Exemplo de configuração de VPN SSL thin-client (WebVPN) no ASA com ASDM

Contents

Introduction **Prerequisites** Requirements Componentes Utilizados Diagrama de Rede **Conventions** Informações de Apoio Configuração de VPN SSL Thin-Client usando ASDM Etapa 1. Habilitar WebVPN no ASA Etapa 2. Configurar características de encaminhamento de porta Etapa 3. Crie uma política de grupo e vincule-a à lista de encaminhamento de portas Etapa 4. Crie um grupo de túnel e vincule-o à política de grupo Etapa 5. Crie um usuário e adicione esse usuário à política de grupo Configuração de VPN SSL Thin-Client usando CLI Verificar Procedimento Comandos Troubleshoot O processo de handshake SSL está concluído? O Thin Client da VPN SSL está funcionando? Comandos Informações Relacionadas

Introduction

A tecnologia de Thin-Client SSL VPN permite um acesso seguro para aplicativos que têm portas estáticas, como Telnet(23), SSH(22), POP3(110), IMAP4(143) e SMTP(25). É possível usar a Thin-Client SSL VPN como um aplicativo executado por usuário, aplicativo executado por políticas ou ambos. Isto é, você pode configurar o acesso em uma base de usuário por usuário ou criar Políticas de Grupo nas quais adicionará um ou mais usuários.

 VPN SSL sem cliente (WebVPN)—Fornece um cliente remoto que exige um navegador Web habilitado para SSL para acessar servidores Web HTTP ou HTTPS em uma rede local corporativa (LAN). Além disso, a VPN SSL sem cliente fornece acesso para a navegação de arquivos do Windows através do protocolo CIFS (Common Internet File System). O Outlook Web Access (OWA) é um exemplo de acesso HTTP.Consulte <u>Exemplo de Configuração de</u> <u>VPN SSL Sem Clientes (WebVPN) no ASA</u> para saber mais sobre a VPN SSL Sem Clientes.

- Thin-Client SSL VPN (Port Forwarding)—Fornece um cliente remoto que faz o download de um pequeno miniaplicativo baseado em Java e permite acesso seguro para aplicativos TCP (Transmission Control Protocol) que usam números de porta estáticos. Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), secure shell (ssh) e Telnet são exemplos de acesso seguro. Como os arquivos na máquina local mudam, os usuários devem ter privilégios administrativos locais para usar esse método. Esse método de VPN SSL não funciona com aplicativos que usam atribuições de porta dinâmicas, como alguns aplicativos de protocolo de transferência de arquivos (FTP).Observação: o User Datagram Protocol (UDP) não é suportado.
- SSL VPN Client (Tunnel Mode) Faz download de um pequeno cliente para a estação de trabalho remota e permite acesso totalmente seguro aos recursos em uma rede corporativa interna. Você pode baixar permanentemente o SSL VPN Client (SVC) em uma estação de trabalho remota ou pode remover o cliente quando a sessão segura é fechada.Consulte <u>Exemplo de Configuração de SSL VPN Client (SVC) no ASA com ASDM</u> para saber mais sobre o SSL VPN Client.

Este documento demonstra uma configuração simples para o Thin-Client SSL VPN no Adaptive Security Appliance (ASA). A configuração permite que um usuário faça telnet com segurança para um roteador localizado no interior do ASA. A configuração neste documento é suportada para o ASA versão 7.x e posterior.

Prerequisites

Requirements

Antes de tentar esta configuração, verifique se você atende a estes requisitos para as estações cliente remotas:

- navegador da Web habilitado para SSL
- SUN Java JRE versão 1.4 ou posterior
- Cookies ativados
- Bloqueadores de pop-up desabilitados
- Privilégios administrativos locais (não obrigatórios, mas altamente sugeridos)

Observação: a versão mais recente do SUN Java JRE está disponível como download gratuito no site Java.

Componentes Utilizados

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

- Cisco Adaptive Security Appliance série 5510
- Cisco Adaptive Security Device Manager (ASDM) 5.2(1) Observação: consulte <u>Permitindo</u> <u>Acesso HTTPS para ASDM</u> para permitir que o ASA seja configurado pelo ASDM.
- Software Cisco Adaptive Security Appliance versão 7.2(1)
- Cliente remoto do Microsoft Windows XP Professional (SP 2)

As informações neste documento foram desenvolvidas em um ambiente de laboratório. Todos os dispositivos usados neste documento foram redefinidos para sua configuração padrão. Se sua rede estiver ativa, certifique-se de que você entendeu o impacto potencial de qualquer comando. Todos os endereços IP usados nesta configuração foram selecionados de endereços RFC 1918

em um ambiente de laboratório; esses endereços IP não são roteáveis na Internet e são apenas para fins de teste.

Diagrama de Rede

Este documento usa a configuração de rede descrita nesta seção.

Quando um cliente remoto inicia uma sessão com o ASA, o cliente faz o download de um pequeno miniaplicativo Java para a estação de trabalho. O cliente recebe uma lista de recursos pré-configurados.



Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

Para iniciar uma sessão, o cliente remoto abre um navegador SSL para a interface externa do ASA. Depois que a sessão é estabelecida, o usuário pode usar os parâmetros configurados no ASA para invocar qualquer Telnet ou acesso de aplicativo. O ASA faz o proxy da conexão segura e permite que o usuário acesse o dispositivo.

Observação: as listas de acesso de entrada não são necessárias para essas conexões porque o ASA já está ciente do que constitui uma sessão legal.

Configuração de VPN SSL Thin-Client usando ASDM

Para configurar o Thin-Client SSL VPN no ASA, faça o seguinte:

- 1. Habilitar WebVPN no ASA
- 2. Configurar características de encaminhamento de porta
- <u>Crie uma Política de Grupo e vincule-a à Lista de Encaminhamento de Portas</u> (criada na Etapa 2)
- 4. Crie um Grupo de Túneis e vincule-o à Política de Grupo (criada na Etapa 3)
- 5. <u>Crie um usuário e adicione esse usuário à política de grupo</u> (criada na Etapa 3)

Etapa 1. Habilitar WebVPN no ASA

Para habilitar o WebVPN no ASA, faça o seguinte:

- 1. No aplicativo ASDM, clique em Configuration e em VPN.
- 2. Expanda WebVPN e escolha WebVPN

Access.										
Cisco ASDM 1	5.2 for ASA	- 10.2.2.1								
File Options Too	sis Wizardis	Help						Search		Find v
			-			-				Carea Sections
S	2		0	(2)	2 6	<u>الا</u> ﴿	?			
Home C	Configuration	Monitoring	Back	Forward Packet	Tracer Refr	esh Save	Help			السيرالي
	Configuratio	in > VPN > Web	VPN > V	VebVPN Access						
	VPN VPN	Wzard	1	bVPN Access						
Interfaces	Gene	tral								
	B-IB PSec	4		configure access paramet	ers for WebVPN	l.				
۵,	B B P Ad	idress Manageme	nt							
Security Policy	NAC 1									
34.	E - E Web	VPN		Interface		WebVPN Enab	led		Enable	
NAT.		Provies		inside			No			
NAT	-27	APCF		outside			Yes		Disable	
<u> </u>		Auto Signon								
VPN		Cache								
r Ma		lava Trustpoint								
I	- S F	Proxy Bypass								
PS	- 🗊 s	Servers and URLs	5		Euro:					
A	- <u></u>	Port Forwarding		Port Number:	443					
CSD Mapager		Vebpage Custom ACL +	62.65	Default Idle Timeout	1800	seconds				
	- 66	Encoding								
428		SSL VPN Client		Max. Sessions Limit:	2					
Routing		SSO Servers			-			100		
(A)	E-ma	a Proxy		WebVPN Memory Size:	50	% of total physic	al memory	×		
Ciphal Objects				Enable Tunnel Group D	rop-down List o	n WebVPN Login Pa	sge			
Cioble Cojects										
2										
Properties										
						Apply	Rese	t		
	<		>							
					ci	sco 15			6/27/0	6 7:01:44 AM UT

- 3. Realce a interface e clique em Enable (Habilitar).
- 4. Clique em Aplicar, clique em Salvar e clique em Sim para aceitar as alterações.

Etapa 2. Configurar características de encaminhamento de porta

Para configurar as características de encaminhamento de portas, faça o seguinte:

1. Expanda WebVPN e escolha Port Forwarding.



2. Clique no botão Adicionar.

File Options 1	Tools Wizards	Help							Search	:	Find •
Shome	Configuration	Monitoring	Back	Forward	Packet Tracer	Refresh	Save	? Нер			Cisco Systems
Interfaces	Continuation	IN - VEN - We Wizerd eral VPN System Opt Client Update Tunnel Group Group Policy Users Default Tunnel G Zone Labs Integr	ovPN > Po ions ateway rity Server	rt Forwardins	Configure port for This parameter	warding lists fo is enforced it Local TCP P	r application n either a Vi tort Rem	access over PN <u>user</u> or j ote Server	WebVPN. group policy cor Remote TCP	nfiguration.	Add
VPN VPN PS	PSe PSe PAC PAC PAC PAC PAC PAC PAC PAC	c ddress Manager Assignment P Pools WPN	Ki Add	Port Forwa	rding List Routers						×
CSD Manager		WebVPN Acces Provies APCF Auto Signon Cache Content Rewrite Java Trustpoint Proxy Bypass Servers and UR Servers and UR Soft Serversion Webpage Custo ACLs	2	Local TCP Port	Renote Serv	ver Remot	le TCP Port	Description	n		Add Edit Delete
Properues	■ 🥞 E-ma	Encoding SSL VPN Client SSO Servers all Proxy				ок	Car	ncel	Help		7/18/06 12:40:29 PM UTC

 Na caixa de diálogo Add Port Forwarding List (Adicionar lista de encaminhamento de portas), digite um nome de lista e clique em Add.A caixa de diálogo Add Port Forwarding Entry é exibida.

屆 Add Port Forwarding	Entry	×
Local TCP Port:	3044	
Remote Server:	10.2.2.2	
Remote TCP Port:	23	
Description:	Telnet to R1	
ок	Cancel Help	

4. Na caixa de diálogo Adicionar entrada de encaminhamento de porta, digite estas opções:No

campo Porta TCP local, insira um número de porta ou aceite o valor padrão.O valor digitado pode ser qualquer número de 1024 a 65535.No campo Servidor remoto, insira um endereço IP.Este exemplo usa o endereço do roteador.No campo Remote TCP Port (Porta TCP remota), insira um número de porta.Este exemplo usa a porta 23.No campo Descrição, digite uma descrição e clique em **OK**.

- 5. Clique em OK e em Aplicar.
- 6. Clique em Save e, em seguida, clique em Yes para aceitar as alterações.

Etapa 3. Crie uma política de grupo e vincule-a à lista de encaminhamento de portas

Para criar uma política de grupo e vinculá-la à lista de encaminhamento de portas, faça o seguinte:

1. Expanda General e escolha Group



2. Clique em Add e escolha Internal Group Policy. A caixa de diálogo Add Internal Group Policy é

exibida.

Tunneling Protocols:	🔲 Inherit	✓ IPSec ✓ WebVPN ✓ L2TP over IPSec
Filter:	🗹 Inherit	Manage
Connection Settings	_	
Access Hours:	🗹 Inherit	Manage
Simultaneous Logins:	🗹 Inherit	
Maximum Connect Time:	🗹 Inherit	Unlimited minutes
Idle Timeout:	🖌 Inherit	Unlimited minutes
Servers		
DNS Servers:	🗹 Inherit	Primary: Secondary:
WINS Servers:	🗹 Inherit	Primary: Secondary:
DHCP Scope:	🗹 Inherit	

- 3. Insira um nome ou aceite o nome padrão da política de grupo.
- 4. Desmarque a caixa de seleção Tunneling Protocols **Inherit** e marque a caixa de seleção **WebVPN**.
- 5. Clique na guia **WebVPN** localizada na parte superior da caixa de diálogo e clique na guia **Functions**.
- Desmarque a caixa de seleção Inherit e marque as caixas de seleção Enable auto applet download e Enable port forwarding como mostrado nesta imagem:

📧 Add Internal Group Policy	×
Name: NetAdmins	
General IPSec Client Configuration Client Firewall Hardware Client NAC WebVPN	
Configure WebVPN attributes using the following tabs .	
Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.	
Functions Content Filtering Homepage Port Forwarding Other SSL VPN Client Auto Signon	
Inherit Sachla UEL ante: Inherit	
Enable file server access Enable Outlook/Exchange proxy	
Enable file server entry Apply Web-type ACL	
Enable file server browsing Enable http proxy Enable auto applet download Enable Citrix MetaExame	
OK Cancel Help	

 Além disso, na guia WebVPN, clique na caixa de seleção Port Forwarding (Encaminhamento de portas) e desmarque a opção Port Forwarding List Inherit (Herdar lista de encaminhamento de portas).

🖬 Add Internal Group Policy			×
Name: NetAdmins			
General IPSec Client Configu	ration Client Firewall	Hardware Client NAC WebVPN	
Configure WebVPN attributes	using the following tabs		
Check an Inherit checkbox to i	the corresponding set	and the state from the detault group policy.	
Functions Content Filtering	Homepage FortForw	aroung Other SSL VPN Client Auto Signon	
	_		
Port Forwarding List:	lnherit	Routers New	
Applet Name:	lnherit	Secure Router Access	
	ок	Cancel Help	

- 8. Clique na seta suspensa **Lista de encaminhamento de portas** e escolha a lista de encaminhamento de portas que você criou na <u>Etapa 2</u>.
- 9. Desmarque a caixa de seleção Nome do miniaplicativo **Herdar** e altere o nome no campo de texto.O cliente exibe o nome do miniaplicativo na conexão.
- 10. Clique em **OK** e em **Aplicar**.
- 11. Clique em Save e, em seguida, clique em Yes para aceitar as alterações.

Etapa 4. Crie um grupo de túnel e vincule-o à política de grupo

Você pode editar o grupo de túneis *DefaultWebVPNGroup* padrão ou criar um novo grupo de túneis.

Para criar um novo grupo de túneis, faça o seguinte:

1. Expanda General e escolha Tunnel Group.



 Clique em Add e escolha WebVPN Access. A caixa de diálogo Add Tunnel Group (Adicionar grupo de túnel) é exibida.

Add Tu	innel Group					X
Nar	ne: NetGroup)	Туре:	webvpn		
Gene	ral WebVPN					
Cor	nfigure general acce	ess attributes from	the following sub	tabs.		
Bas	ic Authentication	Authorization A	ccounting Client	Address Assignment	Advanced	
	Group Policy:	NetAdmins	~			
	Strip the realm 1	rom username bef	ore passing it on t	o the AAA server		
	Christina array an	from usarnama haf	are needing it on t	o the AAA cenuer		
	Strip trie group	from username ber	ore passing it on	U ITIE AAA SERVER		
1	Password Manage	ment	ation from AAA s	arvar		
	Enable notifi	cation upon passw	ord expiration to a	llow user to change p	assword	
	Enable	notification prior to	expiration	Notify	days prior to expiration	
2						
		ок	Can	cel He	elp	

- 3. Digite um nome no campo Nome.
- 4. Clique na seta suspensa **Política de grupo** e escolha a política de grupo criada na Etapa 3.
- 5. Clique em **OK** e em **Aplicar**.
- 6. Clique em **Save** e, em seguida, clique em **Yes para aceitar as alterações.**O grupo de túneis, a política de grupo e as características de encaminhamento de portas agora estão vinculadas.

Etapa 5. Crie um usuário e adicione esse usuário à política de grupo

Para criar um usuário e adicioná-lo à política de grupo, faça o seguinte:

1. Expanda **General** e escolha **Users**.

File Options To	ols Wizards	Help							Search		Find •
Shore a	oggi Configuration	Monitoring	O Back	Forward	C Packet Tracer	Q Refresh	Save	? Help			Cisco Systems
Interfaces Security Policy NAT	Confoundo VPNI Confo Con	In 2 VPN 2 Gane Wizard rai /PN System Option /ient Update unnel Group Aroup Policy Jone Secone Labo Integrity 25ec Rules	ral > Usor -Usors Is C It VM S C C It It S C It It S C It It S C It It It It It It It It It It	IS Create entries he user acco User Name nable_15 Isco usrmi ales1	a in the ASA local unt privileges to I Privilege 15 15 15 4	user datab be enforced Level (Role)	ase, Comman To enable co VPN Group Po MA DitGrpPolicy DitGrpPolicy SalesGroupPoli	d author mmand licy cy	ization must be en authorization, go to VPN Group Lock NUA Inhert Group Polic. Inhert Group Polic. Inhert Group Polic.	abled in order for	
PS PS CSD Manager & Routing		ransform Sets tre-Fragmentation kissignment > Pools VPN Neb/VPN Access troxies upOF Luto Signon acche	e								
Global Objects		Content Rewrite lava Trustpoint troxy Bypass Servers and URLs fort Forwarding Vebpage Customiz NCLs incoding SL VPN Client ISO Servers Il Proxy	ot .				Apply:		Reset		

2. Clique no botão Adicionar. A caixa de diálogo Adicionar conta de usuário é exibida.

🖆 Add User Account	
Identity VPN Policy WebVPN	
The second second	
Username:	user1
Password:	*****
Confirm Password:	*****
	advision MCCH4D
	a using MSCHAP
Privilege level is used with	h command authorization.
Privilege Level:	2
OK R	Cancel Help

 Insira valores para o nome de usuário, senha e informações de privilégio e clique na guia Política de VPN.

Check an Inherit checkbox to let the o	corresponding sett	ing take its value from the group policy.
Tunneling Protocols:	🗹 Inherit	IPSec WebVPN L2TP over IPSec
Filter:	🗹 Inherit	Manage
Tunnel Group Lock:	🗹 Inherit	×
Store Password on Client System:	🗹 Inherit	⊖ Yes ⊖ No
Connection Settings		
Access Hours:	🗹 Inherit	New
Simultaneous Logins:	🗹 Inherit	
Maximum Connect Time:	🗹 Inherit	Unlimited minutes
Idle Timeout:	🔽 Inherit	Unlimited minutes
Dedicated IP Address (Optional)		
IP Address:	Subr	net Mask:

- Clique na seta suspensa Política de grupo e escolha a política de grupo criada na Etapa <u>3</u>.Este usuário herda as características e políticas do WebVPN da política de grupo selecionada.
- 5. Clique em OK e em Aplicar.
- 6. Clique em Salvar e em Sim para aceitar as alterações.

Configuração de VPN SSL Thin-Client usando CLI

ASA
ASA Version 7.2(1)
1
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
1
interface Ethernet0/0
nameif inside

```
security-level 100
ip address 10.1.1.1 255.255.255.0
!--- Output truncated port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
!--- Configure the set of applications that WebVPN
users !--- can access over forwarded TCP ports group-
policy NetAdmins internal
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
vpn-tunnel-protocol IPSec 12tp-ipsec webvpn
!--- Configure group policy attributes webvpn
 functions port-forward auto-download
!--- Configure group policies for WebVPN
                                           port-forward
value portforward
!--- Configure port-forward to enable WebVPN
application access !--- for the new group policy port-
forward-name value Secure Router Access
!--- Configure the display name that identifies TCP
port !--- forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
vpn-group-policy NetAdmins
!--- Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
default-group-policy NetAdmins
!--- Create a new tunnel group and link it to the group
policy telnet timeout 5 ssh timeout 5 console timeout 0
! 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 ! service-policy global_policy global webvpn
enable outside
!--- Enable Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context
```

Verificar

Use esta seção para verificar se sua configuração funciona corretamente.

Procedimento

Este procedimento descreve como determinar a validade da configuração e como testar a configuração.

 Em uma estação de trabalho cliente, digite https:// outside_ASA_IP Address; onde outside_ASA_IPAaddress é a URL SSL do ASA.Quando o certificado digital for aceito e o usuário for autenticado, a página Web do WebVPN Service será exibida.

File Edit View Favo	prites Tools Help	c explorer				
🚱 Back 🔹 🕥 🕤	🗷 🗟 🏠 🎾	💭 Search 🛛 🔶 Fi	avorites 🧭	Ø- 🕹	w •	, »
Address Address //172.2	22. 1. 160/+webvpn+/p	ortal.html		1	🗸 💽 Co	Links »
Google -	~ G	Search 🝷 🧭	爹 🛃 Popu	ps okay »	Snagl	it 🛃
Cisco Systems	ebVPN Servi	ce				_
				?	?⊁@[\times
ACCESS Start Application C Close this win Please wait for If you shut do later have pro- details.	lient Go 2.1.160 - Secure R dow when you fu or the table to be wn your compute oblems running th	touter Access - M nish using Appl displayed befor er without closin te applications	Aicrosoft Int ication Acc re starting ig this wind listed below	ernet Ex ess. applications low, you mig v. <u>Click her</u>	s. s. <u>e for</u>	
Name Telnet to R1	Local 127.0.0.1:3044	Remote 10.2.2.2:23	Bytes Out	Bytes In S	ockets 0	
Done	11211010110200) Internet		
🛃 Done			21	🔒 🌒 In	iternet	

As informações de endereço e porta necessárias para acessar o aplicativo são exibidas na coluna local. As colunas Bytes Out e Bytes In não exibem nenhuma atividade porque o aplicativo não foi chamado no momento.

- 2. Use o prompt do DOS ou outro aplicativo Telnet para iniciar uma sessão Telnet.
- 3. No prompt de comando, digite telnet 127.0.0.1 3044.Observação: esse comando fornece um exemplo de como obter acesso à porta local exibida na imagem da página Web do WebVPN Service neste documento. *O comando não inclui dois-pontos (:)*. Digite o comando conforme descrito neste documento.O ASA recebe o comando pela sessão segura e, como armazena um mapa das informações, o ASA sabe imediatamente para abrir a sessão Telnet segura para o dispositivo mapeado.



Quando você digitar seu nome de usuário e senha, o acesso ao dispositivo estará concluído.

4. Para verificar o acesso ao dispositivo, verifique as colunas Bytes Out e Bytes In como mostrado nesta

imagem:

 https://172.22.1.160 - Secure Router Access - Microsoft Internet Ex Close this window when you finish using Application Access. Please wait for the table to be displayed before starting applications. If you shut down your computer without closing this window, you might later have problems running the applications listed below. <u>Click here for details.</u> 											
Name	Local	Remote	Bytes Out	Bytes In	Sockets						
Telnet to R1	127.0.0.1:3044	10.2.2.2:23	56	127	1						
SSH to R1	127.0.0.1:3255	10.2.2.2:22	0	0	0						

Comandos

Vários **comandos show estão associados ao WebVPN.** Você pode executar estes comandos na interface de linha de comando (CLI) para mostrar estatísticas e outras informações. Para obter informações detalhadas sobre os **comandos show, consulte** <u>Verificação da Configuração do</u> <u>WebVPN</u>.

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

Troubleshoot

Use esta seção para resolver problemas de configuração.

O processo de handshake SSL está concluído?

Depois de se conectar ao ASA, verifique se o registro em tempo real mostra a conclusão do handshake SSL.

🎼 Real-time Log Viewer									
0 Pause	в 🗈 Сору 🌡	🕽 Save 👸	Clear 👩	Color Settings	🔁 Create Rule 🥈	Show Rule 🔞 Show Details 🤗 Help			
Filter By		~	Elter	Show Al					
Severity	Date	Time	Syslog	Source IP	Destination IP	Description			
2	Jun 27 2006	11:40:42	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3102 to 216.2	239.53.1		
@ 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.70.157.215	Deny inbound UDP from 172.22.1.203/3101 to 171.70.157.215/1	029 on i		
@ 2	Jun 27 2006	11:40:34	106006	172.22.1.203	64.101.176.170	Deny inbound UDP from 172.22.1.203/3101 to 64.101.176.170/1	029 on i		
@ 2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.68.222.149	Deny inbound UDP from 172.22.1.203/3101 to 171.68.222.149/1	029 on i		
@ 2	Jun 27 2006	11:40:32	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172 22.1 203/3100 to 216.	239.53.1		
2	Jun 27 2006	11:40:24	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.	239.53.1		
2	Jun 27 2006	11:40:22	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.3	239.53.1		
4.6	Jun 27 2006	11:40:18	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.2	03/3097		
A 6	Jun 27 2006	11:40:18	725003	172.22.1.203		SSL client outside:172.22.1.203/3097 request to resume previou	us sessi		
A 6	Jun 27 2006	11:40:18	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3097 ft	or TLSv		
A 6	Jun 27 2006	11:40:18	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3711 for outside:172.22.1.203/309	7 (172.		
A 6	Jun 27 2006	11:40:18	725007	172.22.1.203		SSL session with client outside:172.22.1.203/3096 terminated.			
A 6	Jun 27 2006	11:40:17	302014	172.22.1.203	172.22.1.160	Teardown TCP connection 3710 for outside:172.22.1.203/3096	to NP Ide		
A 6	Jun 27 2006	11:40:17	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.2	03/3096		
A 6	Jun 27 2006	11:40:17	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3096 f	or TLSv		
A 6	Jun 27 2006	11:40:17	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3710 for outside:172.22.1.203/309	6 (172.		
G 3	Jun 27 2006	11:40:16	305005	64.101.176.170		No translation group found for udp src inside:10.2.2.4/1830 dst	outside:		
🔂 3	Jun 27 2006	11:40:16	305005	171.70.157.215		No translation group found for udp src inside:10.2.2.4/1830 dst	outside:		
63	Jun 27 2006	11:40:16	305005	171,68.222,149		No translation group found for udp src inside:10.2.2.4/1830 dst	outside:		
2	Jun 27 2006	11:40:15	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.3	239.53.1		
0 2	Jun 27 2006	11:40:12	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.3	239.53.1		
<			10				>		
Please select a syslog entry to see the explanation ×									
Explanation Recommended Action Details									
🗿 Emergencies 🔇 Alerts 🙆 Critical 🙆 Errors 🛦 Warnings 🔺 Notifications 🗼 Informational 🛞 Debugging									

O Thin Client da VPN SSL está funcionando?

Para verificar se o Thin-Client de VPN SSL está funcionando, faça o seguinte:

- 1. Clique em Monitoring e, em seguida, clique em VPN.
- Expanda VPN Statistics e clique em Sessions.Sua sessão SSL VPN Thin-Client deve aparecer na lista de sessões. Certifique-se de filtrar por WebVPN conforme mostrado nesta imagem:



Comandos

Vários **comandos debug estão associados ao WebVPN.** Para obter informações detalhadas sobre estes comandos, consulte <u>Uso de Comandos de Depuração do WebVPN</u>.

Observação: o uso de comandos **debug** pode afetar adversamente seu dispositivo Cisco. Antes de utilizar **comandos debug, consulte** <u>Informações Importantes sobre Comandos Debug</u>.

Informações Relacionadas

- Exemplo de configuração de VPN SSL sem cliente (WebVPN) no ASA
- Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- ASA com WebVPN e logon único usando o exemplo de configuração de ASDM e NTLMv1
- Suporte Técnico e Documentação Cisco Systems