# Configurar a postura de VPN ASA com CSD, DAP e AnyConnect 4.0

### Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Configurar Diagrama de Rede ASA Etapa 1. Configuração básica de VPN SSL Etapa 2. Instalação do CSD Etapa 3. Políticas de DAP ISE Verificar Provisionamento de CSD e AnyConnect Sessão AnyConnect VPN com postura - Não compatível Sessão AnyConnect VPN com postura - Compatível **Troubleshoot** DART do AnyConnect Informações Relacionadas

## Introduction

Este documento descreve como executar a postura para sessões de VPN remotas encerradas no Adaptive Security Appliance (ASA). A postura é executada localmente pelo ASA com o uso do Cisco Secure Desktop (CSD) com o módulo HostScan. Depois que a sessão VPN é estabelecida, a estação compatível tem acesso total à rede, enquanto a estação não compatível tem acesso limitado à rede.

Além disso, os fluxos de provisionamento do CSD e do AnyConnect 4.0 são apresentados.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco ASA VPN
- Cisco AnyConnect Secure Mobility Client

#### **Componentes Utilizados**

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

- Microsoft Windows 7
- Cisco ASA, versão 9.3 ou posterior
- Software Cisco Identity Services Engine (ISE), versões 1.3 e posteriores
- Cisco AnyConnect Secure Mobility Client, versão 4.0 e posterior
- CSD, versão 3.6 ou posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

#### Diagrama de Rede



A política corporativa é a seguinte:

- Os usuários remotos de VPN com arquivo c:\test.txt (compatível) devem ter acesso total à rede para os recursos internos da empresa
- Os usuários remotos de VPN que não têm o arquivo c:\test.txt (não compatível) devem ter acesso limitado à rede aos recursos internos da empresa: somente o acesso ao servidor de correção 1.1.1.1 é fornecido.

A existência de arquivo é o exemplo mais simples. Qualquer outra condição (antivírus, antispyware, processo, aplicativo, registro) pode ser usada.

O fluxo é o seguinte:

- Os usuários remotos não têm o AnyConnect instalado. Eles acessam a página da Web do ASA para provisionamento de CSD e AnyConnect (junto com o perfil de VPN)
- Após a conexão via AnyConnect, usuários não compatíveis são permitidos com acesso limitado à rede. A DAP (Dynamic Access Policy, Política de acesso dinâmico) chamada FileNotExists é combinada.
- O usuário executa a correção (instale manualmente o arquivo c:\test.txt) e se conecta novamente com o AnyConnect. Desta vez, é fornecido acesso total à rede (a política DAP chamada FileExists é combinada).

O módulo HostScan pode ser instalado manualmente no endpoint. Arquivos de exemplo (hostscan-win-4.0.00051-pre-Deployment-k9.msi) são compartilhados no Cisco Connection Online (CCO). Mas também pode ser empurrado da ASA. O HostScan faz parte do CSD que pode ser provisionado do ASA. Esta segunda abordagem é utilizada neste exemplo.

Para versões mais antigas do AnyConnect (3.1 e anteriores), havia um pacote separado disponível no CCO (por exemplo: hostscan\_3.1.06073-k9.pkg) que poderia ter sido configurado e provisionado no ASA separadamente (com o comando **csd hostscan image**) - mas essa opção não existe mais para o AnyConnect versão 4.0.

#### ASA

#### Etapa 1. Configuração básica de VPN SSL

O ASA é pré-configurado com acesso VPN remoto básico (Secure Sockets Layer (SSL)):

```
webvpn
enable outside
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
anyconnect enable
tunnel-group-list enable
group-policy AllProtocols internal
group-policy AllProtocols attributes
vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless
tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
address-pool POOL
authentication-server-group ISE3
default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
group-alias TAC enable
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0
aaa-server ISE3 protocol radius
aaa-server ISE3 (inside) host 10.1.1.100
key ****
O pacote do AnyConnect foi baixado e usado.
```

#### Etapa 2. Instalação do CSD

A configuração subsequente é executada com o Adaptive Security Device Manager (ASDM). O pacote CSD precisa ser baixado para que o flash e a referência da configuração sejam mostrados na imagem.

Home 🗞 Configuration 📴 Monitor	ing 🔚 Save 🔇 Refresh 🔇 Back 💭 Forward 🧳 Help
Device List 🗗 🖗 🗡	Configuration > Remote Access VPN > Secure Desktop Manager > Setup
Add      Delete      Connect      Go      10.48.67.158:8443      10.48.67.229:444	Secure Desktop Image Update Cisco Secure Desktop. Location: disk0:/csd_3.6.6249-k9.pkg Browse Flash
10.62.145.45:8443           10.62.97.56:8443           10.62.97.56:8443           10.62.97.56:8444           10.62.97.56:8444           10.62.97.56:8444           10.62.97.56:8444	Enable Secure Desktop      Upload      Uninstall
Remote Access VPN     Image       Introduction     Image       Image     AAA/Local Users       Image     Image       Image     Image	

Sem habilitar o Secure Desktop, não seria possível usar atributos de CSD nas políticas de DAP como mostrado na imagem.



Depois de habilitar o CSD, várias opções em Secure Desktop Manager são exibidas.

**Note**: Esteja informado de que alguns deles já estão em decadência. Mais informações sobre recursos obsoletos podem ser encontradas: <u>Aviso de Deterioração de Funcionalidade</u> para Ambiente de Trabalho Seguro (Cofre), Limpeza de Cache, Detecção de Bloqueador de <u>Teclas e Detecção de Emulação de Host</u>

O HostScan ainda é totalmente suportado, uma nova regra básica do HostScan é adicionada. A existência de c:\test.txt é verificada como mostrado na imagem.

🛞 Home 🖧 Configuration 📴 Monitori	ng 🔚 Save 🔇 Refresh 🔇 Back (	💭 Forward 🧳 Help		CISCO
Device List 🗗 🖗 🗡	Configuration > Remote Access VPI	> Secure Desktop Manager > Host S	Scan	
Add Delete & Connect      Find:     Go     10.48.67,158.8443     A	Host Scan Create entries to be scanned on the information can be configured under	endpoint system. The scanned information Dynamic Access Policies	n will then be stored in the endpoint attribute	Access policies using the endpoint
10.62.145.45:8443 10.62.97.56:8443 192.168.11.250:444	Basic Host Scan			
Remote Access VPN 2 P	Туре	ID	Info	
Introduction     Network (Clent) Access     Identises SSL VPN Access     Add_tocal Users     Host Scan Image     Secure Desktop Manager     Global Settings     Global Settings     Global Settings     Freidign Policy     Secure Desktop Customization     Forst Scan	Endpoint ID: 1 File Path: C:\test.f	txt Cancel	c: (test. bit	Add 🕶 Edit Delete
Ervice Setup      Ereval      Remote Access VPN	Host Scan Extensions	t ver 3.6.6259.2 259.2		Configure

Além disso, uma regra adicional de avaliação de endpoint avançado é adicionada conforme mostrado na imagem.

rus			
Vendor	Product	Note	
Symantec Corp.	Norton AntiVirus 20.x	1100	A00
			Delete
Error Sile Custom Destantio			
Porce File System Protecto	20		
Force Virus Definitions Upd	ate		
if not updated in last	days		
if not updated in last	days		
if not updated in last	days		
if not updated in last	days		
if not updated in last	days		
if not updated in last	days Product	Note	Add
if not updated in last nal Firewall Vendor Microsoft Corp.	Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add
if not updated in last nal Firewall Vendor Microsoft Corp.	days Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add Delete
if not updated in last	days Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add Delete
if not updated in last nal Firewall Vendor Microsoft Corp. Firewall Action: None	days Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add Delete
if not updated in last nal Firewall Vendor Microsoft Corp. Firewall Action: None Rules	days Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add Delete
if not updated in last nal Firewall Vendor Microsoft Corp. Firewall Action: None Rules ALLOW Application CustomaA	Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add Delete
if not updated in last nal Firewall Vendor Microsoft Corp. Firewall Action: None Rules ALLOW Application CustomaA	Product Microsoft Windows Firewall 7	Note Supports firewall rules	Add Delete

Essa opção verifica a existência do Symantec Norton AntiVirus 20.x e do Microsoft Windows Firewall 7. O módulo de postura (HostScan) verifica esses valores, mas não haverá aplicação (a política de DAP não verifica isso).

#### Etapa 3. Políticas de DAP

As políticas de DAP são responsáveis por usar os dados coletados pelo HostScan como condições e aplicar atributos específicos à sessão VPN como resultado. Para criar uma política de DAP a partir do ASDM, navegue para **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** como mostrado na imagem.

Home 🖓 Configuration 📴 Monitorin	o 🔚 Save 🥝	Refresh 🔇 Back	🕑 Forward 💡 Help			CISCO
Device List ⊡ ₽ ×	Configuration	> Remote Access VPI	I > Clientless SSL VPN Access	> Dynamic Access Policies		[
Add Delete & Connect Find: Go     10.48.67.158.8443     10.48.67.229:444     10.62.145.4518443	Configure Dynan For IPsec, Any resources a us policies are ma	ic Access Policies Connect Client, Clienties er is authorized to acces tched, the ASA will enfo	s SSL VPN, and Cut-Through-Pros s. All policies in the table below ar roe the DftAccessPolicy.	cy sessions, you can configure ( e evaluated for matching criteri	dynamic access policies (DAP) that on during session establishment. V	define which network When none of the DAP
- B 192.168.11.250:444 *	ACL Priority	Name	Network ACL List	Webtype ACL List	Description	Add
Remote Access VPI   Remote Access VPI  Introduction  Network (Client) Access  Clientiess SSL VPI Access  Portal  Portal  Portal  Portal  Advanced  Advanced	0	FileNotExists FileExists DfRAccessPolicy	AQL1			Edt Delete

A primeira política (FileExists) verifica o nome do grupo de túneis que é usado pelo perfil VPN configurado (a configuração do perfil VPN foi omitida para maior clareza). Em seguida, a verificação adicional do arquivo **c:\test.txt** é executada como mostrado na imagem.

ollowing endpoint attributes are satisfied. t ID Name/Operation/Value Add exists = true Edit Delete	and the following Endpoint ID file.1	Add	owing AAA Attributes values	User has ANY of the follow
t ID Name/Operation/Value Add Edit Delete	Endpoint ID file.1	Add	Oncerting Malue	
exists = true Edit Delete	file.1		Operation/value	AAA Attribute
Delete		Edit	= TAC	cisco.tunnelgroup
		Delete		
Logical O				
				Advanced
verride those values obtained from the AAA system and the ites, AAA attributes, and group-policy hierarchy attributes (thos	ere will override t AP attributes, AA	ribute values specified I y is an aggregation of [	y Attributes ization attributes for this policy. The resulting VPN authorization DAP).	cess/Authorization Policy Configure access/authorizi group-policy hierarchy. The hat are not specified in D/
abune ACL Elters (clientless) Eurotions	AnyConne Webturge A	Access Method	Lists   Bookmarks Network ACL Filters (die	Port Forwarding L
work ACLs	Network AC			AC001
Arribe those values obtained from the AAA system a ites, AAA attributes, and group-policy hierarchy attri hyConnect AnyConnect Custom Attri ebtype ACL Filters (dientless)	AP attributes, AA AnyConne Webtype A Network AC	Access Method	Lists Bookmarks Network ACL Filters (die	group-policy hierarchy. Th that are not specified in D/ Port Forwarding L Action

Como resultado, nenhuma ação é executada com a configuração padrão para permitir a conectividade. Nenhuma ACL é usada - é fornecido acesso total à rede.

Os detalhes da verificação do arquivo são como mostrado na imagem.

🔤 Edit Endpoint	Attribute		×
Endpoint Attribute	Type: File		
	Exists	Does not exist	
Endpoint ID:	1		
	c:\test.txt		_
Last Update:	<		days
Checksum:	= –		
		Compute CRC32 Checksum	
		·	_
	ок	Cancel Help	

A segunda política (FileNotExists) é semelhante - mas esta condição de tempo é se o arquivo não

#### existir como mostrado na imagem.

efine the AAA and end	point attributes used to select th	is access policy. A policy is u	sed when a user's aut	thorization attributes match the	AAA attribute cri
ecify the logical expre	int autoute has been satisfied. It	nese attributes can be diea	ted dailing the tables be	elow anajor by expanding the r	Auvanceu opuorru
Jser has ANY of the fo	lowing AAA Attributes values	Add	Endocine TD	Name (Operation Makes	Ad
isco.tunnelgroup	= TAC	Edit	file.1	exists != true	Edi
		Delete			Dele
					Logical
Advanced					
Advanced	cy Attributes				
Advanced ess/Authorization Polic onfigure access/autho oup-policy hierarchy.	cy Attributes rization attributes for this policy. The resulting VPN authorization p	Attribute values specified h	ere will override those VP attributes, AAA att	values obtained from the AAA ributes, and group-policy hiera	system and the rchy attributes (th
Advanced ess/Authorization Polic onfigure access/autho oup-policy hierarchy. at are not specified in	cy Attributes rization attributes for this policy. The resulting VPN authorization p DAP).	Attribute values specified h	ere will override those AP attributes, AAA att	values obtained from the AAA ributes, and group-policy hiera	system and the rchy attributes (th
Advanced ess/Authorization Polic onfigure access/autho oup-policy hierarchy.' at are not specified in Port Forwardin Action	cy Attributes rization attributes for this policy. The resulting VPN authorization p DAP). o Lists Bookmarks Network ACL Filters (clien	Attribute values specified h policy is an aggregation of D Access Method nt)	ere will override those AP attributes, AAA att AnyConnect Webtype ACL Fi	values obtained from the AAA ributes, and group-policy hiera AnyConnect Cus ilters (clientless)	system and the rchy attributes (th tom Attributes Function:
Advanced ess/Authorization Polic onfigure access/autho oup-policy hierarchy. at are not specified in Port Forwardin Action	cy Attributes rization attributes for this policy. The resulting VPN authorization p DAP). a Lists Bookmarks Network ACL Filters (dien	Attribute values specified h kolicy is an aggregation of D Access Method ht)	are will override those AP attributes, AAA att AnyConnect Webtype ACL Fi Network ACLs	values obtained from the AAA ributes, and group-policy hiera AnyConnect Cus ilters (clientless)	system and the rchy attributes (th tom Attributes Functions
Advanced cess/Authorization Polic onfigure access/autho roup-policy hierarchy. nat are not specified in Port Forwardin Action	cy Attributes rization attributes for this policy. The resulting VPN authorization p DAP). a Lists Bookmarks Network ACL Filters (dien	Attribute values specified h xolicy is an aggregation of D Access Method ht)	ere will override those AP attributes, AAA att AnyConnect Webtype ACL Fi Network ACLs ACL 1	values obtained from the AAA ributes, and group-policy hiera AnyConnect Cus ilters (clientless)	system and the rchy attributes (th tom Attributes Function:

O resultado tem a ACL1 da lista de acesso configurada. Isso é aplicado a usuários VPN não compatíveis com o fornecimento de acesso limitado à rede.

As duas políticas de DAP enviam o acesso **do AnyConnect Client**, conforme mostrado na imagem.

Action	Netv	work ACL Filters (client)		Webtype ACL Filters	(clientless)	Function
Port Forwa	arding Lists	Bookmarks	Access Method	AnyConnect	AnyConnect Cu	stom Attributes
	AnyConnect	Client				
	Web-Portal					
	Both default	-Web-Portal				
	DUUI-UCIQUI					
	Oburbeiduit					

#### ISE

O ISE é usado para autenticação de usuário. Somente o dispositivo de rede (ASA) e o nome de usuário correto (cisco) devem ser configurados. Esta parte não é abrangida por este artigo.

### Verificar

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

#### Provisionamento de CSD e AnyConnect

Inicialmente, o usuário não é provisionado com o cliente AnyConnect. O usuário também não está em conformidade com a política (o **arquivo c:\test.txt** não existe). Digite <u>https://10.62.145.45</u> e o usuário será imediatamente redirecionado para a instalação do CSD, como mostrado na imagem.

Cisco	Secure Desktop
🙆 WebLaunch	Using ActiveX for Installation Launching Cisco Secure Desktop.
Platform Detection	If the software does not start properly, <u>Click here</u> to
- ActiveX	end the session cleanly.
- Java Detection	
🔄 - Sun Java	
- WebLaunch	
Access Denied	
- Critical Error	
Success	Download
- Access Denied	

Isso pode ser feito com Java ou AtiveX. Quando o CSD é instalado, ele é relatado como mostrado na imagem.

Cisco	Secure Desktop
WebLaunch  Platform Detection	<b>System Validated</b> Cisco Secure Desktop successfully validated your system. Success. Reloading. Please wait
<ul> <li>ActiveX</li> <li>Java Detection</li> <li>Sun Java</li> <li>WebLaunch</li> </ul>	
<ul> <li>Access Denied</li> <li>- Critical Error</li> <li>- Success</li> </ul>	Download
Access Denied	

Em seguida, o usuário é redirecionado para autenticação, conforme mostrado na imagem.

Login
Please enter your username and password.
GROUP: TAC  USERNAME: PASSWORD: Login

Se bem-sucedido, o AnyConnect e o perfil configurado são implantados - novamente, o AtiveX ou o Java podem ser usados como mostrado na imagem.

cisco AnyC	connect Secure Mobility Client			
NebLaunch	Using ActiveX for Installation			
	Launching Cisco AnyConnect Secure Mobility Client.			
<ul> <li>Platform</li> <li>Detection</li> </ul>	If the software does not start properly, <u>Click here</u> to end the session cleanly.			
- ActiveX	AnyConnect Secure Mobility Client Downloader			
- Java Detection	Downloading AnyConnect Secure Mobility Client 4.0.00051.			
🔄 - Java	Please wait Time Left: 9 secs (672.0 KB of 3.34 MB copied)			
- Download				
Connected	Cancel			
	Help Download			

E a conexão VPN é estabelecida conforme mostrado na imagem.

cisco AnyC				
WebLaunch  Platform Detection	Using ActiveX for Installation Launching Cisco AnyConnect Secure Mobility Client. If the software does not start properly, <u>Click here</u> to end			
- ActiveX	AnyConnect Secure Mobility Client Downloader			
<ul> <li>Java Detection</li> <li>Java</li> <li>Jownload</li> </ul>	Please wait while the VPN connection is established	A T		
Connected	Help Download			

A primeira etapa do AnyConnect é executar verificações de postura (HostScan) e enviar os relatórios ao ASA, como mostrado na imagem.

🕥 Cisco AnyConnect Secure Mobility Client 📃 🖃 💌				
	VPN: Posture Assessment: Initiating asav	▼ [	Connect	
Limited Access	s - DNS Failure			
<b>\$</b> (i)				altalta cisco

Em seguida, o AnyConnect autentica e conclui a sessão de VPN.

### Sessão AnyConnect VPN com postura - Não compatível

Quando você estabelece uma nova sessão de VPN com o AnyConnect, o primeiro passo é a postura (HostScan), conforme apresentada na captura de tela anterior. Em seguida, a autenticação ocorre e a sessão VPN é estabelecida conforme mostrado nas imagens.

🕙 Cisco	AnyConnect	: 10.62.145.45		
	Please enter	your username and password.		
_	Group:	TAC		
	Username:	cisco		
	Password:	******		
		OK Cancel		
N Cisco AnyConnect Secure Mobility Client				
VPN:         Please enter your username and password.         asav         Connect				
Limite	ed Access - DN	NS Failure		
¢ (	<b>i</b>		altalta cisco	

O ASA relata que o relatório do HostScan é recebido:

%ASA-7-716603: Received 4 KB Hostscan data from IP <10.61.87.251>
Em seguida, executa a autenticação do usuário:

\*ASA-6-113004: AAA user authentication successful : server = 10.62.145.42 : user = cisco E inicia a autorização para essa sessão VPN. Quando você tem "debug dap trace 255" habilitado, as informações sobre a existência do arquivo c:\test.txt são retornadas:

```
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.file["1"].exists="false"
DAP_TRACE: endpoint.file["1"].exists = "false"
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.file["1"].path="c:\test.txt"
DAP_TRACE: endpoint.file["1"].path = "c:\\test.txt"
Além disso, informações sobre o Firewall do Microsoft Windows:
```

```
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].exists="false"
DAP_TRACE: endpoint.fw["MSWindowsFW"].exists = "false"
DAP_TRACE[128]:
dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].description="Microsoft Windows
Firewall"
DAP_TRACE: endpoint.fw["MSWindowsFW"].description = "Microsoft Windows Firewall"
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].version="7"
DAP_TRACE: endpoint.fw["MSWindowsFW"].version = "7"
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].enabled="failed"
DAP_TRACE: endpoint.fw["MSWindowsFW"].enabled = "failed"
```

E o Symantec AntiVirus (de acordo com as regras de avaliação de endpoint avançado do HostScan configuradas anteriormente).

Como resultado, a política de DAP é combinada:

#### DAP\_TRACE: Username: cisco, Selected DAPs: ,FileNotExists

Essa política força o uso do AnyConnect e também aplica a ACL1 da lista de acesso que fornece acesso restrito à rede para o usuário (não compatível com a política corporativa):

DAP\_TRACE: The DAP policy contains the following attributes for user: cisco DAP\_TRACE:-----

DAP\_IRACE: DAP\_TRACE:1: tunnel-protocol = svc

DAP\_TRACE:2: svc ask = ask: no, dflt: svc DAP\_TRACE:3: action = continue DAP\_TRACE:4: network-acl = ACL1

Os registros também apresentam extensões ACIDEX que podem ser usadas pela política de DAP (ou mesmo transmitidas em Solicitações de RADIUS ao ISE e são usadas em Regras de Autorização como condições):

endpoint.anyconnect.clientversion = "4.0.00051"; endpoint.anyconnect.platform = "win"; endpoint.anyconnect.devicetype = "innotek GmbH VirtualBox"; endpoint.anyconnect.platformversion = "6.1.7600 "; endpoint.anyconnect.deviceuniqueid = "A1EDD2F14F17803779EB42C281C98DD892F7D34239AECDBB3FEA69D6567B2591"; endpoint.anyconnect.macaddress["0"] = "08-00-27-7f-5f-64"; endpoint.anyconnect.useragent = "AnyConnect Windows 4.0.00051"; Como resultado, a sessão VPN está ativa, mas com acesso restrito à rede:

#### ASAv2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

```
Username : cisco
                                                                                Index
                                                                                                          : 4
                                                                                Public IP : 10.61.87.251
Assigned IP : 192.168.1.10
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
                         : AnyConnect Premium
License
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Hashing
Bytes Tx : 11
The second seco
                                                                              Bytes Rx : 14709
                        : 11432
                                                                                                        : 146
                                                                               Pkts Rx
Pkts Tx Drop : 0
                                                                                Pkts Rx Drop : 0
Group Policy : AllProtocols
                                                                               Tunnel Group : TAC
Login Time : 11:58:54 UTC Fri Dec 26 2014
Duration : 0h:07m:54s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                                                              VLAN : none
Audt Sess ID : 0add006400004000549d4d7e
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
  Tunnel ID : 4.1
  Public IP
                            : 10.61.87.251
                                                                               Hashing : none
  Encryption : none
  TCP Src Port : 49514
                                                                                TCP Dst Port : 443
  Auth Mode : userPassword
  Idle Time Out: 30 Minutes
                                                                         Idle TO Left : 22 Minutes
  Client OS : win
  Client OS Ver: 6.1.7600
  Client Type : AnyConnect
  Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
                                                                               Bytes Rx : 764
  Bytes Tx : 5716
  Pkts Tx
                           : 4
                                                                                 Pkts Rx
                                                                                                            : 1
  Pkts Tx Drop : 0
                                                                                 Pkts Rx Drop : 0
SSL-Tunnel:
  Tunnel ID
                             : 4.2
 Assigned IP : 192.168.1.10Public IP : 10.61.87.251Encryption : RC4Hashing : SHA1Encapsulation: TLSv1.0TCP Src Port : 49517TCD Dat Datt : 442Puth Made : unsuppresented
  TCP Dst Port : 443
                                                                              Auth Mode : userPassword
  Idle Time Out: 30 Minutes
                                                                               Idle TO Left : 22 Minutes
  Client OS : Windows
  Client Type : SSL VPN Client
  Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
                                                                                 Bytes Rx : 2760
  Bytes Tx : 5716
  Pkts Tx
                          : 4
                                                                                 Pkts Rx
                                                                                                            : 12
  Pkts Tx Drop : 0
                                                                                Pkts Rx Drop : 0
  Filter Name : ACL1
DTLS-Tunnel:
  Tunnel ID
                             : 4.3
  Assigned IP : 192.168.1.10
                                                                               Public IP : 10.61.87.251
```

```
Encryption : AES128 Hashing -
Encapsulation: DTLSv1.0 UDP Src Port : 52749
Auth Mode : userPa
                                     Auth Mode : userPassword
Idle Time Out: 30 Minutes
                                     Idle TO Left : 24 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx
                                      Bytes Rx : 11185
             : 0
Pkts Tx
            : 0
                                     Pkts Rx
                                                   : 133
Pkts Tx Drop : 0
                                     Pkts Rx Drop : 0
Filter Name : ACL1
ASAv2# show access-list ACL1
access-list ACL1; 1 elements; name hash: 0xe535f5fe
access-list ACL1 line 1 extended permit ip any host 1.1.1.1 (hitcnt=0) 0xe6492cbf
```

O histórico do AnyConnect mostra as etapas detalhadas do processo de postura:

```
12:57:47 Contacting 10.62.145.45.
12:58:01 Posture Assessment: Required for access
12:58:01 Posture Assessment: Checking for updates...
12:58:02 Posture Assessment: Updating...
12:58:03 Posture Assessment: Initiating...
12:58:13 Posture Assessment: Active
12:58:13 Posture Assessment: Initiating...
12:58:37User credentials entered.12:58:43Establishing VPN session...
12:58:43 The AnyConnect Downloader is performing update checks...
12:58:43 Checking for profile updates...
12:58:43 Checking for product updates...
12:58:43 Checking for customization updates...
12:58:43 Performing any required updates...
12:58:43The AnyConnect Downloader updates have been completed.12:58:43Establishing VPN session...
12:58:43 Establishing VPN - Initiating connection...
12:58:48 Establishing VPN - Examining system...
12:58:48 Establishing VPN - Activating VPN adapter...
12:58:52 Establishing VPN - Configuring system...
12:58:52 Establishing VPN...
12:58:52 Connected to 10.62.145.45.
```

#### Sessão AnyConnect VPN com postura - Compatível

Depois de criar o arquivo c:\test.txt, o fluxo é semelhante. Quando uma nova sessão do AnyConnect é iniciada, os registros indicam a existência do arquivo:

%ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute endpoint.file["1"].exists="true" %ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute endpoint.file["1"].path="c:\test.txt" Como resultado, outra política de DAP é usada:

DAP\_TRACE: Username: cisco, **selected DAPs: ,FileExists** A política não impõe nenhuma ACL como a restrição para o tráfego de rede.

E a sessão está ativa sem qualquer ACL (acesso total à rede):

#### ASAv2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

```
Index : 5
Public IP : 10.61.87.251
          : cisco
Username
Assigned IP : 192.168.1.10
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
          : AnyConnect Premium
License
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing
           : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx
           : 11432
                                  Bytes Rx : 6298
Pkts Tx
          : 8
                                   Pkts Rx : 38
Pkts Tx Drop : 0
                                  Pkts Rx Drop : 0
Group Policy : AllProtocols
                                  Tunnel Group : TAC
Login Time : 12:10:28 UTC Fri Dec 26 2014
          : 0h:00m:17s
Duration
Inactivity : 0h:00m:00s
VLAN Mapping : N/A
                                   VLAN
                                          : none
Audt Sess ID : 0add006400005000549d5034
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 5.1
Public IP : 10.61.87.251
Encryption : none
                                  Hashing : none
TCP Src Port : 49549
                                  TCP Dst Port : 443
Auth Mode : userPassword
                              Idle TO Left : 29 Minutes
Idle Time Out: 30 Minutes
Client OS : win
Client OS Ver: 6.1.7600
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx : 5716
                                   Bytes Rx : 764
           : 4
Pkts Tx
                                               : 1
                                    Pkts Rx
Pkts Tx Drop : 0
                                    Pkts Rx Drop : 0
SSL-Tunnel:
Tunnel ID : 5.2
                              Public IP : 10.61.87.251
Hashing : SHA1
Assigned IP : 192.168.1.10
Encryption : RC4
Encapsulation: TLSv1.0
                                  TCP Src Port : 49552
                                  Auth Mode : userPassword
TCP Dst Port : 443
                           Idle TO Left : 29 Minutes
Idle Time Out: 30 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx : 5716
                                   Bytes Rx : 1345
           : 4
                                              : 6
Pkts Tx
                                    Pkts Rx
Pkts Tx Drop : 0
                                    Pkts Rx Drop : 0
DTLS-Tunnel:
Tunnel ID
            : 5.3
                                Public IP : 10.61.87.251
Hashing : SHA1
Assigned IP : 192.168.1.10
Encryption : AES128
Encapsulation: DTLSv1.0
                                  UDP Src Port : 54417
UDP Dst Port : 443
                                  Auth Mode : userPassword
                               Idle TO Left : 30 Minutes
Idle Time Out: 30 Minutes
Client OS : Windows
```

Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051 Bytes Tx : 0 Bytes Rx : 4189 Pkts Tx 0 Pkts Rx : 31 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Além disso, o Anyconnect relata que o HostScan está ocioso e aguardando a próxima solicitação de verificação:

13:10:15 Hostscan state idle 13:10:15 Hostscan is waiting for the next scan

Note: Para reavaliação, é aconselhável usar um módulo de postura integrado ao ISE.

### Troubleshoot

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

### DART do AnyConnect

O AnyConnect fornece diagnósticos conforme mostrado na imagem.

0	🕥 Cisco AnyConnect Secure Mobility Client					x		
	ار، د	ı.ılı. Isco	AnyC	onnect Se	cure Mobil	ity Client	(	D
	Virtual Private Network (VPN)					Diagnostics		
	f	Preferences	Statistics	Route Details Firewa	Message History			
	<ul> <li>13:45:00 Contacting asav.</li> <li>13:45:09 Connection attempt has failed.</li> <li>13:45:13 Contacting 10.62.145.45.</li> <li>13:45:21 Posture Assessment: Required for access</li> <li>13:45:21 Posture Assessment: Checking for updates</li> <li>13:45:22 Posture Assessment: Initiating</li> <li>13:45:31 Posture Assessment: Active</li> <li>13:45:31 Posture Assessment: Initiating</li> <li>13:45:32 User credentials entered.</li> <li>13:45:41 Hostscan state idle</li> <li>13:45:42 Establishing VPN session</li> <li>13:45:42 The AnyConnect Downloader is performing update checks</li> <li>13:45:42 Checking for profile updates</li> <li>13:45:42 Checking for customization updates</li> <li>13:45:42 Performing any required updates</li> <li>13:45:42 The AnyConnect Downloader shave been completed.</li> <li>13:45:42 Establishing VPN session</li> <li>13:45:42 Establishing VPN session</li> <li>13:45:42 Establishing VPN session</li> <li>13:45:42 Establishing VPN session</li> <li>13:45:43 Establishing VPN session</li> <li>13:45:44 Establishing VPN session</li> <li>13:45:45 Establishing VPN session</li> <li>13:45:47 Establishing VPN session</li> <li>13:45:47 Establishing VPN session</li> <li>13:45:47 Establishing VPN session</li> <li>13:45:47 Establishing VPN session</li> <li>13:45:52 Establishing VPN session</li> </ul>							
							Clear	

Que reúne e salva todos os logs do AnyConnect em um arquivo zip na área de trabalho. Esse arquivo zip inclui os registros no Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

Isso fornece informações sobre o ASA e solicita que o HostScan reúna dados:

 Date
 : 12/26/2014

 Time
 : 12:58:01

 Type
 : Information

 Source
 : acvpnui

Description : Function: ConnectMgr::processResponseString
File: .\ConnectMgr.cpp
Line: 10286
Invoked Function: ConnectMgr::processResponseString
Return Code: 0 (0x0000000)
Description: HostScan request detected.

Em seguida, vários outros registros revelam que o CSD está instalado. Este é o exemplo de um provisionamento de CSD e conexão subsequente do AnyConnect junto com a postura:

CSD detected, launching CSD Posture Assessment: Required for access Gathering CSD version information. Posture Assessment: Checking for updates... CSD version file located Downloading and launching CSD Posture Assessment: Updating... Downloading CSD update CSD Stub located Posture Assessment: Initiating... Launching CSD Initializing CSD Performing CSD prelogin verification. CSD prelogin verification finished with return code 0 Starting CSD system scan. CSD successfully launched Posture Assessment: Active CSD launched, continuing until token is validated. Posture Assessment: Initiating...

Checking CSD token for validity Waiting for CSD token validity result CSD token validity check completed CSD Token is now valid CSD Token validated successfully Authentication succeeded Establishing VPN session...

A comunicação entre o ASA e o AnyConnect é otimizada, as solicitações do ASA para executar apenas verificações específicas - o AnyConnect faz o download de dados adicionais para poder realizar isso (por exemplo, verificação específica de antivírus).

Ao abrir o caso com o TAC, anexe os logs do Dart junto com "show tech" e "debug dap trace 255" do ASA.

### Informações Relacionadas

- <u>Configurando a verificação de host e o módulo de postura Guia do administrador do Cisco</u> <u>AnyConnect Secure Mobility Client</u>
- Serviços de postura no Guia de configuração do Cisco ISE
- Guia do administrador do Cisco ISE 1.3
- <u>Suporte Técnico e Documentação Cisco Systems</u>