupe de tunnels avec une carte de chiffrement associée. Assurez-vous que vous pouvez atteindre le BQASA avec la nouvelle adresse IP avant d'utiliser ce nouveau profil de connexion.

Modifier la configuration VPN existante

Une autre manière d'ajouter un nouvel homologue consiste à modifier la configuration existante. Le profil de connexion existant ne peut pas être modifié pour les nouvelles informations d'homologue, car il est lié à un homologue spécifique. Pour modifier la configuration existante, vous devez effectuer les étapes suivantes :

- 1. Créer un nouveau groupe de tunnels
- 2. Modifier la carte de chiffrement existante

Créer un nouveau groupe de tunnels

Accédez à *Configuration > Site-to-Site VPN > Advanced > Tunnel groups* et cliquez sur *Add* pour créer un nouveau tunnel-group qui contient les nouvelles informations d'homologue VPN. Spécifiez les champs *Nom* et *Clé prépartagée*, puis cliquez sur *OK*.

Remarque : assurez-vous que la clé pré-partagée correspond à l'autre extrémité du 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				
 Disable keepalives 				
O Monitor keepalives				
Confidence Interva	¢ .	seconds		
Retry Interval:		seconds		
O Headend will never	initiate keepaliv	e monitoring		
Default Group Policy				
Group Policy:	DfltGrpPolicy		~	Manage

Remarque : dans le champ Nom, seule l'adresse IP de l'homologue distant doit être entrée lorsque le mode d'authentification est des clés pré-partagées. N'importe quel nom ne peut être utilisé que lorsque la méthode d'authentification passe par des certificats. Cette erreur apparaît lorsqu'un nom est ajouté dans le champ Nom et que la méthode d'authentification est pré-partagée :

📽 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

Modifier la carte de chiffrement existante

La carte de chiffrement existante peut être modifiée afin d'associer les nouvelles informations d'homologue.

Procédez comme suit :

1. Accédez à *Configuration > Site-to-Site VPN > Advanced > Crypto Maps*, puis sélectionnez la crypto-carte requise et cliquez sur

Edit.										
Configurati	on >	Site-to-Site VPN > Advanced	d > Crypto Maps							
🗣 Add 🔹	C'	dt - 👔 Delete 🛧 🗸 👗	10 m · Q.F	ind 🖭 Diag	ram					
Transferre	đ	Edit				Transform East	E.e.e.	nec	MAT T Pachlad	Davide Davida Davida
туресяно	đ	Edit Crypto Map	Destination	Service	Action	Trensrumn Sec.	Peer	PTS	INAT-1 Enabled	Reverse Koute Enabled
🖃 interfac	đ	Edit Traffic Selection	Market and the second	Ser a			<u></u>	-	123	
static: 1	57	1nside-netwo	192.168.25	. 💌 ip	Protect	ESP-AES-128-SHP	200.200.200		2	

La fenêtre Modifier la règle IPSec apparaît.

2. Sous l'onglet Tunnel Policy (Basic), dans la zone Peer Settings, spécifiez le nouvel homologue dans le champ IP Address of Peer to add. Puis, cliquez sur Add (ajouter).

	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 v added: 200.200.2 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. Sélectionnez l'adresse IP d'homologue existante et cliquez sur *Supprimer* pour conserver uniquement les nouvelles informations d'homologue. Click 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

Remarque : après avoir modifié les informations d'homologue dans la crypto-carte actuelle, le profil de connexion associé à cette crypto-carte est supprimé instantanément dans la fenêtre ASDM.

4. Les détails des réseaux chiffrés restent les mêmes. Si vous devez les modifier, accédez à l'onglet *Traffic*

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

Selection.

5. Accédez au volet Configuration > Site-to-Site VPN > Advanced > Crypto Maps afin d'afficher la crypto-carte modifiée. Cependant, ces modifications ne sont pas effectuées avant que vous cliquiez sur Appliquer. Après avoir cliqué sur Apply, accédez au menu Configuration > Site-to-Site VPN > Advanced > Tunnel groups afin de vérifier si un groupe de tunnels associé est présent ou non. Si oui, un profil de connexion associé sera oréé

Tunic Bright	Traf	fic Selection				Transform Cab	Deer	DEC	MAT.T Enabled	Daviasian Doctor
cyper-mancy	#	Source	Destination	Service	Action	Transform Sec	Peer	. PF-2	Part Frenderou	Preverse Produe e
interface: outside	in an		- 61 T 1		10000					
static: 1	1	10.10.10.0/24	192.168.25	10	Protect	ESP-AES-128-SHA	209.165.201.2		Image:	
							Ť			
¢.							Ĩ			

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'<u>Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines</u> <u>commandes show.</u> Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

 Utilisez cette commande pour afficher les paramètres d'association de sécurité spécifiques à un homologue unique :<u>show crypto ipsec sa peer <adresse IP de l'homologue></u>

<u>Dépannage</u>

Utilisez cette section pour dépanner votre configuration.

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

Cette erreur s'affiche dans les messages du journal lors de la tentative de modification de l'homologue VPN d'un concentrateur VPN à ASA.

Solution :

Cela peut être dû à des étapes de configuration incorrectes suivies lors de la migration. Assurezvous que la liaison de chiffrement à l'interface est supprimée avant d'ajouter un nouvel homologue. Vérifiez également que vous avez utilisé l'adresse IP de l'homologue dans le groupe de tunnels, mais pas le nom.

Informations connexes

- VPN site à site (L2L) avec ASA
- Problèmes VPN les plus courants
- Page d'assistance technique ASA
- Support et documentation techniques Cisco Systems