ASA/PIX: IP Estático que endereça para o cliente do IPSec VPN com CLI e exemplo da configuração ASDM

Índice

Introdução Pré-requisitos Requisitos Componentes Utilizados **Produtos Relacionados Convenções** Configurar Diagrama de Rede Configurar o acesso remoto VPN (o IPsec) Configuração do ASA/PIX com a CLI Configuração de Cisco VPN Client Verificar comandos show Troubleshooting Cancele associações de segurança Comandos para Troubleshooting Informações Relacionadas

Introdução

Este documento descreve como configurar a ferramenta de segurança adaptável do Cisco 5500 Series (ASA) para fornecer o endereço IP estático ao cliente VPN o Security Device Manager adaptável (ASDM) ou o CLI. O ASDM oferece gerenciamento de segurança de nível mundial e monitoramento através de uma interface de gerenciamento baseada na Web intuitiva e fácil de usar. Uma vez que a configuração ASA Cisco está completa, pode-se verificar com o Cisco VPN Client.

Refira <u>PIX/ASA 7.x e Cisco VPN Client 4.x com exemplo da configuração de autenticação do</u> <u>RAIO de Windows 2003 IAS (contra o diretório ativo)</u> a fim estabelecer a conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500. O usuário de cliente VPN remoto autentica contra o diretório ativo com um servidor Radius do Internet Authentication Service de Microsoft Windows 2003 (IAS).

Refira <u>PIX/ASA 7.x e Cisco VPN Client 4.x para o exemplo da configuração de autenticação do</u> <u>Cisco Secure ACS</u> a fim estabelecer uma conexão VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e a ferramenta de segurança 7.x da série PIX 500 com um Serviço de controle de acesso Cisco Secure (versão de ACS 3.2) para a autenticação extendida (XAUTH).

Pré-requisitos

Requisitos

Este documento supõe que o ASA é plenamente operacional e configurado para permitir que Cisco ASDM ou CLI faça alterações de configuração.

Nota: Refira <u>permitir o acesso HTTPS para ASDM</u> ou <u>PIX/ASA 7.x: SSH no exemplo de</u> <u>configuração da interface interna e externa</u> para permitir que o dispositivo seja configurado remotamente pelo ASDM ou pelo Shell Seguro (ssh).

Componentes Utilizados

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

- Versão de software adaptável 7.x da ferramenta de segurança de Cisco e mais tarde
- Versão 5.x e mais recente adaptável do Security Device Manager
- Versão Cliente VPN Cisco 4.x e mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão 7.x e mais recente da ferramenta de segurança de Cisco PIX.

Convenções

Consulte as <u>Convenções de Dicas Técnicas da Cisco</u> para obter mais informações sobre convenções de documentos.

<u>Configurar</u>

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918, que foram usados em um ambiente de laboratório.

Configurar o acesso remoto VPN (o IPsec)

Procedimento ASDM

Termine estas etapas a fim configurar o acesso remoto VPN:

 Escolha a configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > das políticas de IKE a fim criar uma política de ISAKMP.

Gisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards Window Help					
🔥 Home 🗞 Configuration 😥 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🤗 Help					
Remote Access D 4 × ? Introduction Network (Client) Access AnyConnect Connection IPsec Connection Profile Group Policies Opnamic Access Policie Address Assignment Advanced Advanced SSL VPN SSL VPN IPsec	Configuration > Remote Access VPN > Network (Client) Access > Advance Configure specific Internet Key Exchange (IKE) algorithms and parameters, within the Add Edit Delete Priority # Encryption Hash				
Fornaça os datalhas da pali	ítica do				

2. Forneça os detalhes da política de ISAKMP.

🗲 Add IKE Polic	у			
Priority:	2	Authentication:	pre-share 🗸	
Encryption:	des 💌	D-H Group:	2 🗸	
Hash:	sha 💌	Lifetime:	 Unlimited 86400 	seconds 💌
	<u> </u>	Cancel	Help	

Clique a **APROVAÇÃO** e **aplique-a**.

 Escolha a configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > IPsec > parâmetros IKE para permitir o IKE na interface
 externa

externa.					
🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards Window Help					
😚 Home 😘 Configuration 📴 Monitoring 🔚 Save 🐼 Refresh 🚫 Back 🚫 Forward 🦻 Help					
Remote Access P × Introduction Network (Client) Access AnyConnect Connection Psec Connection Profile Group Policies Connection Profile Address Assignment Address Assignment Address Assignment Address Assignment Address Assignment Address Assignment Address Assignment Figure Endpoint Security Figure SSL VPN Figure Policies NE Policies Figure Policies	Interface IKE Enable Interface IKE Enable Inside No Outside Yes Interface IKE Enable Enable INE Enable Inside No Oisable Enable IPsec over NAT-T NAT Keepalive: 20 Seconds Enable IPsec over TCP Enable IPsec over TCP Enable IPsec over TCP Interface IC 65535): IO000 IO000				
Prec. Transform Prec. Transform Prec. Prefragme Prec. Prefragme Upload Software Prec. Transform Prec. Prefragme Prefragme Prec. Prefragme Pre	Identity: Automa Key Id String: Disable inbound aggressive mode connections				
Clientless SSL VPN Access AAA/Local Users Access Science Desktop Manager Certificate Manager	Alert peers before disconnecting Wait for all active sessions to voluntarily terminate before rebooting				

4. Escolha a configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > IPsec > IPsec transformam o > Add dos grupos a fim criar o ESP-DES-SHA transformam o grupo, como mostrado.

🖆 Add Transform Set 🛛 🛛 🔀	
Set Name: ESP-DES-SHA	
Properties	
Mode: 💿 Tunnel 🚫 Transport	
ESP Encryption: DES	
ESP Authentication:	
OK Cancel Help	
	Clique

APROVAÇÃO e aplique-a.

5. Escolha a configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > dos crypto map a fim criar um crypto map com a política dinâmica da prioridade 1, como mostrado.

🖆 Create IPsec Rule	
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Selection	
Interface: outside 💙 Policy Type: dynamic 💙	Priority: 1
Transform Sets	
Transform Set to Be Added:	Move Up
Remove	Move Down
Peer Settings - Optional for Dynamic Crypto Map Entries	
The Connection Type is applicable to static tunnel policies only. Uni-directional connection for LAN-to-LAN redundancy. Tunnel policies of the 'Originate Only' connection type may redundant peers.	n type policies are used specify up to 10
OK Cancel Help	

Clique a APROVAÇÃO e aplique-a.

6. Escolha a **configuração > o acesso remoto VPN > o AAA Setup > > Add dos usuários locais** a fim criar a conta de usuário (por exemplo, username - cisco123 e senha - cisco123) para o acesso de cliente

VPN.

🖆 Add User Account			
Identity			
	Username:	cisco123	
	Password:	*****	
	Confirm Password:	****	
	User authentica	ated using MSCHAP	
	Access Restriction		
	Select one of the	options below to restrict ASDM, SSH, Teln	et and Console access.
	Note: All users ha	ave network access, regardless of these se	attings.
	 Full access(A: 	SDM, SSH, Telnet and Console)	
	Privilege le	vel is used with command authorization.	
	Privilege Le	evel: 2	
	🚫 CLI login pror	npt for SSH, Telnet and console (no ASDM	access)
	This setting	; is effective only if AAA authenticate cons	ole command is configured.
	🔿 No ASDM, SS	H, Telnet or Console access	
	This setting) is effective only if AAA authenticate cons	ole command is configured.
Find:		🔘 Next 🛛 🔘 Previous	
	(OK Cancel Help	·

7. Vá à política de VPN e adicionar o estático/dedicou o endereço IP de Um ou Mais Servidores Cisco ICM NT para o usuário "cisco123," como

segue.						
🖆 Cisco ASDM 6.1 for ASA	- 10.77	.241.111				
File View Tools Wizards W	indow H	Help				
Home 🖓 Configuration	Monitorin	g 🔚 Save 💽 Refresh	🔇 Back 🔘 Forward 🦻 Help			
Remote Access a # ×	Config	uration > Remote Access	s VPN > AAA/Local Users > Local	Users		
-? Introduction	Crea	🖆 Add User Accoun	ŧ			
AnyConnect Connection P	Corr	dentity	Check an Inherit checkbox to let th	ne correspond	ing setting take its value	from the
Group Policies Dynamic Access Policies	AAA		Group Policy:	🔽 Inherit		
Assignment Policy	Use		Tunneling Protocols:	🗹 Inherit	Clientless SSL VPN	SSL
Advanced Gentless SSL VPN Access	ena		Filter:	🗹 înherit		
AAA/Local Users			Tunnel Group Lock:	🗹 Inherit		
LDAP Attribute Map			Store Password on Client System:	🖌 Inherit	O Yes O No	
- A Secure Desktop Manager			Connection Settings			
			Access Hours:	🗹 înherit		
- 😤 Load Balancing - 😰 DHCP Server			Simultaneous Logins:	🗹 Inherit		
- Advanced			Maximum Connect Time:	🗹 Inherit	Unlimited	Minute
			Idle Timeout:	🗹 Inherit	Unlimited	Minute
			Dedicated IP Address (Optional)			
			IP Address: 192.168.5.1	Subnet Mask	: 255.255.255.0	

8. Escolha a configuração > o acesso remoto VPN > o acesso > a atribuição de endereço > os

conjuntos de endereços da rede (cliente) e o clique **adiciona** para adicionar o cliente VPN para usuários de cliente

VPN.

VI I 1					
G Cisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards Window Help					
🚓 Home 💁 Configuration 🔯 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Forward 🦻 Help					
Remote Access 🗗 🔍 👋	Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools				
Introduction Network (Client) Access AnyConnect Connection P Proceed Connection Profiles Group Policies Adverse Assignment Access Policies Adverse Assignment Policy Adverse Social A	Configure named IP Address pools. This parameter is enforced in either a VPN IPsec Connection Profiles, AnyConnect Connection Profiles or Group Policies Add E Edit Delete Pool Name Star Name: vpnclient1 Starting IP Address: 192.168.5.100 Ending IP Address: 192.168.5.100 Subnet Mask: Starting V				
Address Assignment Address Assignment Address Social	Pool Name Star Name: vpnclent1. Starting IP Address: 192.168.5.10 Ending IP Address: 192.168.5.100 Subnet Mask: 55.255.255.0 OK Cancel				

 Escolha a configuração > o acesso remoto VPN > do acesso > da conexão IPSec da rede (cliente) > Add dos perfis a fim adicionar um grupo de túneis (por exemplo, TunnelGroup1 e a chave Preshared como o cisco123), como

He Mew Tools Wizards Window He	slp		Look For:	
🔥 Home 🦓 Configuration 🔯 Monitoria	ng 🔚 Save 🔇 Refresh 🤇	🕽 Back 🔘 Forward 🦓 He	4p	
Remote Access VPN P Introduction Network (Client) Access AnyConnect Connection Profiles	Configuration > Remote Acces Access Interfaces Enable interfaces for IPsec acc	ess. <u>VPN > Hetwork (Client) Ac</u>	cess > IPsec Connection Profile	2
IPsec Connection Profiles	Interface Allow Access		cess	
Dynamic Access Policies	outside	<u> </u>		
Dep Address Assignment	amz			
🗄 🐻 Advanced	in blac			
Secure Desktop Manager Certificate Management Certificate Management Longuage Localization DHCP Server BNS	Connection Profiles Connection profile (tunnel gro	up) specifies how user is authenti	cated and other parameters.	a trafficience
Gertificate Manager Gertificate Management Gertificate Gertificat	Connection Profiles Connection profile (tunnel gro Add Z Edit 1 Oct Name DefaultWEBUENGroup	up) specifies how user is authenti etc IPsec Enabled	cated and other parameters. L2TP/IPsec Enabled	Autentication
Secure Desktop Manager Secure Desktop Manager Certificate Management Secure Decalization Load Balancing DHCP Server Secure DHCP Server Advanced	Connection Profiles Connection profile (tunnel gro Add E Edit Connection Name DefaultWEBVPNGroup DefaultRAGroup	up) specifies how user is authenti etc IPsec Enabled	cated and other parameters. L2TP/IPsec Enabled	Autentication

autenticação de usuário.Escolha **vpnclient1** como as associações do endereço de cliente para os usuários de cliente

VPN.

🐔 Home 🦓 Configuration 😰 Monitoring 🔚 Save 💽 Refresh 🕓 Back 💭 Forward 🦻 Help						
Remote Access 🗗 🔍 🗵	Configuration > Rem	ote Access VPN > Net	work (Client) Access > IPsec Connection F	rofiles		
Network (Client) Access	🌃 Add IPsec Remote	Access Connection	n Profile			
AnyConnect Connection :						
IPsec Connection Profile	295 G	Name:	TunnelGroup1			
	Advanced		romono copa			
		IKE Peer Authentication				
E-Bp Address Assignment						
Assignment Policy		Pre-shared Key:	*****			
Address Pools				_		
H-65 Advanced		Identity Certificate:	None Y	Manage		
Clientiess SSL VPN Access						
AAA/Local Users		User Authentication				
- In AAA Server Groups		Cerver Oroun:	LOCAL	Managa		
- AC DUE Map		Server Group.	LOCAL	mariage		
Secure Deckton Manager		Falback:	Use LOCAL if Server Group fails			
- Certificate Management						
- Standade Include Include		Client Address Assignme	ant			
- Se Load Balancing		Cheric Auto ess Assigning				
		DHCP Servers:				
A DNS		Client Address Rook	unaction 1	Colort		
Advanced		Citer (Multiress Publis)	vpricientz	Select		
~						
		Default Group Policy —				
		Group Policy:	DfltGrpPolicy V	Manage		
			/Following fields are attributed of the group poli	ou colocted :		
				cy selected a		
			Enable IPsec protocol			
			Enable 2TP over IPsec protocol			
			Fichable C21F over trade protocol			

Clique em **OK**.

10. Escolha avançado > endereçamento do cliente e verifique a caixa de verificação do conjunto de endereços do uso para atribuir o endereço IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN.Nota: Certifique-se desmarcar as caixas de seleção para o Authentication Server do uso e usar o DHCP.

🚔 Add IPsec Remote Access Connection Profile					
Basic Advanced General Authentication Authorization Accounting Gibbal Client Address Assignment Policy Use authentication server Use authentication Server Use address pool Interface-Specific Address Pools Add Edit Delete Interface Address Pools					
Find: 💿 Next 💿 Previous					
OK Cancel Help					

Clique em **OK**.

11. Permita a **interface externa** para o acesso do IPsec. O clique **aplica-se** para continuar.

🚰 Cisco ASDM 6.1 for ASA - 10.77.241.111					
File View Tools Wizards Window Help					
🔥 Home 🦓 Configuration 🔯 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦓 Help					
Remote Access D P × Introduction Network (Client) Access AnyConnect Connection Profiles Dynamic Access Policies Address Assignment Address Policies Address Policie	Configuration > Remote Access VPN > Access Interfaces Enable interfaces for IPsec access. Interface Allow outside allow dmz allow inside allow Connection Profiles connection profile (tunnel group) specifie	Network (Client) Access > IPsec Conne Access Access P P P P P P P P P P P P			

Configuração do ASA/PIX com a CLI

Termine estas etapas a fim configurar o servidor DHCP para fornecer endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes VPN da linha de comando. Refira <u>configurar</u> <u>referências adaptáveis do Dispositivo-comando da Segurança do 5500 Series dos acessos</u> <u>remoto VPN</u> ou do <u>Cisco ASA</u> para obter mais informações sobre de cada comando que é usado.

Configuração running no dispositivo ASA		
ASA# sh run		
ASA Version 8.0(2)		
!		
! Specify the hostname for the Security Appliance.		
hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted		
names ! ! Configure the outside and inside		
interfaces. interface Ethernet0/0 nameif inside		
security-level 100 ip address 10.1.1.1 255.255.255.0 !		
interface Ethernet0/1 nameif outside security-level 0 ip		
address 192.168.1.1 255.255.255.0 ! interface		
Ethernet0/2 nameif DMZ security-level 50 ip address		
192.168.10.2 255.255.255.0 ! Output is suppressed.		
passwd 2KFQnbNIdI.2KYOU encrypted boot system		
disk0:/asa802-k8.bin ftp mode passive access-list 101		
extended permit ip 10.1.1.0 255.255.255.0 192.168.5.0		
255.255.255.0 pager lines 24 logging enable logging asdm		
informational mtu inside 1500 mtu outside 1500 mtu dmz		
1500 ip local pool vpnclient1 192.168.5.10-192.168.5.100		
mask 255.255.255.0 no failover icmp unreachable rate-		
limit 1 burst-size 1 ! Specify the location of the		
ASDM image for ASA to fetch the image for ASDM access.		
asdm image disk0:/asdm-613.bin no asdm history enable		
arp timeout 14400 global (outside) 1 192.168.1.5 nat		
(inside) 0 access-list 101 nat (inside) 1 0.0.0.0		

0.0.0.0 route outside 0.0.0.0 0.0.0.0 192.168.1.2 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0 inside no snmp-server location no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto dynamic-map outside_dyn_map 1 set transform-set ESP-DES-SHA crypto map outside_map 1 ipsec-isakmp dynamic outside_dyn_map !--- Specifies the interface to be used with !--- the settings defined in this configuration. crypto map outside_map interface outside !--- PHASE 1 CONFIGURATION ---! !--- This configuration uses ISAKMP policy 2. !--- The configuration commands here define the Phase !--- 1 policy parameters that are used. crypto isakmp enable outside crypto isakmp policy 2 authentication pre-share encryption des hash sha group 2 lifetime 86400 no crypto isakmp nat-traversal !---Specifies that the IP address to the vpn clients are assigned by the local and not by AAA or dhcp. The CLI vpn-addr-assign local for VPN address assignment through ASA is hidden in the CLI provided by **show run** command. no vpn-addr-assign aaa no vpn-addr-assign dhcp telnet timeout 5 ssh timeout 5 console timeout 0 threatdetection basic-threat threat-detection statistics access-list ! class-map inspection default match default-inspection-traffic ! ! policy-map type inspect dns preset_dns_map parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect netbios inspect rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet inspect sunrpc inspect tftp inspect sip inspect xdmcp ! servicepolicy global_policy global ! group-policy DfltGrpPolicy attributes vpn-tunnel-protocol IPSec webvpn group-policy GroupPolicy1 internal !--- In order to identify remote access users to the Security Appliance, !--- you can also configure usernames and passwords on the device. !--- specify the IP address to assign to a particular user, use the **vpn-framed-ip-address** command !--- in username mode username cisco123 password ffIRPGpDSOJh9YLq encrypted username cisco123 attributes vpn-framed-ip-address 192.168.5.1 255.255.255.0 !---Create a new tunnel group and set the connection !--type to remote-access. tunnel-group TunnelGroup1 type remote-access tunnel-group TunnelGroup1 generalattributes address-pool vpnclient1 !--- Enter the preshared-key to configure the authentication method. tunnel-group TunnelGroup1 ipsec-attributes pre-sharedkey * prompt hostname context Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d : end ASA#

Configuração de Cisco VPN Client

Tente conectar a Cisco ASA com o Cisco VPN Client a fim verificar que o ASA está configurado com sucesso.

- 1. Escolha o Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN.
- 2. Clique novo para lançar a janela de entrada nova da conexão de VPN da



criação.

3. Preencha os detalhes de sua nova conexão.Dê entrada com o nome da entrada de conexão junto com uma descrição. Incorpore o endereço IP externo do ASA à caixa do host. Incorpore então o nome de grupo de túneis VPN (TunnelGroup1) e a senha (chave précompartilhada - cisco123) como configurado no ASA. Clique em

VPN Client Create New VPN Connect	tion Entry	X
Connection Entry: ASA		
Description: vpntunnel		ululu cisco
Host: 192.168.1.1		
Authentication Transport Backup Servers	Dial-Up	
Group Authentication	C Mutual Group	Authentication
Name: TunnelGroup1		
Password: ******		
Confirm Password: *******		
C Certificate Authentication		
Name:		
🔽 Send CA Certificate Chain		
Erase User Password	Save	Cancel

Salvar.

4. Clique a conexão que você quer usar, e o clique **conecta da** janela principal do cliente VPN.

Status: Connected VPN Client - V	ersion 5.0.03.0530	
Connection Entries Status Certificates Log	Options Help	
Connection Entries Certificates Log	Connect New Import Modify Delete	
Connection Entry	Host	Transport
🍅 ASA	192.168.1.1	IPSec/UDP
Not connected.	Co	nnected Time: 0 day(s), 00:01.18

5. Quando alertado, incorpore o **username: cisco123** e **senha: cisco123** como configurado no ASA para o Xauth, e **APROVAÇÃO do** clique a conectar à rede

The server has reque	sted the following	information to complete	the user
authentication.			
ului, Username:	cisco123		
CISCO Password:	*****		
	······		
		ОК	Can

6. O cliente VPN é conectado com o ASA na instalação central

Connection Entries Status Certificates Log Options Help Disconnect New Import Modify Delete CISCO Connection Entries Certificates Log CISCO Connection Entries Certificates Log Transport ASA 192 168 1.1 IPSec/UDP	status: Connected VPN Client - Ve	rsion 5.0.03.0530		
Import Import Modify Delete Import Import	Connection Entries Status Certificates Log	Options Help		
Connection Entries Certificates Log Connection Entry / Host Transport ASA 192 168 1.1 IPSec/UDP	Disconnect New Import Mo	n X	.네. CI	sco
Connection Entry / Host Transport	Connection Entries Certificates Log			
ASA 192 168 1 1 IPSec/UDP	Connection Entry	Host	Transport	
10E.100.1.1	🙆 ASA	192.168.1.1	IPSec/UDP	

7. Uma vez que a conexão é estabelecida com sucesso, escolha **estatísticas do** menu de status verificar os detalhes do

unei.			
🥔 status	: Connected VPN Client - Versio	n 5.0.03.0530	
Connection	Entries Status Certificates Log Optio	ns Help	
Disconne Connectio	Statistics Ctrl+S Notifications Ctrl+N n Entries Reset Stats	Delete	dhaha cisco
	Connection Entry	Host	Transport
0	ASA	192.168.1.1	IPSec/UDP

Verificar

comandos show

Use esta seção para confirmar se a sua configuração funciona corretamente.

A <u>Output Interpreter Tool</u> (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- show crypto isakmp sa Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.
- mostre IPsec cripto sa Mostra os ajustes usados por SA atuais.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração. O exemplo de debug é mostrado igualmente.

Nota: Para obter mais informações sobre do IPSec VPN do Acesso remoto do Troubleshooting consulte <u>a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos</u> <u>soluções</u>.

Cancele associações de segurança

Quando você pesquisa defeitos, certifique-se cancelar associações de segurança existentes depois que você faz uma mudança. No modo privilegiado do PIX, use estes comandos:

• clear [crypto] ipsec sa — Suprime do IPSec ativo SA. As palavras-chave crypto são

opcionais.

• clear [crypto] isakmp sa — Suprime do IKE ativo SA. As palavras-chave crypto são opcionais.

Comandos para Troubleshooting

A <u>Output Interpreter Tool</u> (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

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

- IPsec 7 do debug crypto Indica as negociações de IPSEC de fase 2.
- isakmp 7 do debug crypto Indica as negociações de ISAKMP de fase 1.

Informações Relacionadas

- Página de Suporte dos Cisco ASA 5500 Series Adaptive Security Appliances
- Referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500
- Página de Suporte dos Cisco PIX 500 Series Security Appliances
- Referência de comandos do Dispositivos de segurança Cisco PIX série 500
- <u>Cisco Adaptive Security Device Manager</u>
- Página de Suporte de Negociação IPSec/Protocolos IKE
- Página de Suporte do Cisco VPN Client
- <u>Cisco PIX Firewall Software</u>
- <u>Referências do comando Cisco Secure PIX Firewall</u>
- Avisos de campo de produto de segurança (incluindo PIX)
- <u>Solicitações de Comentários (RFCs)</u>
- Suporte Técnico e Documentação Cisco Systems