Exemplo de configuração de ASA para ASA de IKEv1/IPsec dinâmico para estático

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados Configurar Diagrama de Rede Configuração do ASDM Central-ASA (Peer estático) Remote-ASA (Peer dinâmico) Configuração de CLI Configuração do ASA central (peer estático) Remote-ASA (Peer dinâmico) Verificar **ASA** central ASA remoto Troubleshoot Remote-ASA (iniciador) Central-ASA (respondedor) Informações Relacionadas

Introduction

Este documento descreve como permitir que o Adaptive Security Appliance (ASA) aceite conexões VPN IPsec site-to-site dinâmicas de qualquer peer dinâmico (ASA neste caso). Como mostra o Diagrama de Rede neste documento, o túnel IPsec é estabelecido quando o túnel é iniciado somente a partir da extremidade do Remote-ASA. O Central-ASA não pode iniciar um túnel VPN devido à configuração dinâmica do IPsec. O endereço IP do Remote-ASA é desconhecido.

Configure o Central-ASA para aceitar dinamicamente conexões de um endereço IP curinga (0.0.0/0) e de uma chave pré-compartilhada curinga. O Remote-ASA é, então, configurado para criptografar o tráfego das sub-redes local para o Central-ASA, conforme especificado pela lista de acesso de criptografia. Ambos os lados executam a isenção de NAT (Network Address Translation Conversão de Endereço de Rede) para ignorar o NAT para o tráfego IPsec.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no software Cisco ASA (5510 e 5520) Firewall versão 9.x e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Note: Use a <u>Command Lookup Tool (somente clientes registrados) para obter mais</u> informações sobre os comandos usados nesta seção.



Diagrama de Rede

Configuração do ASDM

Central-ASA (Peer estático)

Em um ASA com um endereço IP estático, configure a VPN de forma que aceite conexões dinâmicas de um peer desconhecido enquanto ela autentica o peer usando uma chave précompartilhada IKEv1:

 Escolha Configuration > Site-to-Site VPN > Advanced > Crypto Maps. A janela exibe a lista de entradas do mapa de criptografia que já estão em vigor (se houver). Como o ASA não sabe qual é o endereço IP do peer, para que o ASA aceite a conexão configure o mapa dinâmico com um conjunto de transformação correspondente (Proposta de IPsec). Clique em

Add.

File View Tools Wizards Window Help						Fype	topic to search	h
🔥 Home 🔥 Configuration 📄 Monitoring 🔚 Save 🔇	Refresh 😋 Back 🌔	Porward ? Help						
Site-to-Site VPN d ² 0	Configuration > S	te-to-Site VPN > Adva	nced > Crypto Map					
Connection Profiles	♦ Add • 🛒 Eck	- 🏦 Delete 🕈 🗲	二面面-二角	Find 🔠 Diagram				
Certificate Management Advanced Tornel Genuss	Type:Priority	Traffic Selection Source	Destination	Service Action	Transform Set (IKEv1)	IPsec Proposal (IKEv2)	Peer	PPS P
- B DE Polices								
DE Parameters DEsec Proposals (Transform Sets)								
Proce Prefragmentation Policies Certificate to Connection Profile Maps								
- System Options - Drypto Engine								
- By ACI, Manager								
0								
Device Setup								
🕄 Frend								
G Remote Access VPN								
🚱 Ske-to-Ske VPN	Crable Anti-rep	lay window size: 64						
Device Management	() - and the tag							
					Apply Reset			

2. Na janela Create IPsec Rule, na guia Tunnel Policy (Crypto Map) - Basic, escolha outside na lista suspensa Interface e dynamic na lista suspensa Policy Type. No campo Prioridade, atribua a prioridade para essa entrada caso haja várias entradas em Mapa dinâmico. Em seguida, clique em Selecionar ao lado do campo Proposta IPsec IKE v1 para selecionar a proposta

IPsec.

, (,	/pto Map) - Basic	Tunnel Policy (Crypto Map)	- Advanced Traffic Se	lection
Interface:	outside	 Policy Type: 	dynamic 👻	Priority: 1
IPsec Propo	sals (Transform S	Sets)		
IKE v1 IPsec	: Proposal:			Select
IKE v2 IPsec	: Proposal:			Select
Deer Settie	Ontional for	Dupania Cruzka Man Fakuiaa		
Peer Setting	gs - Optional for	Dynamic Crypto Map Entries		
Peer Setting The Conner for LAN-to-	gs - Optional for ction Type is appl LAN redundancy.	Dynamic Crypto Map Entries icable to static tunnel policies Tunnel policies of the 'Origina	only. Uni-directional cor ate Only' connection typ	nnection type policies are used be may specify up to 10
Peer Setting The Connec for LAN-to- redundant	gs - Optional for ction Type is appl LAN redundancy. peers.	Dynamic Crypto Map Entries icable to static tunnel policies . Tunnel policies of the 'Origina	only. Uni-directional cor ate Only' connection typ	nnection type policies are used be may specify up to 10
Peer Setting The Connec for LAN-to- redundant	gs - Optional for ction Type is appl LAN redundancy. peers.	Dynamic Crypto Map Entries icable to static tunnel policies . Tunnel policies of the 'Origina	only. Uni-directional cor ate Only' connection typ	nnection type policies are used be may specify up to 10
Peer Setting The Conner for LAN-to- redundant	gs - Optional for ction Type is appl LAN redundancy. peers.	Dynamic Crypto Map Entries icable to static tunnel policies . Tunnel policies of the 'Origina	only. Uni-directional cor ate Only' connection typ	nnection type policies are used be may specify up to 10
Peer Setting The Connec for LAN-to- redundant	gs - Optional for ction Type is appl LAN redundancy. peers.	Dynamic Crypto Map Entries icable to static tunnel policies . Tunnel policies of the 'Origina	only. Uni-directional cor ate Only' connection typ	nnection type policies are used be may specify up to 10
Peer Setting The Connec for LAN-to- redundant IP Address	gs - Optional for ction Type is appl LAN redundancy. peers. of Peer to Be Ad	Dynamic Crypto Map Entries icable to static tunnel policies . Tunnel policies of the 'Origina ded:	only. Uni-directional con ate Only' connection typ	nnection type policies are used be may specify up to 10
Peer Setting The Connec for LAN-to- redundant IP Address	gs - Optional for ction Type is appl LAN redundancy. peers. of Peer to Be Ad	Dynamic Crypto Map Entries icable to static tunnel policies . Tunnel policies of the 'Origina ded: Add >>	only. Uni-directional cor ate Only' connection typ	nnection type policies are used be may specify up to 10 Move Up
Peer Setting The Connec for LAN-to- redundant IP Address	gs - Optional for ction Type is appl LAN redundancy. peers. of Peer to Be Ad	Dynamic Crypto Map Entries icable to static tunnel policies . Tunnel policies of the 'Origina ded:	only. Uni-directional con ate Only' connection typ	Move Up

3. Quando a caixa de diálogo Selecionar propostas de IPsec (Conjuntos de transformações) for aberta, escolha entre as propostas de IPsec atuais ou clique em **Adicionar** para criar uma nova e usar a mesma. Clique em **OK** quando terminar.

					1
Psec Propos	als (Transform Sets)				
E v1 IPsec F	Proposal: tset			Select	
E V2 IPS	Select IPsec Prop	osals (Transfo	rm Sets)		23
	Selectifisee riop				
	🖨 add 🗖 cab	🛱 Dalata			
	A WOO S COIC	Delece			
	Name	Mode	ESP Encryption	ESP Authentication	
	EED ODEC CHA	Transach	20.55	CUA	
eer Settii	ESP-3DES-SHA	Transport	JUES	SHA	
The Conne	ESP-SUES-PIUS	Turnsport	JUES	MUS	
	ESP-DES-SHA	Tunnel	DES	MOE	
or LAN-to	EDP*DED*PID5	Tunnel	DES	MUS	
or LAN-to edundani	ECD DEC CHA T		DED	MIC	-
or LAN-to edundani	ESP-DES-SHA-T	Transport	DEC	MOE	=
or LAN-to edundani	ESP-DES-SHA-T ESP-DES-MDS-T	Transport	DES	MD5	
or LAN-to edundan	ESP-DES-SHA-T ESP-DES-MD5-T tset	Transport	DES AES-256	MD5 SHA	-
edundani P. Addrec	ESP-DES-SHA-T ESP-DES-MD5-T tset Assigned IPsec Pro	Transport Tunnel posals	DES AES-256	MD5 SHA	•
or LAN-to edundan P Addres	ESP-DES-SHA-T ESP-DES-MD5-T tset Assigned IPsec Pro Assign-> ts	Transport Transport Tunnel posals	DES AES-256	MD5 SHA	•

4. Na guia Tunnel Policy (Crypto Map)-Advanced (Política de túnel (Mapa de criptografia)-Advanced), marque a caixa de seleção Enable NAT-T (Habilitar NAT-T) (necessária se um dos pares estiver atrás de um dispositivo NAT) e a caixa de seleção Enable Reverse Route Inject (Habilitar injeção de rota reversa). Quando o túnel VPN é ativado para o peer dinâmico, o ASA instala uma rota dinâmica para a rede VPN remota negociada que aponta para a interface

VPN.

Create IPsec Rule	23
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
C Enable NAT-T	
Enable Reverse Route Injection	
Security Association Lifetime Settings	
Time: 8:0:0 hh:mm:ss	
Traffic Volume: 🔲 unlimited 4608000 KBytes	
Validate incoming ICMP error messages	
Enable Do Not Fragment (DF) policy	
Enable Traffic Flow Confidentiality (TFC) packets, This is unavailable if IKEv1 is enabled,	
OK Cancel Help	

Opcionalmente, na guia Seleção de tráfego, você também pode definir o tráfego de VPN interessante para o peer dinâmico e clicar em OK.

Create IPsec	Rule	Σ
Tunnel Policy ((Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Action: 💿 F	Protect 💿 Do not Protect	
Source Criter	ia	
Source:	any4	
Destination C	Iriteria	
Destination:	any4	
Service:	ip	
Description:		
More Opti	ons	۲
📝 Enable	Rule	
Source Ser	vice: (TCP or UDP service only) 😗	
Time Range	e:	
	OK Cancel Help	

Configuration > Site-t	:o-Sil	e VPN > Advance	d > <u>Crypto Maps</u>			
🖶 Add 🕶 📝 Edit 👻 🛛	🗍 De	lete 🛧 🗲 🐰	🛍 💼 - 🛛 🔍 Fin	d 👥 Diagi	am	
T Diation	Traff	ic Selection				Turn from Cab (IVE1)
Type:Priority	#	Source	Destination	Service	Action	Transform Set (IKEV1)
🖃 interface: outside						
ⁱ dynamic: 65535.1	1	🌍 any4	🌍 any4	IP ip	🖌 Protect	tset
•			III			
📝 Enable Anti-replay w	vindov	v size: 64 👻				
					Apply	Reset

Como mencionado anteriormente, como o ASA não tem nenhuma informação sobre o endereço IP do peer dinâmico remoto, a solicitação de conexão desconhecida fica no DefaultL2LGroup que existe no ASA por padrão. Para que a autenticação seja bem-sucedida, a chave pré-compartilhada (cisco123 neste exemplo) configurada no peer remoto precisa corresponder a uma em DefaultL2LGroup.

5. Escolha Configuration > Site-to-Site VPN > Advanced > Tunnel Groups, selecione DefaultL2LGgroup, clique em Edit e configure a chave pré-compartilhada desejada. Clique em OK quando terminar.

	Group Policy	IKEv1 En	abled	IKEv2 Enabled
faultL2LGroup	DfltGrpPolicy			
		Edit IPsec Site-to-site	unnel Group: DefaultL2LGroup	
		Name: D	efaultL2LGroup	
		IPsec Enabling		
		Group Policy Name:	fltGrpPolicy	✓ Manage
		0	ollowing two fields are attributes of	the group policy selected abo
			/ Enable IKE v1 📄 Enable IKE v2	
		IDser Settings		
		IKE v1 Settings		
		Authentication		
		Pre-shared Key: •		
		Pre-shared Key: • Device Certificate:	None	▼ Manage
		Pre-shared Key: • Device Certificate: IKE Peer ID Validation:	None	Manage
		IKE Peer ID Validation:	None tequired	▼ Manage
		IKE Keepalive	None tequired	Manage
		IKE Peer ID Validation:	None tequired	▼ Manage
		Pre-shared Key: Device Certificate: IKE Peer ID Validation: IKE Keepalive Disable keepalives Monitor keepalives Confidence Interval:	None tequired	Manage

ofiguration > Site-to-Site VPN > Advanced > Tun

Note: Isso cria uma chave pré-compartilhada curinga no peer estático (Central-ASA). Qualquer dispositivo/peer que conheça essa chave pré-compartilhada e suas propostas correspondentes podem estabelecer com êxito um túnel VPN e acessar recursos por VPN. Certifique-se de que esta chave pré-desenhada não é partilhada com entidades desconhecidas e não é fácil de adivinhar.

6. Escolha Configuration > Site-to-Site VPN > Group Policies e selecione a política de grupo de sua escolha (política de grupo padrão neste caso). Clique em Editar e edite a política de grupo na caixa de diálogo Editar política interna de grupo. Clique em OK quando terminar.

	Туре	Tunneling Protocol	Connection Profiles/Users Assigned To
irpPolicy (System Default)	Internal	kev1;ssl-clientless;l2tp-ipsec	DefaultRAGroup;DefaultWEBVPI
	Edit Internal Group Pol	icy: DfltGrpPolicy	2
	Name:	DfltGrpPolicy	
	Tunneling Protocols:	Clientless SSL VPN 📄 SSL VPN Client 🕑 IPser	c IKEv1 🔄 IPsec IKEv2 📝 L2TP/IPsec
	Filter:	None	▼ Manage
	Idle Timeout:	Unlimited 30 minutes	
	Maximum Connect Time:	V Linimited minutes	
	PidAmuni Comico, milo,	• or minored	
	Prevention Competer Inter		
	PROVINGIN CONNECC. HINES		
	PROVINGIN CONNECC. HINES	OK Cancel Help	

 Escolha Configuration > Firewall > NAT Rules e, na janela Add Nat Rule, configure uma regra no nat (NAT-EXEMPT) para tráfego VPN. Clique em OK quando terminar.

Configuration 2	> Firewall > NAT Rules			
🗣 Add 🗸 📝	📧 Add NAT Rule	6 4 m Bran	e	X
# Match 0	Match Criteria: Original Packet			
" Source Ir	Source Interface:	inside 🔹 👻	Destination Interface:	outside 👻
"Network Ol	Source Address:	10.1.2.0-inside_network	Destination Address:	10.1.1.0-remote_networ
			Service:	any
	Action: Translated Packet			
	Source NAT Type:	Static 👻		
	Source Address:	10.1.2.0-inside_network -	Destination Address:	10.1.1.0-remote_networ
	Use one-to-one address transla	tion		
	PAT Pool Translated Address:		Service:	Original
	Round Robin			
	Extend PAT uniqueness to pe	er destination instead of per int	erface	
	Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-1023	3
	Eall through to interface PAT			
	Use IPv6 for source interface P	AT	Use IPv6 for destin	ation interface PAT
	Options			
	🔽 Enable rule			
	Translate DNS replies that mate	h this rule		
	Disable Proxy ARP on egress inl	terface		
	Lookup route table to locate eg	ress interface		
	Direction: Both 👻			
		OK Cancel	Help	

Remote-ASA (Peer dinâmico)

1. Escolha Assistentes > Assistentes VPN > Assistente de VPN Site a Site assim que o aplicativo ASDM se conectar ao

ASA. Cisco ASDM 7.1 for	ASA - 1	0.105.130.220		-	-		_
File View Tools	Wizards	Window Help					
Home 😪 Conf	Sta	rtup Wizard		Ba	ack 👩 Forward 🛛	Help	
Deuise List	VP	N Wizards	F		Site-to-site VPN Wit	zard	
Add Delete	Hig	gh Availability and Scalability Wiza	rd		AnyConnect VPN W	∕izard	
A AUG Celete	Uni	ified Communication Wizard			Clientless SSL VPN	Wizard	
Find:	Pac	:ket Capture Wizard			IPsec (IKEv1) Remot	te Access VPN Wiza	ird
			Gener	alL	icense		
- 3 10.105.130.54			Host	Nam	e: 121-neer		
- 10.105.130.72			ASA	Versi	on: 9.1(3)	Device Uptime:	2d 1h 42m 5(
■ 10.105.130.89 ■ 10.105.130.105			ASD	M Ver	sion: 7.1(4)	Device Type:	ASA 5520
2. Clique em							

Next.



 Escolha fora da lista suspensa VPN Access Interface para especificar o endereço IP externo do peer remoto. Selecione a interface (WAN) em que o mapa de criptografia é aplicado. Clique em

teps	Peer Device Identificati	on	
1. Introduction	This step lets you ident	ify the peer VPN device by its IP address and the interface used to access the peer	
2. Peer Device Identification	Peer IP Address:	172.16.2.1	
3. Traffic to protect			
4. Security	VPN Access Interface:	outside 👻	
5. NAT Exempt			
6. Summary			

4. Especifique os hosts/redes que devem ter permissão para passar pelo túnel VPN. Nesta etapa, você precisa fornecer as redes locais e as redes remotas para o túnel VPN. Clique nos botões ao lado dos campos Rede local e Rede remota e escolha o endereço conforme o requisito. Clique em Avançar quando

terminar.

Site-to-site VPN Connection	Setup Wizard
Steps	Traffic to protect
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you identify the local network and remote network between which the traffic is to be protected using IPsec encryption IP Address Type: ID:1.1.0/24 ID:1.1.0/24 ID:1.2.0/24
	< Back Next >

5. Insira as informações de autenticação a serem usadas, que é a chave pré-compartilhada neste exemplo. A chave pré-compartilhada usada neste exemplo é cisco123. O nome do grupo de túnel é o endereço IP do peer remoto por padrão se você configurar a VPN LAN-to-LAN

iteps	Security
Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary	This step lets you secure the selected traffic. Simple Configuration ASA uses the pre-shared key entered here to authenticate this device with the peer. ASDM will select common IKE and ISAKMP security parameters for that will allow tunnel establishment. It is recommended that this option is also selected when configuring the remote peer. Pre-shared Key: Customized Configuration You can use pre-shared key or digital certificate for authentication with the peer device. You can also fine tune the data encryption algorithms ASDM selected for you.

OUVocê pode personalizar a configuração para incluir a política IKE e IPsec de sua escolha. Deve haver pelo menos uma política correspondente entre os correspondentes:Na guia Métodos de autenticação, insira a chave pré-compartilhada IKE versão 1 no campo Chave pré-compartilhada. Neste exemplo, é **cisco123**.

eps	Security				
. Introduction	This step lets you secure the selected traffic.				
Peer Device Identificatio					
. Traffic to protect	Simple Configuration				
. Security	ASA uses the pre-shared key entered here that will allow burned establishment. It is re-	to authenticate this device with	the peer. ASDM will select	common IKE and ISAKMP securit	ty parameters fo
NAT Exempt	Under wire datum von mich eine auf die ferenzen die fer	contributed under und oppoints de	so selected when contriguin	g ure remote peer.	
Summary					
	Customized Configuration				
	You can use pre-shared key or digital certifi	icate for authentication with the	peer device. You can also	fine tune the data encryption al	gorithms ASDM
	selected for you.				
	IKE Version Authentication Method	Is Encryption Algorithms Pe	rfect Forward Secrecy		
	IXE version 1				
	Pre-shared Key:	•••••			
	Device Certificate:	None	•	Manage	
	IXE version 2				
	I ocal Pre-shared Key:				
	Cocarrie analogica				
	Local Device Certificate:	None		Manage	
	Local Device Certificate:	None	Ţ	Manage	
	Coal Perior Interesting Coal Device Certificate: Remote Peer Pre-shared Key:	None	v	Manage	
	Coal Perior Interesting Coal Device Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	- None	v	Manage	
	Coal Perior Interesting Coal Perior Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None	v	Manage	
	Coal Program Control (Control of Control of	None	¥	Manage Manage	
	Coal Province Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None	¥	Manage Manage	
	Cocal Province Certificate: Remote Peer Pre-shared Key: Remote Peer Certificate Authentication:	None	¥	Manage	

Clique na guia Encryption Algorithms (Algoritmos de criptografia).

 Clique em Gerenciar ao lado do campo Diretiva IKE, clique em Adicionar e configure uma política IKE personalizada (fase-1). Clique em OK quando terminar.



7. Clique em Selecionar ao lado do campo Proposta de IPsec e selecione a Proposta de IPsec

desejada. Clique em **Avançar** quando terminar.

Site-to-site VPN Connection	n Setup Wizard			
Steps	Security			
 Introduction Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	This step lets you secure the select Simple Configuration ASA uses the pre-shared key ent ISAKMP security parameters for t when configuring the remote pee Customized Configuration You can use pre-shared key or di data encryption algorithms ASDM IKE Version Authenticati	ed traffic. ered here to authenticate this device of hat will allow tunnel establishment. It i r. gital certificate for authentication with selected for you.	with the peer. ASDM will sele is recommended that this opt the peer device. You can al Perfect Forward Secrecy	oct common IKE and tion is also selected so fine tune the
	IKE version 1			
	IKE Policy: pre-share-ae	s-256-sha		Manage
	IPsec Proposal: ESP-AES-256	-SHA		Select
	IKE version 2			
	IKE Policy: aes-256-sha-	sha		Manage
	IPsec Proposal: AES256, AES	192, AES, 3DES, DES		Select
	< Back Next >			Cancel Help

Opcionalmente, você pode ir até a guia Perfect Forward Secsecret e marcar a caixa de seleção **Enable Perfect Forward Secsecret (PFS)**. Clique em **Avançar** quando terminar.



8. Marque a caixa de seleção Isentar host/rede do lado ASA da conversão de endereço para

impedir o tráfego do túnel do início da Conversão de endereço de rede. Escolha **local ou interno** na lista suspensa para definir a interface onde a rede local pode ser alcançada. Clique em

Next.

teps	NAT Exempt
1. Introduction	This step allows you to exempt the local network addresses from network translation.
 Peer Device Identificatio Traffic to protect Security NAT Exempt Summary 	Exempt ASA side host/network from address translation inside -

9. O ASDM exibe um resumo da VPN recém-configurada. Verifique e clique em **Concluir**.



Configuração de CLI

Configuração do ASA central (peer estático)

 Configure uma regra NO-NAT/ NAT-EXEMPT para tráfego VPN como mostrado neste exemplo:

object network 10.1.1.0-remote_network subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-inside_network subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.2.0-inside_network 10.1.2.0-inside_network
destination static 10.1.1.0-remote_network 10.1.1.0-remote_network
no-proxy-arp route-lookup

2. Configure a chave pré-compartilhada em DefaultL2LGroup para autenticar qualquer peer

Dynamic-L2L remoto:

tunnel-group DefaultL2LGroup ipsec-attributes
 ikev1 pre-shared-key cisco123

3. Defina a política de fase 2/ISAKMP:

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

4. Defina o conjunto de transformações da fase 2/política de IPsec:

crypto ipsec ikev1 transform-set tset esp-aes-256 esp-sha-hmac

5. Configure o mapa dinâmico com estes parâmetros: Conjunto de transformação necessárioHabilitar RRP (Reverse Route Inject, injeção de rota reversa), que permite que o Security Appliance aprenda informações de roteamento para clientes conectados (Opcional) crypto dynamic-map outside_dyn_map 1 set ikev1 transform-set tset crypto dynamic-map outside_dyn_map 1 set reverse-route

 Vincule o mapa dinâmico ao mapa de criptografia, aplique o mapa de criptografia e ative ISAKMP/IKEv1 na interface externa:

crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map

crypto map outside_map interface outside crypto ikev1 enable outside

Remote-ASA (Peer dinâmico)

 Configure uma regra de isenção de NAT para tráfego VPN: object network 10.1.1.0-inside_network subnet 10.1.1.0 255.255.255.0

object network 10.1.2.0-remote_network subnet 10.1.2.0 255.255.255.0

nat (inside,outside) source static 10.1.1.0-inside_network 10.1.1.0-inside_network
destination static 10.1.2.0-remote_network 10.1.2.0-remote_network
no-proxy-arp route-lookup

2. Configure um grupo de túneis para um par de VPN estático e chave pré-compartilhada.

tunnel-group 172.16.2.1 type ipsec-121 tunnel-group 172.16.2.1 ipsec-attributes ikev1 pre-shared-key cisco123

3. Defina a política de FASE-1/ISAKMP:

```
crypto ikev1 policy 10
authentication pre-share
encryption aes-256
hash sha
group 2
lifetime 86400
```

- 4. Defina um conjunto de transformação da fase 2/política de IPsec: crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
- 5. Configure uma lista de acesso que defina o tráfego/rede de VPN interessante: access-list outside_cryptomap extended permit ip object 10.1.1.0-inside_network object 10.1.2.0-remote_network
- 6. Configure o mapa de criptografia estático com estes parâmetros: Crypto/VPN accesslistEndereço IP do peer IPsec remotoConjunto de transformação necessário crypto map outside_map 1 match address outside_cryptomap crypto map outside_map 1 set peer 172.16.2.1 crypto map outside_map 1 set ikev1 transform-set ESP-AES-256-SHA
- 7. Aplique o mapa de criptografia e ative ISAKMP/IKEv1 na interface externa: crypto map outside_map interface outside crypto ikev1 enable outside

Verificar

Use esta seção para confirmar se a configuração funciona corretamente.

A <u>ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns</u> <u>comandos de exibição.</u>. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

 show crypto isakmp sa - Exibe todas as Associações de Segurança IKE (SAs) atuais em um peer. • show crypto ipsec sa - Exibe todas as SAs IPsec atuais.

Esta seção mostra um exemplo de saída de verificação para os dois ASAs.

ASA central

```
Central-ASA#show crypto isakmp sa
 IKEv1 SAs:
    Active SA: 1
   Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
    IKE Peer: 172.16.1.1
 1
                            Role : responder
    Type : L2L
   Rekey : no
                            State : MM_ACTIVE
    Central-ASA# show crypto ipsec sa
interface: outside
   Crypto map tag: outside_dyn_map, seq num: 1, local addr: 172.16.2.1
        local ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
      current_peer: 172.16.1.1
        #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0
       local crypto endpt.: 172.16.2.1/0, remote crypto endpt.: 172.16.1.1/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 30D071C0
      current inbound spi : 38DA6E51
      inbound esp sas:
      spi: 0x38DA6E51 (953839185)
         transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (3914999/28588)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x0000000 0x000001F
   outbound esp sas:
      spi: 0x30D071C0 (818966976)
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 28672, crypto-map: outside_dyn_map
        sa timing: remaining key lifetime (kB/sec): (3914999/28588)
         IV size: 16 bytes
         replay detection support: Y
```

ASA remoto

Remote-ASA#show crypto isakmp sa IKEv1 SAs: Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 IKE Peer: **172.16.2.1** : L2L Role Tvpe : initiator Rekey : no State : MM_ACTIVE Remote-ASA#show crypto ipsec sa interface: outside Crypto map tag: **outside_map**, seq num: 1, local addr: 172.16.1.1 access-list outside_cryptomap extended permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0 local ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.1.2.0/255.255.255.0/0/0) current_peer: 172.16.2.1 #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #TFC rcvd: 0, #TFC sent: 0 #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.16.2.1/0 path mtu 1500, ipsec overhead 74(44), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: 38DA6E51 current inbound spi : 30D071C0 inbound esp sas: spi: 0x30D071C0 (818966976) transform: esp-aes-256 esp-sha-hmac no compression in use settings ={L2L, Tunnel, IKEv1, } slot: 0, conn_id: 8192, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4373999/28676) IV size: 16 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x000001F outbound esp sas: spi: 0x38DA6E51 (953839185) transform: esp-aes-256 esp-sha-hmac no compression in use settings ={L2L, Tunnel, IKEv1, } slot: 0, conn_id: 8192, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4373999/28676) IV size: 16 bytes

```
replay detection support: Y
Anti replay bitmap:
    0x00000000 0x00000001
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

A <u>ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns</u> <u>comandos de exibição.</u>. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Note: Consulte <u>Informações Importantes sobre Comandos de Depuração antes de usar</u> <u>comandos</u> debug.

Use estes comandos da forma mostrada:

clear crypto ikev1 sa <peer IP address> Clears the Phase 1 SA for a specific peer.

Caution: O comando clear crypto isakmp sa é invasivo, pois limpa todos os túneis VPN ativos.

No software PIX/ASA versão 8.0(3) e posterior, um SA IKE individual pode ser limpo usando o comando clear crypto isakmp sa *<peer ip address>*. Nas versões de software anteriores à 8.0(3), use o comando <u>vpn-sessiondb logoff tunnel-group *<tunnel-group-name>* para limpar SAs de IKE e IPsec para um único túnel.</u>

Remote-ASA#**vpn-sessiondb logoff tunnel-group 172.16.2.1** Do you want to logoff the VPN session(s)? [confirm] INFO: Number of sessions from TunnelGroup "172.16.2.1" logged off : 1

clear crypto ipsec sa peer <peer IP address>
!!! Clears the required Phase 2 SA for specific peer.
debug crypto condition peer < Peer address>
!!! Set IPsec/ISAKMP debug filters.
debug crypto isakmp sa <debug level>
!!! Provides debug details of ISAKMP SA negotiation.
debug crypto ipsec sa <debug level>
!!! Provides debug details of IPsec SA negotiations
undebug all
!!! To stop the debugs

Depurações usadas:

debug cry condition peer <remote peer public IP> debug cry ikev1 127 debug cry ipsec 127

Remote-ASA (iniciador)

Insira este comando packet-tracer para iniciar o túnel:

```
Remote-ASA#packet-tracer input inside icmp 10.1.1.10 8 0 10.1.2.10 detailed
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1 DEBUG]Pitcher: received a key acquire message, spi 0x0
IPSEC(crypto_map_check)-3: Looking for crypto map matching 5-tuple:
Prot=1, saddr=10.1.1.10, sport=0, daddr=10.1.2.10, dport=0
IPSEC(crypto_map_check)-3: Checking crypto map outside_map 1: matched.
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE Initiator: New Phase 1, Intf
inside, IKE Peer 172.16.2.1 local Proxy Address 10.1.1.0, remote Proxy Address
10.1.2.0, Crypto map (outside_map)
:
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0)
total length : 132
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
<skipped>...
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message (msgid=0) with
payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) + VENDOR (13) +
NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Automatic NAT Detection Status: Remote end is NOT behind a NAT device
This end is NOT behind a NAT device
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128)
+ VENDOR (13) + NONE (0) total length : 96
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR ID received 172.16.2.1
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, Connection landed on tunnel_group 172.16.2.1
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1,
Oakley begin guick mode
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1, PHASE 1 COMPLETED
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1, IKE Initiator
starting QM: msg id = c45c7b30
:
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, Transmitting Proxy Id:
Local subnet: 10.1.1.0 mask 255.255.255.0 Protocol 0 Port 0
Remote subnet: 10.1.2.0 Mask 255.255.255.0 Protocol 0 Port 0
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE
(10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
```

```
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE RECEIVED Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) +
ID (5) + ID (5) + NONE (0) total length : 172
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID IPV4 ADDR SUBNET ID received--10.1.1.0--255.255.255.0
Jan 19 22:00:06 [IKEv1 DEBUG]Group = 172.16.2.1, IP = 172.16.2.1, processing ID payload
Jan 19 22:00:06 [IKEv1 DECODE]Group = 172.16.2.1, IP = 172.16.2.1,
ID_IPV4_ADDR_SUBNET ID received--10.1.2.0--255.255.255.0
•
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
Security negotiation complete for LAN-to-LAN Group (172.16.2.1)
Initiator, Inbound SPI = 0x30d071c0, Outbound SPI = 0x38da6e51
Jan 19 22:00:06 [IKEv1]IP = 172.16.2.1, IKE_DECODE SENDING Message
(msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 76
Jan 19 22:00:06 [IKEv1]Group = 172.16.2.1, IP = 172.16.2.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
```

Central-ASA (respondedor)

```
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + NONE (0) total length : 172
:
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length
132
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304
:
Jan 20 12:42:35 [IKEv1] IP = 172.16.1.1, Connection landed on tunnel group
DefaultL2LGroup
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Generating keys for Responder...
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) +
VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) +
NONE (0) total length : 304
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8)
+ IOS KEEPALIVE (128) + VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1 DECODE]Group = DefaultL2LGroup, IP = 172.16.1.1,
ID_IPV4_ADDR ID received172.16.1.1
:
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (128) +
VENDOR (13) + NONE (0) total length : 96
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, PHASE 1 COMPLETED
:
```

```
Jan 20 12:42:35 [IKEv1 DECODE]IP = 172.16.1.1, IKE Responder starting QM:
msg id = c45c7b30
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE
RECEIVED Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + SA (1) +
NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Received remote
IP Proxy Subnet data in ID Payload: Address 10.1.1.0, Mask 255.255.255.0,
Protocol 0, Port 0:
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup,
IP = 172.16.1.1, Received local
IP Proxy Subnet data in ID Payload: Address 10.1.2.0, Mask 255.255.255.0,
Protocol 0, Port 0Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup,
IP = 172.16.1.1, processing notify payload
Jan 20 12:42:35 [IKEv1] Group = DefaultL2LGroup, IP = 172.16.1.1, QM
IsRekeyed old sa not found by addr
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Static Crypto Map
check, map outside_dyn_map, seq = 1 is a successful match
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, IKE
Remote Peer configured for crypto map: outside_dyn_map
:
Jan 20 12:42:35 [IKEv1 DEBUG]Group = DefaultL2LGroup, IP = 172.16.1.1,
Transmitting Proxy Id: Remote subnet: 10.1.1.0 Mask 255.255.255.0 Protocol 0 Port 0
Local subnet: 10.1.2.0 mask 255.255.255.0 Protocol 0 Port 0:
Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE SENDING Message (msgid=c45c7b30)
with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE
(0) total length : 172 Jan 20 12:42:35 [IKEv1]IP = 172.16.1.1, IKE_DECODE RECEIVED
Message (msgid=c45c7b30) with payloads : HDR + HASH (8) + NONE (0) total length : 52:
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Security
negotiation complete for LAN-to-LAN Group (DefaultL2LGroup) Responder,
Inbound SPI = 0x38da6e51, Outbound SPI = 0x30d071c0:
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1,
PHASE 2 COMPLETED (msgid=c45c7b30)
Jan 20 12:42:35 [IKEv1]Group = DefaultL2LGroup, IP = 172.16.1.1, Adding static
```

route for L2L peer coming in on a dynamic map. address: 10.1.1.0, mask: 255.255.255.0

Informações Relacionadas

- <u>Referências de comandos do Cisco ASA Series</u>
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Solicitações de Comentários (RFCs)
- <u>Suporte técnico e documentação Cisco System</u>