Configurar o túnel VPN de gerenciamento do AnyConnect no ASA

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Funcionamento do túnel de gerenciamento Limitações Configurar Configuração no ASA através do ASDM/CLI Criação do perfil de VPN de gerenciamento do AnyConnect Métodos de implantação para o perfil de VPN de gerenciamento do AnyConnect (Opcional) Configure um Atributo Personalizado para Suportar a Configuração Tunnel-AII Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve como configurar um ASA quando o gateway VPN aceita conexões do Cisco AnyConnect Secure Mobility Client através do túnel VPN de gerenciamento.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN através do Adaptive Security Device Manager (ASDM)
- Configuração CLI do ASA (Basic Adaptive Security Appliance)
- Certificados X509

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco ASA versão 9.12(3)9
- Software Cisco ASDM versão 7.12.2
- Windows 10 com Cisco AnyConnect Secure Mobility Client versão 4.8.03036

Observação: faça download do pacote de implantação Web do AnyConnect VPN (anyconnect-

win*.pkg or anyconnect-macos*.pkg) no <u>Download de Software da</u> Cisco (somente clientes registrados). Copie o AnyConnect VPN Client para a memória flash do ASA que deve ser baixada para os computadores de usuários remotos para estabelecer a conexão VPN SSL com o ASA. Consulte a seção <u>Instalação do AnyConnect Client</u> do guia de configuração do ASA para obter mais informações.

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Um túnel VPN de gerenciamento garante a conectividade com a rede corporativa sempre que o sistema cliente é ligado, não apenas quando uma conexão VPN é estabelecida pelo usuário final. Você pode executar o gerenciamento de patches em endpoints fora do escritório, especialmente em dispositivos que raramente são conectados pelo usuário, via VPN, à rede do escritório. Os scripts de login de SO de endpoint que exigem conectividade de rede corporativa também se beneficiam desse recurso.

O túnel de gerenciamento do AnyConnect permite que os administradores conectem o AnyConnect sem intervenção do usuário antes de quando o usuário faz login. O túnel de gerenciamento do AnyConnect pode funcionar em conjunto com a Detecção de rede confiável e, portanto, é acionado somente quando o endpoint está fora do local e desconectado de uma VPN iniciada pelo usuário. O túnel de gerenciamento do AnyConnect é transparente para o usuário final e se desconecta automaticamente quando o usuário inicia a VPN.

SO/aplicativo ASA ASDM Versão do Windows AnyConnect Versão do AnyConnect para MacOS Linux Requisitos mínimos de versão 9.0.1 7.10.1 4.7.00136 4.7.01076 Sem suporte

Funcionamento do túnel de gerenciamento

O serviço AnyConnect VPN Agent é iniciado automaticamente na inicialização do sistema. Ele detecta que o recurso de túnel de gerenciamento está habilitado (através do perfil VPN de gerenciamento), portanto, inicia a aplicação cliente de gerenciamento para iniciar uma conexão de túnel de gerenciamento. O aplicativo cliente de gerenciamento usa a entrada de host do perfil de VPN de gerenciamento para iniciar a conexão. Em seguida, o túnel VPN é estabelecido como de costume, com uma exceção: nenhuma atualização de software é executada durante uma conexão de túnel de gerenciamento, já que o túnel de gerenciamento deve ser transparente para o usuário.

O usuário inicia um túnel VPN por meio da interface do usuário do AnyConnect, que aciona a terminação do túnel de gerenciamento. No término do túnel de gerenciamento, o estabelecimento do túnel do usuário continua como de costume.

O usuário desconecta o túnel VPN, o que aciona o restabelecimento automático do túnel de gerenciamento.

Limitações

- Não há suporte para interação do usuário
- Somente há suporte para autenticação baseada em certificado por meio do Repositório de Certificados de Computador (Windows)
- A verificação estrita do certificado do servidor é imposta
- Não há suporte para um proxy privado
- Não há suporte para um proxy público (o valor ProxyNative tem suporte em plataformas nas quais as configurações de Proxy Nativo não são recuperadas do navegador)
- Scripts de personalização do AnyConnect não são suportados

Observação: para obter mais informações, consulte Sobre o Túnel VPN de Gerenciamento.

Configurar

Esta seção descreve como configurar o Cisco ASA como o gateway VPN para aceitar conexões de clientes AnyConnect através do túnel VPN de gerenciamento.

Configuração no ASA através do ASDM/CLI

Etapa 1. Crie a política de grupo do AnyConnect. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Clique em Add.

Observação: é aconselhável criar uma nova Política de grupo do AnyConnect que é usada apenas para o túnel de gerenciamento do AnyConnect.



Etapa 2. Fornecer uma Name para a Política de Grupo. Atribuir/Criar um Address Pool.

Escolher Tunneling Protocols como SSL VPN Client e/ou IPsec IKEv2, conforme mostrado na imagem.

Servers	Name: AnyConnect_MGMT_	Tunnel		_
Advanced	Banner: 🗹 Inherit			
	SCEP forwarding URL: 🔽 Inherit	_		
	Address Pools: Inherit VPN_Po	ool		Select
	IPv6 Address Pools: 🗹 Inherit			Select
	More Options			
	Tunneling Protocols:	Inherit	Clientless SSL VPN Client IPsec IKEv1 IPsec IKEv2 L2TP/	IPsec
	Filter:	🗹 Inherit		Manage
	Access Hours:	🗹 Inherit		Manage
	Simultaneous Logins:	🗹 Inherit		
	Restrict access to VLAN:	🗹 Inherit		2
	Connection Profile (Tunnel Group) Lock:	🗹 Inherit		
	Maximum Connect Time:	🗹 Inherit	Unlimited minutes	
	Idle Timeout:	🗹 Inherit	None minutes	
	Security Group Tag (SGT):	🗹 Inherit	None (2 - 65519)	
	On smart card removal:	Inherit	Disconnect Keep the connection	
	Timeout Alerts	_		
	Maximum Connect Time Alert Interval:	🔽 Inherit	Default minutes	
	Periodic Certificate Authentication Interval	: 🗹 Inherit	Unlimited hours	
et. d.	Next	Previous		

Etapa 3. Navegue até Advanced > Split Tunneling. Configurar o Policy como Tunnel Network List Below e escolha a opção Network List, conforme mostrado na imagem.

• • •		Edit Internal G	roup Policy: AnyConnect_MGMT_	lunnel	
General Servers	The VPN client makes split tunneling de fields.	cisions on the	basis of a network list that can	be specified below by providing the proper parameters to 'Policy' and	d 'Networl
Split Tunneling	DNS Names:	🗹 Inherit			
Browser Proxy ► AnyConnect Client ► IPrec(/(Srl)) Client	Send All DNS Lookups Through Tunnel:	Inherit	🔿 Yes 💿 No		
P IFSec(IKEV1) Client	Policy:	Inherit	Tunnel Network List Below	S	
	IPv6 Policy:	🗹 Inherit		\$	
	Network List:	Inherit	VPN-Split	3	Manag
•	Pressing this button to set up split extur Set up Split Exclusion for Web Securi Intercept DHCP Configuration Message	sion for Web S ty	ecurity proxies. ft Clients		
	c				
Find:	Next 🥥	Previous			
		Help	Cancel OK	1	

Observação: se um endereço de cliente não for enviado para ambos os protocolos IP (IPv4 e IPv6), o Client Bypass Protocol configuração deve ser enabled para que o tráfego correspondente não seja interrompido pelo túnel de gerenciamento. Para configurar o,

Etapa 4. Navegue até Advanced > AnyConnect Client. Configurado Client Bypass Protocol para Enable. Clique em OK para Salvar, como mostrado na imagem.

• •		Add Internal Group Policy	
General	Keep Installer on Client System:	V Inherit 🔿 Yes 💿 No	
Servers Advanced	Datagram Transport Layer Security (DTLS):	🗹 Inherit 🔿 Enable 🔿 Disable	
Split Tunneling	DTLS Compression:	🗹 Inherit 🔿 Enable 🔿 Disable	
Browser Proxy AnyConnect Client	SSL Compression:	☑ Inherit O Deflate O LZS O Disable	
IPsec(IKEv1) Client	Ignore Don't Fragment(DF) Bit:	🗹 Inherit 🕜 Enable 🖉 Disable	
	Client Bypass Protocol:	Inherit O Enable Disable	
	FQDN of This Device:	V FQDN	
	MTU:	🗹 Inherit	
	Keepalive Messages:	✓ Inherit	Ш
	Optional Client Modules to Download:	☑ Inherit	
	Always-On VPN:	☑ Inherit O Disable O Use AnyConnect Profile setting ●	Ш
	Client Profiles to Download:	🗹 Inherit	
		Add 1 Delete	
		Profile Name Profile Usage/Type	
			ш
			ш
			ш
Find:	Next	Previous	5
		Help Cancel OK	

Etapa 5. Como mostrado nesta imagem, clique em Apply para enviar a configuração para o ASA.

🔥 н	ome 🔩 Configuration 👩 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	rard ? Help Type topic Go		cisco
	O O Remote Access VPN	○ ○ ○ Configuration > Remote Acc	cess VPN > Network (Client) Acc	ess > Group Policies	
marks	Pintroduction Network (Client) Access AnyConnect Connection Profiles AnyConnect Customization/Localizati AnyConnect Client Profile AnyConnect Client Software Doment Access Policient	Manage VPN group policies.A VPN g policy information is referenced by To enforce authorization attributes Add r C Edit Delete As	roup is a collection of user-orient VPN connection profiles and user from an LDAP server you must use sign	ed authorization attribute/value pairs that may be stored in accounts. an LDAP attribute map.	nternally on the device or externally on a RADIUS/LDAP server. The group
ook	Croup Policies	Name	Type	Tunneling Protocol	Assigned To
60 []]]	IPsec(IKEv1) Connection Profiles	AnyConnect	Internal	ssi-client	AnyConnect
	IPsec(IKEv2) Connection Profiles	And Connect MGMT Tunnel	Internal	ikev2;ikev2;i2tp-ipsec ikev2;ssl-client	Am/Connect_MGMT_Turnel
	Secure Mobility Solution	serveonneee_meant_runner	mema	DOCKET, 331-SITCH	Putyconnect_wown_runeer
	Address Assignment Address Assignment Address Assignment Address Assignment Address Assignment Address SSL VPN Access Address SSL VPN Access Address SSL VPN Access Address SSL VPN Access Address Assignment Address Add				
1	Device Setup				
	Firewall Kemote Access VPN				
	Site-to-Site VPN	Find:	Match Case		
	Device Management			Reset Apply	

Configuração CLI para Diretiva de Grupo:

```
ip local pool VPN_Pool 192.168.10.1-192.168.10.100 mask 255.255.255.0
! access-list VPN-Split standard permit 172.16.0.0 255.255.0.0
! group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-network-list value VPN-Split
client-bypass-protocol enable
address-pools value VPN_Pool
```

Etapa 6. Crie o perfil de conexão do AnyConnect. Navegue até Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profile. Clique em Add.

Nota: É aconselhável criar um novo Perfil de conexão do AnyConnect que é usado somente para o túnel de gerenciamento do AnyConnect.



Passo 7. Fornecer uma Name para o Perfil de Conexão e defina Authentication Method COMO Certificate only. Escolha o Group Policy COMO o criado na Etapa 1.

Basic Advanced	Name:	AnyConnect_MGMT_Tunnel		
Auvanceu	Aliases:			
	Authentication			
	Method:	Certificate only		
	AAA Server Group:	LOCAL	0	Manage
		Use LOCAL if Server Group fails		
	SAML Identity Provider			
	SAML Server :	None	0	Manage
	Client Address Assignmen	t		
	DHCP Servers:	-		
		• None OHCP Link OHCP Subnet		
	Client Address Pools:			Select
	Client IPv6 Address Pool	s:		Select
	Default Group Policy			
	Group Policy:	AnyConnect_MGMT_Tunnel	0	Manage
	(Following fields are link	ed to attribute of the group policy selected above.)		
	🗹 Enable SSL VPN cli	ient protocol		
	C Enable IPsec(IKEv2	?) client protocol		
	DNS Servers:			
	WINS Servers:			
	Domain Name:			
Find:		Next OPrevious		

Observação: verifique se o certificado raiz da CA local está presente no ASA. Navegue até Configuration > Remote Access VPN > Certificate Management > CA Certificates para adicionar/exibir o certificado.

Observação: verifique se um certificado de Identidade emitido pela mesma CA Local existe no Repositório de Certificados do Computador (para Windows) e/ou no Conjunto de Chaves do Sistema (para macOS).

Etapa 8. Navegue até Advanced > Group Alias/Group URL. Clique em Add sob Group URLs e adicionar um URL. Garantir Enabled está marcado. Clique em OK para Salvar, como mostrado na imagem. Add AnyConnect Connection Profile

Basic Advanced General Client Addressing Authentication Secondary Authentication Authorization Accounting Group Alias/Group URL	 Enable the display of Radius Reject-Message on the login screen when authentication is rejected Enable the display of Securld messages on the login screen Connection Aliases This SSL VPN access method will present a list of aliases configured for all connection profiles. You r the Login Page Setting in the main panel to complete the configuration. Add Pelete (The table is in-line editable.) Alias
	Group URLs This SSL VPN access method will automatically select the connection profile, without the need for use Add Delete (The table is in-line editable.) • URL Enabled Add Group URL URL: https://asa.example.com/AnyConnect_MGMT_Tunnel Cancel OK
Find:	Next Previous Help Cancel OK

Se IKEv2 for usado, verifique IPsec (IKEv2) Access está ativado na interface usada para o AnyConnect.

○ ○ ○ Remote Access VPN	O O Config	uration > Remot	e Access VPN > I	Network (Client) A	Access > AnyConnect Co	nnection Profiles
Introduction Network (Client) Access AnyConnect Connection Profiles	The security Client suppo	appliance automa orts IPsec (IKEv2) to	tically deploys th unnel as well as St	e Cisco AnyConnee 5L tunnel with Data	ct VPN Client to remote us agram Transport Layer Sec	sers upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN unity (DTLS) tunneling options.
AnyConnect Customization/Local AnyConnect Client Profile AnyConnect Client Software	Enable C	ces lisco AnyConnect nust be enabled if	VPN Client access	on the interfaces	selected in the table belo	w Web Launch) .
Dynamic Access Policies Group Policies Policies Psec(IKEv1) Connection Profiles	Interface	SSL Access Allow Access	Enable DTLS	IPsec (IKEv2) Acco Allow Access	Enable Client Services	Device Certificate
 IPsec(IKEv2) Connection Profiles Secure Mobility Solution Address Assignment 	inside			Ö		Port Settings

Etapa 9. Clique em Apply para enviar a configuração para o ASA.



Configuração CLI para perfil de conexão (grupo de túneis):

```
tunnel-group AnyConnect_MGMT_Tunnel type remote-access
tunnel-group AnyConnect_MGMT_Tunnel general-attributes
default-group-policy AnyConnect_MGMT_Tunnel
tunnel-group AnyConnect_MGMT_Tunnel webvpn-attributes
authentication certificate
group-url https://asa.example.com/AnyConnect_MGMT_Tunnel enable
```

Etapa 10. Verifique se um certificado confiável está instalado no ASA e associado à interface usada para conexões do AnyConnect. Navegue até Configuration > Remote Access VPN > Advanced > SSL Settings para adicionar/exibir essa configuração.

Observação: consulte Instalação do Certificado de Identidade no ASA.

Remote Access VPN	○ ○ ○ Configuration > Remote Acces	s VPN > Advanced > SSL Settings				
Introduction	r					
Network (Client) Access	Configure SSL parameters. These para	meters affect both ASDM and SSL VPN acc	ess.			
AnyConnect Customization AnyConnect Client Profile	The minimum SSL version for the second	urity appliance to negotiate as a "server":	TLS V1	0	O DTLSV1 O DTLSV1.2	
AnyConnect Client Softwar	The minimum SSL version for the second	urity appliance to negotiate as a "client":	TLS V1	0		
Group Policies	Diffie-Hellman group to be used with	SSL:	Group2 - 1024-bit modulus	0		
IPsec(IKEv1) Connection P IPsec(IKEv2) Connection P	ECDH group to be used with SSL:		Group19 - 256-bit EC	0		
Secure Mobility Solution	Encryption					
Sp Address Assignment	cheryption				10.00.001	
Advanced	Cipher version	Cipher Security Level		Cipher Algorithm	s/ custom string	Edit
Clientless SSL VPN Access	Default	Medium		DES-CBC3-SHA	AES128-SHA DHE-KSA-AES128-SHA AES256-SHA DHE-KSA	
AAA/Local Users	TLSV1	Medium		DHE-RSA-AESZS	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
AAA Server Grouns	TLSV1.1	Medium		DHE-RSA-AESZ	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
Se LDAR Ancibude Man	TLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
	DTLSV1	Medium		DHE-RSA-AES2	6-SHA AES256-SHA DHE-RSA-AES128-SHA AES128-SHA	
I Local Users	DTLSV1.2	Medium		ECDHE-ECDSA-	AES256-GCM-SHA384 ECDHE-RSA-AES256-GCM-SHA384 D	
Secure Desktop Manager						
Certificate Management						
Language Localization						
Load Balancing						
DHCP Server	Server Name Indication (SNI)					
DNS	Domain		Certificate			Add
Advanced						
Connection Gateway						Edit
Reference Identity						Delete
Certificate to AnyConnect						
HTTP Redirect						
Maximum VPN Sessions						
Crypto Engine						
	Certificates					
	Specify which contificator if any of	ould be used for SSL authentication on ea	ch interface. The fallback contificate u	uill be used on interfs	car not prescipted with a cartificate of their own	
	specify which certificates, if any, si	iouid be used for SSL authentication on ea	ich interface. The fanback certificate v	vill be used on interra	ces not associated with a certificate of their own.	
under Cature	Interface	Primary Certificate	Load Balancing Certificate		Key-Type	Edit
evice Setup	inside					
innuall	management					
ineman.	outside	ROOT-CA:hostname=ASA.example	.co		Primary: RSA (2048 bits), Load Balancing: none	
emote Access VPN						
ite-to-Site VPN						
Device Management						
			(Charles) (Charles			

Configuração CLI para Ponto de Confiança SSL:

ssl trust-point ROOT-CA outside

Criação do perfil de VPN de gerenciamento do AnyConnect

Etapa 1. Crie o perfil do AnyConnect Client. Navegue até Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile. Clique em Add,conforme mostrado na imagem.

	Home 🍕 Configuration 📴 Monitorir	ng 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forw	vard 💡 Help Type topic Go			cisco
	O O O Remote Access VPN	○ ○ ○ Configuration > Remote Access VP	PN > Network (Client) Access > AnyCor	nnect Client Profile		
ookmarks	Pintroduction Pintroduction Pintroduction AnyConnect Connection Profil Bintroduction Profile AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Strokare Bintroduction Profile Dynamic Access Policies Connect Belging	This panel is used to manage AnyConnect button to add a new profile. Pressing the In The profile Usage field is introduced with t HostScan configuration can be performed I	Client Profiles and perform group assign port or Export button is for upload and the Secure Mobility Solution. This field co by going to Secure Desktop Manager/Hor	ment for AnyConnect version 2.5 or later. You can select a pro download of client profiles between local machine and device ntains different profile usage in AnyConnect version 3.0 and I stScan. If 'HostScan' is not visible under 'Secure Desktop Mana	ile to edit, change group or to delete. You can select the 'Add' ater. ger', you will need to restart ASDM.	
	IPsec(KEv1) Connection Profil	a trade a second a second a second a second a				
		Profile Name	Profile Usage	Croup Policy	Profile Location	
	Reference identity Certificate to AnyConnect and HTTP Redirect Maximum VPN Sessions Crypto Engine			Reset Apply		

Etapa 2. Fornecer uma Profile Name. Escolha o Profile Usage como AnyConnect Management VPN profile. Escolha o Group Policy criado na <u>Etapa 1</u>. Clique em OK ,conforme mostrado na imagem.

rofile Name		Profile Usage	Group Policy		Profile Location
	• • •	Add AnyConnect Clien	t Profile		
	Profile Name	AnyConnect_MGMT_Profile			
	Profile Usage	AnyConnect Management VPN Profile	O		
	Enter a device f created if it do	file path for an xml file, ie. disk0:/ac_profile. The fi es not exist.	le will be automatically		
	Profile Location	n disk0:/anyconnect_mgmt_profile.vpnm	Br	owse Flash	
				Upload	
	Group Policy	AnyConnect_MGMT_Tunnel			
	_	Enable 'Always On VPN' for selected group			
		Help Cancel	ОК		
			Reset Apply		

Etapa 3. Escolha o perfil criado e clique em Edit, conforme mostrado na imagem.

file Name	Profile Usage	Group Policy	Profile Location
/Connect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm

Etapa 4. Navegue até Server List. Clique em Add para adicionar uma nova Entrada da Lista de Servidores, como mostrado na imagem.

Preferences (Part 1)	Server List				
Preferences (Part 2)					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins
Certificate Matching					
List					
				I.	
	Note: at most o	ne server can be define	d in a management VP	N profile. Add	Delete
			j		
				Edit	Details

Etapa 5. Fornecer uma Display Name. Adicione o comando FQDN/IP address do ASA. Forneça o User Group como o nome do grupo do túnel. Group URL é preenchido automaticamente com O FQDN e User Group. Clique em OK.

Server	Certificate Pinning
Primary Server Display Name (required) AnyConnect_MGMT_Tunnel FQDN or IP Addr User Group (required) asa.example.com / AnyConnect_MGMT. Group URL asa.example.com/AnyConnect_MGMT_Tunnel	Connection Information Primary Protocol SSL 📀 ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect 🗘 IKE Identity (IOS gateway only)
Backup Servers	
Host Address	Add
	Move Up Move Down Delete
ОК	Cancel

Observação: o FQDN/endereço IP + grupo de usuários deve ser o mesmo que o URL do grupo mencionado durante a configuração do Perfil de conexão do AnyConnect na <u>Etapa 8</u>.

Observação: o AnyConnect com IKEv2 como protocolo também pode ser usado para estabelecer a VPN de gerenciamento para o ASA. Garantir Primary Protocol está definido como IPsec na Etapa 5.

Etapa 6. Como mostrado na imagem, clique em ок para Salvar.

8 🕘 🖶	AnyCo	nnect Client Profile Edit	or - AnyConnect_MGMT	_Profile		
Profile: AnyConnect_MG	MT_Profile					About
VPN	Server List					
Backup Servers	Hostname	Host Address	User Group	Backup Server List	Certificate Pins	
Certificate Matching	Anyconnect_MGMT_	i asa.example.com		innenteu	-	
	Note: at most one	server can be defined	in a management VPN p	orofile. Add	Delete	
				Edit	Details	
		Help	ncel OK			
		Ca				

Passo 7. Clique em Apply tPara enviar a configuração para o ASA, como mostrado na imagem.

đ	Home 🦓 Configuration [Monito	ring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Fo	orward 💡 Help Type topic Go			cisco
	O O Remote Access VPN	○ ○ ○ Configuration > Remote Access	VPN > Network (Client) Access > AnyConnect Cl	ient Profile		
ž.	Introduction					
okmarks	Network (Client) Access AnyConnect Connection Profil SAnyConnect Customization/Lc AnyConnect Client Profile AnyConnect Client Software Dynamic Network Deliving	This panel is used to manage AnyConnec button to add a new profile. Pressing the The profile Usage field is introduced with HostScan configuration can be performe	ct Client Profiles and perform group assignment for Import or Export button is for upload and downloa h the Secure Mobility Solution. This field contains d d by going to Secure Desktop Manager/HostScan. II	AnyConnect version 2.5 or later.You can select a prof d of client profiles between local machine and device. ifferent profile usage in AnyConnect version 3.0 and i "HostScan" is not visible under 'Secure Desktop Mana	ile to edit, change group or to delete. You can select the 'Add' ater. ger', you will need to restart ASDM.	
8	Group Bolicies	Add 12 Edit 22 Change Group Policy	Delete Tilmoort 🖪 Export 🖓 Validate			
-	IPrac(IKEv1) Connection Profil	· Add B Earl 22 Change Group Foncy	Delete minport ap Export ap valuate			
	IPsec(KEv2) Connection Profil	Profile Name	Profile Usage	Group Policy	Profile Location	
	Serure Mobility Solution	AnyConnect_MGMT_Profile	AnyConnect Management VPN Profile	AnyConnect_MGMT_Tunnel	disk0:/anyconnect_mgmt_profile.vpnm	
	Address Assignment					
	Advanced					
	Clientless SSL VPN Access					
	🔻 🚅 AAA/Local Users					
	AAA Server Groups					
	Sa LDAP Attribute Map					
	🐨 Local Users					
	Secure Desktop Manager					
	En Certificate Management					
	Language Localization					
	Sector Balancing					
	DHCP Server					
	a DNS					
	* Es Advanced					
	Connection Gateway					
	Reference Identify					
	Certificate to AmConnect and					
	HTTP Redirect					
	Maximum VPN Sessions					
	Crypto Engine					
	B Davies Setur					
	Device Secup					
	Firewall					
	Remote Access VPN					
	Site-to-Site VPN					
	Device Management					
	\$			Reset Apply		

Configuração da CLI após a adição do Perfil de VPN de gerenciamento do AnyConnect.

```
webvpn
enable outside
hsts
 enable
 max-age 31536000
 include-sub-domains
 no preload
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
anyconnect enable
tunnel-group-list enable
cache
 disable
error-recovery disable
1
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-network-list value VPN-Split
client-bypass-protocol enable
address-pools value VPN_Pool
webvpn
 anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Perfil de VPN de gerenciamento do AnyConnect no computador cliente do AnyConnect:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<UseStartBeforeLogon UserControllable="false">false"/useStartBeforeLogon>
```

<ShowPreConnectMessage>false</ShowPreConnectMessage>

```
<ProxySettings>IgnoreProxy</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
```

--- Output Omitted ---

```
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>false</AllowManualHostInput> </ClientInitialization>
```

</AnyConnectProfile>

Observação: se a TND (Trusted Network Detection, detecção de rede confiável) for usada no perfil de VPN do AnyConnect do usuário, é aconselhável corresponder as mesmas configurações no perfil de VPN de gerenciamento para uma experiência de usuário consistente. O túnel VPN de gerenciamento é acionado com base nas configurações TND aplicadas ao perfil de túnel VPN do usuário. Além disso, a ação TND Connect no perfil de VPN de gerenciamento (aplicada somente quando o túnel VPN de gerenciamento está ativo), sempre se aplica ao túnel VPN do usuário, para garantir que o túnel VPN de gerenciamento seja transparente para o usuário final.

Observação: em qualquer PC de usuário final, se o perfil de VPN de gerenciamento tiver as configurações de TND habilitadas e se o perfil de VPN do usuário estiver ausente, ele considerará as configurações de preferências padrão para o TND (ele está desabilitado nas preferências padrão na aplicação de cliente AC) em vez do perfil de VPN do usuário ausente. Essa incompatibilidade pode levar a um comportamento inesperado/indefinido. Por padrão, as configurações de TND são desabilitadas nas preferências padrão. Para superar as configurações codificadas de preferências padrão no aplicativo AnyConnect Client, o PC do usuário final deve ter dois perfis de VPN, um perfil de VPN do usuário e um perfil de VPN de gerenciamento de CA, e ambos devem ter as mesmas configurações de TND.

A lógica por trás da conexão e desconexão do túnel VPN de gerenciamento é que para estabelecer um túnel VPN de gerenciamento, o agente AC usa as configurações TND do perfil VPN do usuário e para desconexão do túnel VPN de gerenciamento, ele verifica as configurações TND do perfil VPN de gerenciamento.

Métodos de implantação para o perfil de VPN de gerenciamento do AnyConnect

• Uma conexão VPN de usuário bem-sucedida é concluída com o Perfil de conexão ASA para fazer o download do Perfil de VPN de gerenciamento do AnyConnect do Gateway VPN.

Nota: se o protocolo usado para o túnel VPN de gerenciamento for IKEv2, a primeira conexão será necessária através de SSL (para baixar o perfil de VPN de gerenciamento do AnyConnect do ASA).

 O Perfil de VPN de gerenciamento do AnyConnect pode ser carregado manualmente para as máquinas cliente por meio de um envio de GPO ou por instalação manual (Verifique se o nome do perfil é VpnMgmtTunProfile.xml).

Local da pasta onde o perfil precisa ser adicionado: Windows: C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun MacOS: /opt/cisco/anyconnect/profile/mgmttun/

(Opcional) Configure um Atributo Personalizado para Suportar a Configuração Tunnel-All

O túnel VPN de gerenciamento requer uma divisão que inclui configuração de tunelamento, por padrão, para evitar um impacto na comunicação de rede iniciada pelo usuário. Isso pode ser substituído quando você configura o atributo personalizado na política de grupo usada pela

conexão de túnel de gerenciamento.

Etapa 1. Navegue atéConfiguration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes. Clique em Add,conforme mostrado na imagem.

1	Home 🍓 Configuration 📴 Monitoring	🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help Type topic Go	cisco
	O O Remote Access VPN	Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes	
3	2 Introduction	Declarations of custom attribute types and these attributes are enforced in AppConnect group policy. AppConnect dynamic access policy and AppConnect custom attribute names	
Ś	Network (Client) Access	becomment of custom attribute types and these attributes are emotion in <u>anyconnect group pointy</u> , anyconnect dynamic access pointy and <u>anyconnect dynamics</u>	
å	AnyConnect Connection Profiles		
	AnyConnect Customization/Localizati	Add E Edit Delete	
	AnyConnect Client Profile	Type Description	
s	AnyConnect Client Software		
Ξ.	Dynamic Access Policies		
8	Group Policies		
	IPsec(IKEv1) Connection Profiles		
	IPsec(IKEv2) Connection Profiles		
	Secure Mobility Solution		
	Address Assignment		
	Advanced		
	AnyConnect Essentials		
	AnyConnect Custom Attributes		
	AnyConnect Custom Attribute Nar		
	▶ 🎼 IPsec		
	Manager Science Action		
	Clientless SSL VPN Access		
	AAA/Local Users		
	AAA Server Groups		
	LDAP Attribute Map		
	👩 Local Users		
	Secure Desktop Manager		
	Certificate Management		
	Language Localization		
	Load Balancing		
	P DHCP Server		
	and DNS		
	Advanced		
	0		
	Bevice Setup		
	Eirewall		
	and the second		
	Remote Access VPN		
	CA Site-to-Site VPM		
	Sile-to-sile vrid		_
	Device Management		
		Reset Apply	
	:		

Etapa 2. Defina o Tipo de atributo personalizado como ManagementTunnelAllAllowed e fornecer uma Description. Clique em OK, conforme mostrado na imagem.

			De	cription		
	C	create Custom Attr	ribute Type			
•••	C	Preate Custom Attr	ribute Type			
• • • Type:	ManagementTunne	Create Custom Attr	ribute Type			
Type:	(ManagementTunne ManagementTunne	Create Custom Att	ribute Type			
Type: Descriptio	C ManagementTunne ManagementTunne n:	Create Custom Att elAllAllowed elAllAllowed	ribute Type			
Type: Description	ManagementTunne ManagementTunne n:	Create Custom Att elAllAllowed	ribute Type			
Type: Description	ManagementTunne ManagementTunne n:	Create Custom Att elAllAllowed ElAllAllowed	ribute Type			

Etapa 3. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names. Clique em Add, conforme mostrado na imagem.



Etapa 4. Escolha o Tipo como ManagementTunnelAllAllowed . Defina o nome como true. Clique em Addpara fornecer um valor de atributo personalizado, como mostrado na imagem.

me Values		
	Create Custom Attribute Nan	ne
Type:	ManagementTunnelAllAllowed	ᅌ Manage
Name:	true	
	Value	Add
		Edit
		Delete
Configure Values:		
5		

Etapa 5. Definir o valor como true. Clique em ok, conforme mostrado na imagem.

Type:	ManagementTunnelAllAllowed		\$	Manage
Name:	true			
	Value		Add	
•		Add Value	- U.	
true				
(-)				
arue:				

Etapa 6. Navegue até Configuration > Remote Access VPN > Network (Client) Access > Group Policies. Escolha a Diretiva de Grupo. Clique em Edit ,conforme mostrado na imagem.

🚮 Home 🦓 Configuration 📴 Monitoring 🏾	🔜 Save 🔇 Refresh 🔇 Back 🔘 Fo	rward 💡 Help Type topic Go			cisco
000 Remote Access VPN	Configuration > Remote A	ccess VPN > Network (Client) A	ccess > Group Policies		
Pinroduction Introduction Network (Client) Access Access Acconect Connection Profiles SnyConnect Client Profile AryConnect Client Profile AryConnect Client Profile	Manage VPN group policies A VPN server. The group policy informati To enforce authorization attribute Add & Edit Delete	group is a collection of user-ori on is referenced by VPN connecti s from an LDAP server you must Assign	ented authorization attribute/value pairs that ma on profiles and user accounts. use an <u>LDAP attribute map</u> .	y be stored internally on the device or externally on a RADI	JS/LDAP
Dynamic Access Policies	Name	Туре	Tunneling Protocol	Connection Profiles/Users	
S Group Policies	Am/Connect	Internal	ssl_client	Assigned to	
IPsec(IKEv1) Connection Profiles	DfltGrpPolicy (System Default)	Internal	ikev1:ikev2:l2tp-ipsec	Default8AGroup:Default121Group:DefaultADMIN	Group Def
IPsec(IKEv2) Connection Profiles	AnyConnect MGMT Tunnel	Internal	ikev2:ssl-client	AnyConnect MGMT Tunnel	oroup;oenn
Address Assignment Address Assignment Address Assignment Advanced AnyConnect Essentials AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attributes AnyConnect Custom Attributes Advanced AnyConnect Custom AnyConnect Custom Advanced Advanced Advanced					
Bevice Setup					
Site-to-Site VPN	Find	Match Case			
Device Management			Reset Apply		

Passo 7. Como mostrado nesta imagem, navegue até Advanced > Split Tunneling. Configure a política como Tunnel All Networks.

• •		Edit Interr	nal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers	The VPN client makes split tunneling de fields.	cisions on the	e basis of a network list that can be specified below by providing the proper parameters to 'Policy' a	nd 'Network Li:
 Advanced Split Tunneling 	DNS Names:	🗹 Inherit		
Browser Proxy AnyConnect Client	Send All DNS Lookups Through Tunnel:	Inherit	Ves ONO	
IPsec(IKEv1) Client	Policy:	🗌 Inherit	Tunnel All Networks	
	IPv6 Policy:	🗹 Inherit	0	
	Network List:	🗹 Inherit	0	Manage
	Pressing this button to set up split exlu Set up Split Exclusion for Web Securi	sion for Web S ty	Security proxies.	
Find:	Next	Previous		
			Help Cancel OK	

Etapa 8. Navegue até Advanced > Anyconnect Client > Custom Attributes. Clique em Add, conforme mostrado na imagem.

• •	Edit Internal Group Policy: AnyConnect_MGMT_Tunnel	
General Servers ▼ Advanced Split Tunneling Browser Proxy ▼ AnyConnect Client Login Setting Client Firewall Key Regeneration Dead Peer Detection Customization Custom Attributes ► IPsec(IKEv1) Client	Configuration of custom policy attributes. Image: Configuration of custom policy attributes. Type Name of Value	
Find:	Next Previous	
	Help Cancel OK	

Etapa 9. Escolha o tipo de Atributo como ManagementTunnelAllAllowed e escolha o Valor como true. Clique em ok,conforme mostrado na imagem.

2		Name of V	alue
	• • •	Create Custom Attribute	
	Attribute type:	ManagementTunnelAllAllowed	Manage
	Omit the value		
	Select Value:	true	Manage
		Help Capcel OK	

Etapa 10. Clique em Apply para enviar a configuração para o ASA, como mostrado na imagem.

1	Home 🦓 Configuration 📴 Monitoring 🔚	Save 🔇 Refresh 🔇 Back 🔘 Forw	ard ? Help Type topic Go			diala
	O O Remote Access VPN	○ ○ ○ Configuration > Remote Acc	ess VPN > Network (Client) Acces	s > Group Policies		
kmarks Device List	Introduction Metwork (Clent) Access AnyConnect Connection Profiles AnyConnect Customization/Jocalizati AnyConnect Client Profile AnyConnect Client Profile AnyConnect Client Software An	Manage VPN group policies.A VPN g policy information is referenced by V To enforce authorization attributes f Add C C Edit Delete As	roup is a collection of user-orientee VPN connection profiles and user ac from an LDAP server you must use a sign	authorization attribute/value pairs that may be stored i counts. In LDAP attribute map. Tunneling Protocol	nternally on the device or externally on a RADIUS/LDAP server. The group	,
800	Group Policies	AmConnect	Internal	schelient	Assigned to	_
	IPsec(IKEv1) Connection Profiles	DftGroPolicy (System Default)	Internal	ikev1:ikev2:l2tp=insec	DefaultRAGroup: DefaultL2LGroup: DefaultADMINGroup: Defa	dtWE.
	Psec(IKEv2) Connection Profiles	AnyConnect_MGMT_Tunnel	Internal	ikev2:ssl-client	AnyConnect_MGMT_Tunnel	
	Address Assignment Control of the set of th					
	Site-to-Site VPN	Find:	Match Case			
	Device Management			Reset Apply		

Configuração da CLI após o comando ManagementTunnelAllAllowed Atributo Personalizado é adicionado:

enable outside

 $\verb+anyconnect-custom-attr ManagementTunnelAllAllowed description ManagementTunnelAllAllowed hsts$

```
max-age 31536000
 include-sub-domains
 no preload
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.8.02045-webdeploy-k9.pkg 1
anyconnect profiles AnyConnect_MGMT_Profile disk0:/anyconnect_mgmt_profile.vpnm
anyconnect enable
tunnel-group-list enable
cache
 disable
error-recovery disable
Ţ
anyconnect-custom-data ManagementTunnelAllAllowed true true
1
group-policy AnyConnect_MGMT_Tunnel internal
group-policy AnyConnect_MGMT_Tunnel attributes
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelall
client-bypass-protocol enable
address-pools value VPN_Pool
anyconnect-custom ManagementTunnelAllAllowed value true
webvpn
 anyconnect profiles value AnyConnect_MGMT_Profile type vpn-mgmt
```

Verificar

ASA# show vpn-sessiondb detail anyconnect

Verifique a conexão do túnel VPN de gerenciamento no ASA CLI com o comando show vpn-sessiondb detail anyconnect comando.

```
Session Type: AnyConnect Detailed
Username
           : vpnuser
                                    Index
                                                : 10
Assigned IP : 192.168.10.1
                                   Public IP : 10.65.84.175
            : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
License
            : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-
256
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Hashing
Bytes Tx
           : 17238
                                    Bytes Rx : 1988
           : 12
                                    Pkts Rx
                                                : 13
Pkts Tx
Pkts Tx Drop : 0
                                    Pkts Rx Drop : 0
Group Policy : AnyConnect_MGMT_Tunnel Tunnel Group : AnyConnect_MGMT_Tunnel
Login Time : 01:23:55 UTC Tue Apr 14 2020
          : 0h:11m:36s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                    VLAN
                                                : none
Audt Sess ID : c0a801010000a0005e9510ab
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
--- Output Omitted ---
DTLS-Tunnel:
 Tunnel ID
             : 10.3
 Assigned IP : 192.168.10.1
                                     Public IP : 10.65.84.175
 Encryption : AES-GCM-256
                                      Hashing
                                                  : SHA384
```

Ciphersuite :	ECDHE-ECDSA-AES256-GCM	I-SHA384	
Encapsulation:	DTLSv1.2	UDP Src Port :	57053
UDP Dst Port :	443	Auth Mode :	Certificate
Idle Time Out:	30 Minutes	Idle TO Left :	18 Minutes
Client OS :	Windows		
Client Type :	DTLS VPN Client		
Client Ver :	Cisco AnyConnect VPN A	gent for Windows	4.8.03036
Bytes Tx :	17238	Bytes Rx	: 1988
Pkts Tx :	12	Pkts Rx	: 13
Pkts Tx Drop :	0	Pkts Rx Dro	op : 0

Verifique a conexão do túnel VPN de gerenciamento no ASDM.

Navegue para **Monitoring > VPN > VPN Statistics > Sessions** . Filtre por **AnyConnect Client** para ver a sessão do cliente.

축 Home 🦓 Configuration [M	onitoring 🔒 Save (🔇 Refresh 🔇 Ba	ck 🔘 Forward 💡	Help Type topic	Go					cisco
Device List Bookmarks	OOO Monitoring	> VPN > VPN Stati	istics > Sessions							
O O O Device List										
Add 🚺 Delete 🔊 Connect	Туре	Active		Cumulative		Peak Concurrer	it	Inactive	í.	
ind: Go	AnyConnect Client		1		1	.9		1		0
A 10.106.39.196	SSL/TLS/DTLS		1		1	.9		1		0
10.106.64.230										
10.197.227.47										
10.106.51.99:444										
OO VPN										
VPN Statistics	Filter By AnyCo	onnect Client	🗧 All S	essions 😒		Filt	er			
Sessions		Group Policy	Assigned IP Address	Protocol		Login Time	Bytes Tx	1		Details
Comto Statistics	Username	Connection Profile	Public IP Address	Encryption		Duration	Bytes Ra	Inactivity	Audit :	Details
Compression Statistics	vpnuser	AnyConnect_MGMT.	192.168.10.1	AnyConnect-Parer	nt	10:52:25 UTC	34688	0h:00m:00s	c0a80	Logout
Encryption Statistics		panyconnect_mom1.		Anyconnect-Parer	nt. (1)none	00.010.315	55954			Logout
Global IKE/IPsec Statistics										Ping
Protocol Statistics										
VLAN Mapping Sessions										
E Clientless SSL VPN										
🛃 Shared SSL VPN										
VPN Connection Graphs										
WSA Sessions										
Interfaces										
CH VPN										
	To sort VPN sessio	ns, right-click on th	he above table and s	elect Table Sort Ord	der from pop	up menu.				
Routing			in and in a second s							
S Properties	Logout By: /	All Sessio ᅌ		Logout Sessions						

Verificação da conexão do túnel VPN de gerenciamento na máquina cliente:

Sisco AnyConnect Secure Mobil	ity Client	- 🗆 X	
cisco AnyCon	nect Secure Mobility Clie	ent	
Virtual Private Network (VPI	۷)	Diagnostics	
Preferences Statistics Route Detail	ls Firewall Message History		
Connection Information State: Tunnel Mode (IPv4):	Disconnected Not Available	Cisco AnyConnect Secure Mobility Client –	×
Dynamic Tunnel Exclusion: Dynamic Tunnel Inclusion: Duration: Session Disconnect: Management Connection State:	Not Available Not Available 00:00:00 None Connected (asa.example.com)	VPN: Ready to connect.	nect
Address Information			
Client (IPv4): Client (IPv6): Server:	Not Available Not Available Not Available	\$ (i)	uluulu cisco
Bytes		· ·	
	Reset	Export Stats	

Troubleshoot

A nova linha de estatísticas da interface do usuário (Estado da conexão de gerenciamento) pode ser usada para solucionar problemas de conectividade do túnel de gerenciamento. Estes são os estados de erro comumente vistos:

Desconectado (desabilitado):

- O recurso está desabilitado.
- Certifique-se de que o perfil de VPN de gerenciamento foi implantado no cliente, através da conexão de túnel do usuário (requer que você adicione o perfil de VPN de gerenciamento à política de grupo de túnel do usuário) ou fora da banda através do upload manual do perfil.
- Verifique se o perfil de VPN de gerenciamento está configurado com uma única entrada de host que inclua um grupo de túneis.

Desconectado (rede confiável):

• O TND detectou uma rede confiável, portanto, o túnel de gerenciamento não foi estabelecido.

Desconectado (túnel do usuário ativo):

• Um túnel VPN de usuário está ativo no momento.

Desconectado (falha na inicialização do processo):

• Uma falha de inicialização de processo foi encontrada quando houve uma tentativa de conexão do túnel de gerenciamento.

Desconectado (falha na conexão):

- Uma falha de conexão foi encontrada quando o túnel de gerenciamento foi estabelecido.
- Verifique se a autenticação de certificado está configurada no grupo de túneis, se não há nenhum banner presente na política de grupo e se o certificado do servidor deve ser confiável.

Desconectado (configuração de VPN inválida):

- Uma configuração inválida de separação de túneis foi recebida do servidor VPN.
- Verifique a configuração do tunelamento dividido na política de grupo de túneis de gerenciamento.

Desconectado (atualização de software pendente):

• Uma atualização de software do AnyConnect está pendente.

Desconectado:

• O túnel de gerenciamento está prestes a ser estabelecido ou não pode ser estabelecido por alguma outra razão.

Colete o DART para solucionar problemas.

Informações Relacionadas

- <u>Configuração do túnel VPN de gerenciamento</u>
- Troubleshooting de Túnel VPN de Gerenciamento
- <u>Suporte Técnico e Documentação Cisco Systems</u>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.