ASA/PIX: Servidor de VPN remoto com o NAT de entrada para o tráfego do cliente VPN com CLI e exemplo da configuração ASDM

Índice

Introdução Pré-requisitos Requisitos Componentes Utilizados Produtos Relacionados Convenções Informações de Apoio Configurações Configurar o ASA/PIX como um servidor de VPN remoto com ASDM Configurar o ASA/PIX como um servidor de VPN remoto e para o NAT de entrada com o CLI Configurar o ASA/PIX como um servidor de VPN remoto e para o NAT de entrada com o CLI Verificar Ferramenta de segurança ASA/PIX - comandos show Troubleshooting Informações Relacionadas

Introdução

Este documento descreve como configurar o Cisco 5500 Series Adaptive Security Appliance (ASA) para atuar como um servidor de VPN remoto usando o Adaptive Security Device Manager (ASDM) ou CLI e NAT para o tráfego de entrada do cliente VPN. 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 através do Cisco VPN Client.

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. O ASA é suposto igualmente para ser configurado para o NAT de partida. Consulte <u>para permitir o acesso dos host internos às redes</u> <u>externas com o uso da PANCADINHA</u> para obter mais informações sobre de como configurar o NAT de partida.

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.

Informações de Apoio

As configurações do Acesso remoto fornecem o Acesso remoto seguro para Cisco VPN Client, tais como usuários móvéis. Um acesso remoto VPN deixa usuários remotos firmemente alcançar recursos de rede centralizada. O Cisco VPN Client segue com o protocolo IPSec e é projetado especificamente trabalhar com a ferramenta de segurança. Contudo, a ferramenta de segurança pode estabelecer conexões IPSec com muitos clientes protocolo-complacentes. Refira <u>manuais</u> <u>de configuração ASA</u> para obter mais informações sobre do IPsec.

Os grupos e os usuários são conceitos do núcleo no Gerenciamento da Segurança dos VPN e na configuração da ferramenta de segurança. Especificam os atributos a que determine o acesso de usuários e o uso do VPN. Um grupo é uma coleção de usuários tratada como uma entidade única. Os usuários obtêm seus atributos das políticas do grupo. Os grupos de túneis identificam a política do grupo para conexões específicas. Se você não atribui uma política do grupo particular aos usuários, a política do grupo padrão para a conexão aplica-se.

Um grupo de túneis consiste em um grupo de registros que determine políticas da conexão de túnel. Estes registros identificam os server a que os usuários do túnel são autenticados, assim como os servidores de contabilidade, eventualmente, a que a informação de conexão é enviada. Igualmente identificam uma política do grupo padrão para as conexões, e contêm parâmetros de conexão do específico de protocolo. Os grupos de túneis incluem um pequeno número de atributos que se referem a criação do túnel própria. Os grupos de túneis incluem um ponteiro a uma política do grupo que defina atributos USER-orientados.

Configurações

Configurar o ASA/PIX como um servidor de VPN remoto com ASDM

Termine estas etapas a fim configurar Cisco ASA como um servidor de VPN remoto com ASDM:

 Abra seu navegador e incorpore <IP_Address de https:// da relação do ASA que foi configurado para ASDM Access> a fim alcançar o ASDM no ASA.Certifique-se autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa.O ASA apresenta este indicador para permitir a transferência do aplicativo ASDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java applet.



- 2. Clique a **launcher ASDM da transferência e comece o ASDM** a fim transferir o instalador para o aplicativo ASDM.
- 3. Uma vez as transferências da launcher ASDM, terminam as etapas dirigidas pelas alertas a fim instalar o software e executar o lançador ASDM Cisco.
- Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT para a relação que você configurou com o HTTP - comande, e um nome de usuário e senha se você especificou um.Este exemplo usa o cisco123 como o username e o cisco123 como a

	🖆 Cisco ASDM Launch	er v1.5(30)	
	🤏 Cisco AS	cisco	
	Device IP Address / Name:	10.77.241.111	v
	Username:	cisco123	
	Password:	* * * * * * *	
	📃 Run in Demo Mode		
		OK Close	
senha.			1 🕯 👙 🔒

5. Selecione assistentes > assistente do IPSec VPN do indicador

	Gisco ASDM 6.1 for ASA - 10.77.241.111							
	File View Tools		Wiz	ards	Window	Help		
	Home 2 Co		_	Startup Wizard			-	
	Device List		IPse	ec VPN Wiza	ard	N		
		S	SSL	VPN Wizaro	J	r <u>ç</u>		
		241_10		High	n Availability	y and Se	calability Wizard	
home.	10.77	.241.10		Pack	ket Capture	e Wizaro	±	

6. Selecione o tipo de túnel do **acesso remoto VPN** e assegure-se de que a interface de túnel VPN esteja ajustada como desejada, e clique-se **em seguida** como mostrado aqui.

🖆 VPN Wizard					
VPN Wizard	VPN Tunnel Type (Step 1 of)				
Branch Branch F F F F F F F F F F F F F F F F F F F	Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.				
Corporate	VPN Tunnel Type: Site-to-Site VPN				
THE HE	O Site-to-Site				
	Remote Access				
	VPN Tunnel Interface: Outside				
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.				
	< Back Next > Finish Cancel Help				

 O tipo do cliente VPN é escolhido, como mostrado. O Cisco VPN Client é escolhido aqui. Clique em Next.

🖆 VPN Wizard	
VPN Wizard	Remote Access Client (Step 2 of)
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
	VPN Client Type:
Home	Cisco VPN Client, Release 3 x or higher:
Network	or other Easy VPN Remote product
active to	
A LAN	Microsoft Windows client using L2TP over IPsec
	Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.
-	PAP V CHAP V MS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
	Specify if the client will send tunnel group name as - username@tunnelgroup.
A	Client will send tunnel group name as username@tunnelgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next > Finish Cancel Help

8. Dê entrada com um nome para o nome de grupo de túneis. Incorpore a informação da autenticação para usar-se, que é a chave pré-compartilhada neste exemplo. A chave pré-compartilhada usada neste exemplo é cisco123. O nome de grupo de túneis usado neste exemplo é Cisco. Clique em Next.

🖆 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
Branch Branch Horne Corporato Network	The ASA allows you to group remote access tunnel users based on common connection parameters and clent attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote clent. Authentication Method Pre-shared key Pre-Shared Key: Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK)
	< Back Next > Finish Cancel Help

9. Escolha se você quer usuários remotos ser autenticado à base de dados de usuário local ou a um Grupo de servidores AAA externo.Nota: Você adiciona usuários à base de dados de usuário local na etapa 10.Nota: Refira grupos de servidor da authentication e autorização PIX/ASA 7.x para usuários VPN através do exemplo da configuração ASDM para obter informações sobre de como configurar um Grupo de servidores AAA externo com ASDM.

🖆 VPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Branch Branch Branch Branch Home Home Home	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.]
	< Back Next > Finish Cancel He	łp

10. Forneça um username e a senha e o clique opcionais adicionam a fim adicionar novos usuários ao base de dados de autenticação de usuário. Clique em Next.Nota: Não remova os usuários existentes deste indicador. Selecione a configuração > o Gerenciamento de dispositivos > o Users/AAA > as contas de usuário na janela principal de ASDM para editar entradas existentes no base de dados ou para removê-las do base de dados.

🖆 VPN Wizard		×
VPN Wizard	User Accounts (Step 5 of 11)	
	Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.	
Home	User to Be Added	
Corporate Network	Username: disco123	
-14	cisco Add >>	
	Password (optional): Delete	
THI		
The state	Confirm Password (optional):	
	< Back Next > Finish Cancel Help	

11. A fim definir um pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN remotos, clique **novo** para criar um **IP pool** novo.

🖆 VPN Wizard		×
VPN Wizard	Address Pool (Step 6 of 11)	
Branch Branch Dillo Horne Notwork	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients. Tunnel Group Name : cisco	
	Pool Name:	
	- Pool Settings	
THUILIN	Range Start Address:	
T	Range End Address:	
- I - I	Subnet Mask:	
	< Back Next > Finish Cancel Help	2

12. Na nova janela intitulada adicionar o IP pool fornecem esta informação, e clicam a APROVAÇÃO.Nome do IP poolComeçando o endereço IP de Um ou Mais Servidores Cisco ICM NTTerminando o endereço IP de Um ou Mais Servidores Cisco ICM NTMáscara

E	Add IP Pool		×
	Name:	vpnpool	
	Starting IP Address:	192.168.1.1	
	Ending IP Address:	192.168.1.254	
	Subnet Mask:	255.255.255.0	~
	OK R C	ancel Help	

de sub-rede

 Depois que você define o pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN remotos quando conectam, clique em seguida.

🖆 VPN Wizard					×
VPN Wizard	Address Pool	(Step 6 of 11)			
Branch Branch Branch Branch Home	Enter a po clients.	ol of local addresses to be use	ed for assigning dynamic IF	° addresses to remote VPN	
Corporate Network		Tunnel Group Name :	cisco		
THE IN		Pool Name:	vpnpool	New	
		Pool Settings			
THUIL		Range Start Address:	192.168.1.1		
- Internet		Range End Address:	192.168.1.254		
The state		Subnet Mask:	255.255.255.0		
	L				J
			< Back Next >	Finish Cancel Help	P

14. *Opcional:* Especifique o DNS e GANHE a informação do servidor e um Domain Name do padrão a ser empurrado para clientes VPN remotos.

🖆 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional)	(Step 7 of 11)
Branch Branch	Attributes you configure below are push ASA. If you do not want an attribute pu	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate	Tunnel Group:	disco
Franks he	Primary DNS Server:	
	Secondary DNS Server:	
THE	Primary WINS Server:	
	Secondary WINS Server:	
	Default Domain Name:	
		< Back Next > Finish Cancel Help

15. Especifique os parâmetros para o IKE, igualmente conhecidos como a fase 1. IKE.As configurações em ambos os lados do túnel devem combinar exatamente. Contudo, o Cisco VPN Client seleciona automaticamente a configuração apropriada para se. Consequentemente, nenhuma configuração de IKE é necessária no PC cliente.

🖆 VPN Wizard		×
VPN Wizard	IKE Policy (Step 8 of 11)	
Branch Branch Destate Home Home	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.	
Notwork	Encryption: DES	
	Authentication:	
	Diffie-Helman Group: 2	
	< Back Next Finish Cancel Help	•

16. Este indicador mostra um sumário das ações que você tomou. Clique o **revestimento** se você é satisfeito com sua configuração.



Configurar o ASA/PIX ao tráfego do cliente VPN da entrada de NAT com ASDM

Termine estas etapas a fim configurar Cisco ASA ao tráfego do cliente VPN da entrada de NAT com ASDM:

1. Escolha a configuração > o Firewall > regras Nat, e o clique adiciona. Na lista de drop-down,



seleta adicionar a regra dinâmica NAT.

 No indicador dinâmico da regra adicionar NAT, escolha a parte externa como a relação, e clique o botão Browse ao lado da caixa da fonte.

📬 Add	Dyna	amic NAT Rule		×
Original Interl Sourc Translal Selec	face: :e: ted — t a glo	Outside	anslation.	
Poc 0 0	l ID	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Conn	ectio	n Settings		*
			OK Cancel Help	

 No indicador da fonte da consultação, selecione os objetos de rede adequada e igualmente escolha a fonte sob a seção selecionada da fonte, e clique a APROVAÇÃO. O objeto de rede de 192.168.1.0 é escolhido aqui.

🖆 Browse Source								
🗣 Add 🗹 Edit 📋	Delete	Q						
Filter:								Filter Clear
Name	^1 I	P Addres	ss	Netmask		Description		
Network Objects								
i 🥎 any	0.0	0.0.0		0.0.0.0				
inside-netw	ork 17	2.16.1.0	D	255.255.255.0)			
🖓 Outside-ne	twork 10.	.10.10.0	0	255.255.255.0)	_		
i i <u>n</u> ∎ 192.168.1.	0 193	2.168.1	.0	255.255.255.0)			
Selected Source								
Source -> 1	92.168.1	.0/24						
								-
							L _L ox	Cancel

4. O clique controla.

Original Interface: Outside Source: 192.168.0.0 Translated Select a global pool for dynamic translation. Pool ID Interface 0 (outbound) 0 (inbound) Same as original address (identity) 0 (inbound) Same as original address (identity)	🖆 Add Dyne	amic NAT Rule		
Pool ID Interface Addresses Pool 0 (outbound) Same as original address (identity) 0 (inbound) Same as original address (identity)	Original — Interface: Source: Translated — Select a glo	Outside 192.168.0.0	ranslation.	
	Pool ID 0 0	Interface (outbound) (inbound)	Addresses Pool Same as original address (identity) Same as original address (identity)	Manage
Connection Settings	Connectio	n Settings		*

5. No indicador do conjunto global do controlo, o clique

🗯 Manage Gl	obal Pool		
Add 🗹	Edit 🍿 Delete		
Pool ID	Interface	Addresses Pool	
	ОК	Cancel Help	

adiciona.

6. No indicador do conjunto de endereço global adicionar, escolha o interior como a relação e os 2 como o pool ID. Igualmente certifique-se de que o botão de rádio ao lado da PANCADINHA que usa o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação está selecionado. Clique Add>>, e clique então a APROVAÇÃO.

🞼 Add Global Address Pool		×
Interface: inside Pool ID: 2		
IP Addresses to Add		Addresses Pool
Starting IP Address:		inside
Ending IP Address: Netmask (optional):	Add >>	
O Port Address Translation (PAT)	<< Delete	
Netmask (optional):		
 Port Address Translation (PAT) using IP Address of the interface 		
ОК	Cancel	Help

 Clique a APROVAÇÃO depois que você seleciona o conjunto global com o pool ID 2 configurado na etapa precedente.

🕵 Add Dyna	amic NAT Rule		
Original			
Interface:	Outside	~	
Source:	192.168.1.0/24		
Translated — Select a glo	ibal pool for dynamic	translation.	
Pool ID	Interface	Addresses Pool	
0	(outbound)	Same as original address (identity)	
	(inbound)	Same as original address (identity)	Managa
2	Inside	inside	Manage
	- 111		
Lonnection	n Settings		۲
		Cancel Help	

8. Agora o clique **aplica-se** de modo que a configuração seja aplicada ao ASA. This termine a configuração.

Source Destination Service Interface Add Outside (1 Dynamic rules) 1 I 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	π,	Type	Original		Translat	ted
1 Image: Second Sec		туре	Source	Destination	Service Interfac	e Addr
1 Inside Inside Inside Inside (1 Exempt rules, 1 Dynamic rules) any Image: 192.168.1.0/24 (outbound) 2 Image: Dynamic any Image: 192.168.1.0/24 Outside 2 Image: Dynamic any Image: 192.168.1.0/24 Outside	Outsi	ide (1 Dynamic rules	;)			
1 Exempt any # 192.168.1.0/24 (outbound) 2 Dynamic any Outside Image: C	1	Dynamic	192.168.1.0/24		inside	in and
1 Exempt Image: any ima	inside	e (1 Exempt rules, 1	Dynamic rules)			
2 Dynamic 🐼 any Outside 📼 C	1	🞫 Exempt	🌍 any	192.168.1.0/24	(outboun	d)
	2	Dynamic	🏈 any		Outside	555 O

Configurar o ASA/PIX como um servidor de VPN remoto e para o NAT de entrada com o CLI

Configuração running no dispositivo ASA
ciscoasa# show running-config : Saved ASA Version 8.0(3)
! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif Outside
security-level 0 ip address 10.10.10.2 255.255.255.0 !
interface Ethernet0/1 nameif inside security-level 100
ip address 172.16.1.2 255.255.255.0 ! ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-
k8.bin ftp mode passive access-list inside_nat0_outbound
extended permit ip any 192.168.1.0 255.255.255 0 pager
lines 24 logging enable mtu Outside 1500 mtu inside 1500
ip local pool vpnpool 192.168.1.1-192.168.1.254 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-615.bin asdm history
enable arp timeout 14400 nat-control global (Outside) 1
interface global (inside) 2 interface nat (Outside) 2

192.168.1.0 255.255.255.0 outside nat (inside) 0 accesslist inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0 route Outside 0.0.0.0 0.0.0.0 10.10.10.3 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 sipdisconnect 0:02:00 timeout uauth 0:05:00 absolute dynamic-access-policy-record DfltAccessPolicy http server enable no snmp-server location no snmp-server contact !--- Configuration for IPsec policies. !---Enables the crypto transform configuration mode, !--where you can specify the transform sets that are used !--- during an IPsec negotiation. crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto map Outside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map interface Outside crypto isakmp enable Outside !---Configuration for IKE policies. !--- Enables the IKE policy configuration (config-isakmp) !--- command mode, where you can specify the parameters that !--- are used during an IKE negotiation. Encryption and !--- Policy details are hidden as the default values are chosen. crypto isakmp policy 10 authentication pre-share encryption des hash sha group 2 lifetime 86400 crypto isakmp policy 30 authentication pre-share encryption des hash md5 group 2 lifetime 86400 telnet timeout 5 ssh timeout 60 console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list group-policy cisco internal group-policy cisco attributes vpn-tunnel-protocol IPSec !--- Specifies the username and password with their !--respective privilege levels username cisco123 password ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco password ffIRPGpDSOJh9YLq encrypted privilege 0 username cisco attributes vpn-group-policy cisco tunnel-group cisco type remote-access tunnel-group cisco generalattributes address-pool vpnpool default-group-policy cisco !--- Specifies the pre-shared key "cisco123" which must !--- be identical at both peers. This is a global !--- configuration mode command. tunnel-group cisco ipsec-attributes pre-shared-key * ! class-map inspection_default match default-inspection-traffic ! ! policy-map type inspect dns migrated_dns_map_1 parameters message-length maximum 512 policy-map global_policy class inspection_default inspect dns migrated_dns_map_1 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 prompt hostname context Cryptochecksum:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end ciscoasa#

Verificar

Tente conectar a Cisco ASA através do Cisco VPN Client a fim verificar que o ASA está

configurado com sucesso.

1. Clique em

New.			
VPN Client - Version 5.0.03.0530			
Connection Entries Status Certificates Log Options	; Help		
Connect News Import Modify) Delete		ahaha cisco
Connection Entries Certificates Log			
Connection Entry	Host	Transport	
Not connected.			

2. Preencha os detalhes de sua nova conexão.O campo do host deve conter o endereço IP ou nome do host de Cisco previamente configurado ASA. A informação da autenticação do grupo deve corresponder àquela usada na **salvaguarda do** clique de **etapa 4.** quando você é

VPN Client Create New VPN Connection Entry	×
Connection Entry: MyVPNClient	
Description:	
Host: 10.10.10.2	cisco
Authentication Transport Backup Servers Dial-Up	
Group Authentication	Authentication
Name: cisco	
Password: ******	
Confirm Password: *******	
C Certificate Authentication	
Name:	
🔲 Send CA Certificate Chain	
Erase User Password	Cancel

3. Selecione a conexão recém-criado, e o clique **conecta**.

Status: Disconnected VPN Client - Version	on 5.0.03.0530		
Connection Entries Status Certificates Log Options	Help		
Confect New Import Modify Connection Entries Certificates Log	X Delete		cisco
Connection Entry	Host	Transport	
MyVPNClient	10.10.10.2	IPSec/UDP	
Not connected.			

4. Incorpore um nome de usuário e senha para a autenticação extendida. Esta informação deve combinar aquela especificada nas **etapas 5 e**

	VPN Client User Authentication for "MyVPNClient"
	The server has requested the following information to complete the user authentication.
	Username: cisco123 CISCO Password: *******
6.	OK Cancel

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

🥔 status: Connected Vi	PN Client - Ver	ion 5.0.03.0530		
Connection Entries Status Ce	artificates Log Op	otions Help		
Disconnect N	tics Ctrl+S tations Ctrl+N	Delete		ilialia cisco
Connection Entries Reset	Stats			
Connection Entry	Δ	Host	Transport	
MyVPNClient		10.10.10.2	IPSec/UDP	
Connected to "MyVPNClient".			Connected Time: 0 day(s), 00:00.36	5 T

Este indicador mostra o tráfego e a informação de

VPN Client Statistics			
Tunnel Details Route Details	Firewall		
Address Information	Connection Information		
Client: 192.168.1.1	Entry: MyVPNClient		
Server: 10.10.10.2	Time: 0 day(s), 00:01.13		
Bytes	Crypto		
Received: 5412	Encryption: 56-bit DES		
Sent: 5416	Authentication: HMAC-MD5		
Packets	Transport		
Encrypted: 39	Transparent Tunneling:Inactive		
Decrypted:31	Local LAN: Disabled		
Discarded: 8	Compression: None		
Bypassed: 22			
	Reset		
	Close		

criptografia: Este indicador mostra a informação do Split

VPN Client	Statistics			×
Tunnel Details	Route Details Fi	rewall		
Local LAN Rou	Local LAN Routes		Secured Routes	
Network	Subnet Mask	Network 0.0.0.0	0.0.00	
			Close	

Tunneling:

Ferramenta de segurança ASA/PIX - comandos show

- mostre isakmp cripto sa Mostra todo o IKE atual SA em um par.ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE
- mostre IPsec cripto sa Mostra todo o sas de IPSec atual em um par.ASA#show crypto ipsec sa interface: Outside Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 .10.2 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 10.10.10.1, username: cisco123 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0 #prefrag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y
- ciscoasa(config)#debug icmp trace !--- Inbound Nat Translation is shown below for Outside to Inside ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 !--- Inbound Nat Translation is shown below for Inside to Outside ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from

172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8960 len=32

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

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.

Refira <u>a maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções</u> para obter mais informações sobre de como pesquisar defeitos o Local-local VPN.

Informações Relacionadas

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- <u>Cisco Adaptive Security Device Manager</u>
- O Dispositivos de segurança adaptáveis Cisco ASA série 5500 pesquisa defeitos e alertas
- <u>Suporte Técnico e Documentação Cisco Systems</u>