Configuración de AnyConnect Secure Mobility Client con túneles divididos en ASA

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Antecedentes** Información sobre la licencia de AnyConnect Configurar Diagrama de la red Asistente de configuración de ASDM de AnyConnect Configuración del túnel dividido Descarga e instalación de AnyConnect Client Implementación web Implementación independiente Configuración de CLI Verificación Troubleshoot Instalación de la DART Ejecución de la DART Información Relacionada

Introducción

Este documento describe cómo configurar Cisco AnyConnect Secure Mobility Client a través de Cisco Adaptive Security Device Manager (ASDM) en Cisco Adaptive Security Appliance (ASA) que ejecuta la versión de software 9.3(2).

Prerequisites

Requirements

El paquete de implementación web de Cisco AnyConnect Secure Mobility Client debe descargarse en el escritorio local donde está presente el acceso de ASDM a ASA. Para descargar el paquete del cliente, consulte la página web de <u>Cisco AnyConnect Secure Mobility Client</u>. Los paquetes de implementación web para diversos sistemas operativos (SO) se pueden cargar en ASA al mismo tiempo.

Estos son los nombres de archivo de implementación web para los diversos SO:

• SO Microsoft Windows: AnyConnect-win-<version>-k9.pkg

- SO Macintosh (MAC): AnyConnect-macosx-i386-<version>-k9.pkg
- SO Linux: AnyConnect-linux-<version>-k9.pkg

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA versión 9.3(2)
- ASDM versión 7.3(1)101
- AnyConnect versión 3.1

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. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Este documento proporciona detalles paso a paso sobre cómo utilizar el asistente de configuración de Cisco AnyConnect mediante ASDM para configurar AnyConnect Client y habilitar el túnel dividido.

El túnel dividido se utiliza en situaciones en las que solo se debe tunelizar tráfico específico, en lugar de situaciones en las que todo el tráfico generado por la máquina del cliente fluye a través de la VPN cuando se conecta. El uso del asistente de configuración de AnyConnect generará de manera predeterminada una configuración de *túnel completo* en ASA. El túnel dividido debe configurarse por separado, como se explica con más detalle en la sección de este documento.

En este ejemplo de configuración, la intención es enviar tráfico para la subred 10.10.10.0/24, que es la subred de la LAN detrás de ASA, a través del túnel VPN; todo el resto del tráfico de la máquina del cliente se reenvía a través de su propio circuito de Internet.

Información sobre la licencia de AnyConnect

Estos son algunos enlaces a información útil sobre las licencias de Cisco AnyConnect Secure Mobility Client:

- Consulte el documento <u>Características, licencias y SO de AnyConnect Secure Mobility Client,</u> versión 3.1 para determinar las licencias necesarias para AnyConnect Secure Mobility Client y las características relacionadas.
- Consulte la <u>Guía de pedidos de Cisco AnyConnect</u> para obtener información sobre las licencias de AnyConnect Apex y Plus.
- Consulte el documento ¿Qué licencia de ASA se necesita para las conexiones de telefonía IP y VPN móvil? para obtener información sobre los requisitos de licencia adicionales para las

conexiones de telefonía IP y móviles.

Configurar

En esta sección se describe cómo configurar Cisco AnyConnect Secure Mobility Client en ASA.

Diagrama de la red

Esta es la topología que se usa para los ejemplos en este documento:



Asistente de configuración de ASDM de AnyConnect

El asistente de configuración de AnyConnect se puede utilizar para configurar AnyConnect Secure Mobility Client. Asegúrese de que se haya cargado un paquete de AnyConnect Client en la memoria flash o el disco del firewall de ASA antes de continuar.

Complete estos pasos para configurar AnyConnect Secure Mobility Client mediante el asistente de configuración:

1. Inicie sesión en ASDM, inicie el Asistente de configuración y haga clic en Siguiente:

Cisco ASDM 7.3 fr	or A	SA - 10.106.44.21		-		COLUMN TWO	and second	Marriell	
<u>File View T</u> ools	Wi	zards Window Help							
🌀 Home 🗞 Config		Startup Wizard	C	🔵 Forwa	rd 🖁	💡 ныр			
Device List		VPN Wizards		<u>S</u> ite-to	o-site	VPN Wizard			
🗣 Add 📋 Delete 💡		\underline{H} igh Availability and Scalability Wizard		<u>A</u> nyCo	nnec	t VPN Wizard		nboard	
Find:		Unified Communication Wizard		<u>C</u> lient	ess S	SL VPN Wizard			
一基 10.106.44.3 一 設 10.106 .44.21		ASDM Identity \underline{C} ertificate Wizard		<u>I</u> Psec (IKEvd	1) Remote Access VP	N Wizard		
		Packet Capture Wizard				Host Name:	EdgeASA-4		
						ASA Version:	9.3(2)	Device Uptime:	0d 16h 15m 5s
						ASDM Version :	7.3(1)101	Device Type:	ASA 5525
						Firewall Mode:	Routed	Context Mode :	Single
						Environment Status :	🕈 ОК	Total Flash:	8192 MB

2. Ingrese el *nombre del perfil de conexión*, elija la interfaz en la que finalizará la VPN en el menú desplegable *Interfaz de acceso a la VPN* y haga clic en **Siguiente**:

anyConnect VPN Connect	ection Setup Wizard			X		
Steps	Connection Profile Identific	ation				
1. Introduction	This step allows you to configure a Connection Profile Name and the Interface the remote access users will					
2. Connection Profile Identification	access for VPN connection	s.				
3. VPN Protocols	Connection Profile Name:	SSLClient				
4. Client Images	VPN Access Interface:	outside	•			
5. Authentication Meth						

3. Marque la casilla de verificación SSL para habilitar la capa de sockets seguros (SSL). El certificado del dispositivo puede ser un certificado emitido por una autoridad de certificación (CA) de confianza (como Verisign o Entrust) o un certificado firmado automáticamente. Si el certificado ya está instalado en ASA, se puede elegir en el menú desplegable. Nota: Este certificado es el certificado del servidor que se proporcionará. Si no hay ningún certificado instalado actualmente en ASA y se debe generar un certificado firmado automáticamente, haga clic en Administrar.Para instalar un certificado de terceros, siga los pasos que se describen en el documento <u>Certificados de proveedores de terceros para la instalación manual de ASA 8.x para usar con el ejemplo de configuración de WebVPN</u> de Cisco.

	AnyConnect VPN Conn	ection Setup Wizard
ſ	Steps	VPN Protocols
l	1. Introduction	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol
	2. Connection Profile Identification	or protocols you would like this connection profile to support.
	3. VPN Protocols	SSL SSL
	4. Client Images	IPsec
	5. Authentication Meth	Device Certificate
	 Client Address Assignment 	Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.
	7. Network Name Resolution Servers	Device Certificate: None Manage
	8. NAT Exempt	
1		

4. Haga clic en Agregar:

fanage Ider	ntity Certificat	tes				
Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
						Show Details
						Delete
						Export
						Install

5. Escriba un nombre adecuado en el campo *Nombre del punto de confianza* y haga clic en el botón de radio **Agregar un nuevo certificado de identidad**. Si no hay pares de claves Rivest-Shamir-Addleman (RSA) presentes en el dispositivo, haga clic en **Nuevo** para generar uno:

🔄 Add Identity Certificate		X
Trustpoint Name:	SelfsignedCert	
Import the identity certific	ate from a file (PKCS12 format with Cert	ificate(s)+Private Key):
Decryption Passphrase:		
File to Import From:		Browse
Add a new identity certific	cate:	
Key Pair:	<default-rsa-key> ▼</default-rsa-key>	Show New
Certificate Subject DN:	CN=anyconnect.cisco.com	Select
Generate self-signed	certificate	
🗌 Act as local certif	ficate authority and issue dynamic certifica	ates to TLS-Proxy
		Advanced
Add Cert	tificate Cancel H	Help

6. Haga clic en el botón de radio **Usar nombre de par de claves predeterminado** o haga clic en el botón de radio **Introducir nuevo nombre de par de claves** e introduzca un nuevo nombre. Seleccione el tamaño de las claves y haga clic en **Generar ahora**:

E	Add Key F	Pair	X
	Кеу Туре:	RSA	© ECDSA
	Name:	🔘 Use default key pair name	
		Enter new key pair name:	ssicert
	Size:	2048 🗸	
	Usage:	 General purpose 	🔘 Special
		Generate Now Cancel	Help
		Generate Now Cancel	Help

7. Después de generar el par de claves RSA, elija la clave y marque la casilla de verificación **Generar certificado firmado automáticamente**. Ingrese el nombre de dominio (DN) del asunto deseado en el campo *DN del asunto del certificado* y, luego, haga clic en **Agregar certificado**:

Add Identity Certificate	×
Trustpoint Name:	SelfsignedCert
Import the identity certific	cate from a file (PKCS12 format with Certificate(s)+Private Key):
Decryption Passphrase:	
File to Import From:	Browse
Add a new identity certification	cate:
Key Pair:	ssicert Show New
Certificate Subject DN:	CN=anyconnect.cisco.com Select
Generate self-signed	certificate
📃 Act as local certi	ficate authority and issue dynamic certificates to TLS-Proxy
	Advanced
Add Cer	tificate Cancel Help

8. Una vez completada la inscripción, haga clic en Aceptar, Aceptar y, luego, en Siguiente:

🧧 Ar	nyConnect VPN Co	onnection Set	up Wizard				a
Ste	[Manage Ider	ntity Certificat	es				X
1. 2.	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage	Public Key Type	Add
з.	hostname	hostname	16:39:40 M	SelfsignedCert	Gener	RSA (2048 bits)	Show Details
4. 5.							Export
6.							Install
7.	Eind:	U	00	Match Case			
8. 9.	Get your Cis Entrust, Entr	ument co ASA secur rust offers Cis	ity appliance u co customers a	p and running quickly with a special promotional price	an SSL A for certit	dvantage digital cer ficates and trial cert	tificate from ificates for testing.
10	Using a pre	viously saved	certificate sign	ing request, <u>enroll with Er</u>	ntrust.	s	
			Oł	Cancel		Help	

9. Haga clic en Agregar para agregar la imagen de AnyConnect Client (archivo .pkg) desde la

PC o la memoria flash. Haga clic en **Examinar la memoria flash** para agregar la imagen de la unidad de memoria flash o haga clic en **Cargar** para agregar la imagen de la máquina host directamente:



Browse Flash	Regile systems in			x
Folders	Files			
l ⊡• <mark> </mark>	FileName	Size (Date	
🚊 🛄 crypto_archive	anyconnect-win-3.1.05152-k9.pkg	35,167,	12/17/	
	anyconnect-win-3.1.06073-k9.pkg	38,048,	01/02/	
in in in in in iteration in the interview of the intervie	asa932-smp-k8.bin	63,479,	01/02/	
		10.004	11/00/	

10. Una vez que se agrega la imagen, haga clic en Siguiente:

🕈 Add 🗹 Replace 前 Delete 🛧 🎸					
Image	Regular expression to match user-agent				
disk0:/anyconnect-win-3.1.06073-k9.pkg					
You can download AnyConnect Client packages from <u>Cisco</u> <u>here</u> ,	<u>o</u> by searching 'AnyConnect VPN Client' or <u>click</u>				
< <u>B</u> ack <u>N</u> ext >	Cancel Help				

11. La autenticación de usuario se puede completar a través de los grupos de servidores de autenticación, autorización y auditoría (AAA). Si los usuarios ya están configurados, elija LOCAL y haga clic en Siguiente. Nota: En este ejemplo, se configura la autenticación LOCAL, lo que significa que la base de datos de usuarios local en ASA se utilizará para la autenticación.

AnyConnect VPN Co	nnection Setup Wizard	
Steps 1. Introduction	Authentication Methods This step lets you specify the location of the authentication server.	_
2. Connection Profile Identification	You can click on the "New" button to create a new server group.	
 VPN Protocols Client Images 	Local User Database Details	
5. Authentication Methods	cisco	
6. Client Address Assignment	User to be Added User1	
 Network Name Resolution Servers 	Password:	
8. NAT Exempt	Confirm Password: ••••	
9. AnyConnect Client Deployment		
10. Summary		
	< Back Next > Cancel Help]

12. Se debe configurar el conjunto de direcciones para el cliente VPN. Si ya hay uno configurado, selecciónelo en el menú desplegable. Si no lo hay, haga clic en **Nuevo** para configurar uno nuevo. Haga clic en **Siguiente** una vez completado:

J. VENTER OUCCOR				
4. Client Images	IP v4 A	ddress Pool 🛛 IP v6 Address	s Pool	
5. Authentication Meth	Address Poo	l: [Select 🔻 Nev	H	
6. Client Address Assignment	Details of	add IPv4 Pool		×
7. Network Name Resolution Servers		Name:	SSL-Pool	
3. NAT Exempt		Starting IP Address:	10.10.11.1	_
 AnyConnect Client Deployment 		Ending IP Address:	10.10.11.20	
10. Summary		Subnet Mask:	255.255.255.0	•
		ОК	Cancel	Help

13. Ingrese los servidores y los DN del sistema de nombres de dominio (DNS) en los campos *DNS* y *Nombre de dominio*, y luego haga clic en **Siguiente**:

Steps	Network Name R	esolution Servers	
1. Introduction	This step lets you	u specify how domain names are resolved for the remote user wh	en accessing the internal
2. Connection Profile Identification	network.		
3 VPN Protocols	DNS Servers:	10.10.10.23]
4. Client Images	WINS Servers:]
5. Authentication Meth	Domain Name:	Cisco.com]

14. En esta situación, el objetivo es restringir el acceso a través de la VPN a la red 10.10.10.0/24 configurada como la subred *interna* (o LAN) detrás de ASA. El tráfico entre el cliente y la subred interna debe estar exento de cualquier traducción dinámica de direcciones de red (NAT).

Marque la casilla **Exento de tráfico de VPN de traducción de direcciones de red** y configure las interfaces LAN y WAN que se utilizarán para la exención.

 3. VPN Protocols 4. Client Images 5. Authentication Methor 6. Client Address 	
 4. Client Images Inside Interface: Inside 5. Authentication Metho 6. Client Address Inside Interface: Inside Local Network is the network address(es) of the internal network that client can access. 	
 5. Authentication Metho 6. Client Address 	
6. Client Address	
Assignment Local Network: any	
7. Network Name Resolution Servers	-
8. NAT Exempt The traffic between AnyConnect client and internal network will be exempt from network address translation.	
9. AnyConnect Client	

15. Elija las redes locales que deben estar exentas:

A1					Fillerick	lea
Name	IP Address	Netmask	Description	Obje	ct NAT Addr	r
-IPv4 Network	Objects					
- 🏈 any						
모음 Inside.	10.10.10.0	255.255.255.0				
- 🖳 outsid.	10.106.44.0	255.255.255.0				
- 🚅 10.0.0	.0 10.0.0.0	255.0.0.0				
🚅 10.1.2	10.1.232.192	255.255.255				
- IPv4 Network	Object Groups					
🕀 🗱 ANY						
🕀 🎆 OBJ_L.						
🕀 🎆 OBJ_S.						
🗄 Interfaces						
- 🔤 Inside						
🔤 outside						
	2					
Selected Local N	etwork					
Selected Local N Local Netwo	etwork ork ->	ietwork/24				
Selected Local N Local Netwo	etwork ork ->	network/24		OK	Can	nce
Selected Local N Local Netwo	etwork ork -> Inside-r	etwork/24		OK	Can	hce
Selected Local N Local Netwo	etwork ork -> Inside-r	network/24 k is the network addr	ess(es) of the internal net	OK work that client	Can	nce
Selected Local N Local Netwo Authentication Mether Client Address	nx Local Network	hetwork/24 k is the network addr	ess(es) of the internal net	OK work that client	Can	
Selected Local N Local Netwo Authentication Met Client Address Assignment	n Local Network	k is the network addr	ess(es) of the internal net	OK work that client	Can	hCe
Selected Local N Local Netwo Authentication Meth Client Address Assignment Network Name Resolution Servers	n Local Network	k is the network addr k: 10.10.10.0/24	ess(es) of the internal net	OK work that client	Can	nce
Selected Local N Local Netwo Authentication Met Client Address Assignment Network Name Resolution Servers NAT Exempt	etwork ork -> Inside-r Local Networ can access. Local Networ The traffic be from network	k is the network addr k: 10.10.10.0/24	ess(es) of the internal net	OK work that client	Can	1CE

16. Haga clic en Siguiente, Siguiente y, luego, en Finalizar.

La configuración de AnyConnect Client ahora está completa. Sin embargo, cuando configura AnyConnect mediante el asistente de configuración, configura la política de *Túnel dividido*como **Túnel completo** de manera predeterminada. Para tunelizar solo tráfico específico, se debe implementar el *túnel dividido*.

Nota: Si no se configura el túnel dividido, la política de túnel dividido se heredará de la política de grupo predeterminada (DfltGrpPolicy), que se establece de manera predeterminada en **Túnel completo.** Esto significa que una vez que el cliente está conectado a través de la VPN, todo el tráfico (incluido el tráfico a la web) se envía a través del túnel.

Solo el tráfico destinado a la dirección IP de la WAN (o *externa)* de ASA omitirá el túnel en la máquina del cliente. Esto se puede ver en el resultado del comando **route print** en máquinas con Microsoft Windows.

Configuración del túnel dividido

El túnel dividido es una característica que puede utilizar para definir el tráfico para las subredes o los hosts que deben cifrarse. Esto implica la configuración de una lista de control de acceso (ACL) que se asociará con esta función. El tráfico para las subredes o los hosts que se define en esta ACL se cifrará en el túnel desde el extremo del cliente y las rutas para estas subredes se instalarán en la tabla de enrutamiento de la PC.

Complete estos pasos para pasar de la configuración de *Túnel completo* a la configuración de *Túnel dividido*:

1. Vaya a Configuración > VPN de acceso remoto > Políticas de grupo:



 Haga clic en Editar y utilice el árbol de navegación para navegar a Avanzado > Túnel dividido. Desmarque la casilla de verificación Heredar en la sección *Política* y seleccione Lista de redes de túneles a continuación en el menú desplegable:

Conoral	The VPN client makes calit transling de	cicione on the	basis of a potwork list that can be specific
Servers	The vent cheric makes spir cumening up		s basis of a network list that can be specifie
Advanced	DNS Names:	🗸 Inherit	
Browser Proxy AnyConnect Client	Send All DNS Lookups Through Tunnel	: 📝 Inherit	🔘 Yes 🔘 No
- 、 /	Policy:	📃 Inherit	Tunnel Network List Below
	Network List:	📝 Inherit	

3. Desmarque la casilla de verificación Heredar en la sección Lista de redes y haga clic en

Administrar para seleccionar la ACL que especifica las LAN a las que el cliente necesita acceder:

Nstwork List:	🔲 Inherit	inside_access_in	•	Manage
Pressing this button to set up split exit Set up Split Exclusion for Web Sec.	ision for Web S rity	curity proxies.		

4. Haga clic en ACL estándar, Agregar, Agregar ACL y, luego, en Nombre de ACL.

General Servers Advanced	The VPN	lient makes split tunneling decisions on the basis of a network list that can be specif ACL Manager
Browser Proxy AnyConnect Client II-IPsec(IKEv1) Client	Send	Standard ACL Extended ACL ◆ Add ~ I Edit I Delete ↑ ↓ ↓ ■ ■ ■
	Policy	No Address Action Description
	Pressi	Add ACL
	Set	ACL Name: Split-ACL
	Inte	

5. Haga clic en Agregar ACE para agregar la regla:

ACL Mar	lager			
Standard	ACL Extended ACL			
🗣 Add 🖣	🖻 Edit 📋 Delete 🛧	€ % % @	L +	
No	Address	Action	Description	
Split-A	ICL			
🔤 Add	ACE			
Action:	💿 Permit 🛛 🔘 Deny			
Addres	s: 10.10.10.0/24			
Descrin	ition:			

6. Click OK.

General Eervers	The VPN client makes split to me ingide	asions on the	classe of a network, is: that can be specified below by providing the proper parameters to Yolicy' and Network too' fe	elitte .
Advanced -Solt Tunca Inc	DNE Names:	😨 Inherit		
-Browser Proxy HAnyConnect Client HIPsec(IXBy:) Client	Send All DNS Loci ups Through Tunnel:	🔽 Inherit	⊙ wes ⊙No	
	Poloy:	🗌 Inherit	Turnel Network List Selow 👻	
	Network List:	🔲 Inherit	Epit-ACL 👻	Managa
	Pressing this button to set up so it eales Eat up Split Ecolusion for Wab Securi	ion for Web S iy	Security provides.	
	Intercept DHCP Configuration Mes	sage from h	Microsoft Clients	

7. Haga clic en Apply (Aplicar).

Una vez conectadas, las rutas para las subredes o los hosts en la ACL dividida se agregan a la tabla de enrutamiento de la máquina del cliente. En las máquinas con Microsoft Windows, esto se puede ver en el resultado del comando **route print**. El siguiente salto para estas rutas será una dirección IP de la subred del conjunto de IP del cliente (generalmente la primera dirección IP de la subred):

C:\Users\admin>route print IPv4 Route Table _____ Active Routes: Network Destination Netmask Gateway Interface Metric 0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261 10.10.10.0 255.255.255.0 10.10.11.2 10.10.11.1 2 *!!* This is the split tunnel route. 10.106.44.0 255.255.255.0 On-link 10.106.44.243 261 172.16.21.1 255.255.255.255 On-link 10.106.44.243 6 !! This is the route for the ASA Public IP Address. En las máquinas con MAC OS, introduzca el comando netstat -r para ver la tabla de enrutamiento de la PC. \$ netstat -r Routing tables Internet: Destination Gateway Flags Refs Use Netif Expire default hsrp-64-103-236-1. UGSc 34 0 en1 10.10.10/24 10.10.11.2 UGSc 0 44 utun1 *!!* This is the split tunnel route. 10.10.11.2/32 localhost UGSc 1 0 lo0 172.16.21.1/32 hsrp-64-103-236-1. UGSc 1 0 en1 !! This is the route for the ASA Public IP Address. Descarga e instalación de AnyConnect Client

Existen dos métodos que puede utilizar para implementar Cisco AnyConnect Secure Mobility Client en la máguina del usuario:

Implementación web

• Implementación independiente

Ambos métodos se explican con mayor detalle en las secciones siguientes.

Implementación web

Para utilizar el método de implementación web, ingrese https://<ASA's FQDN> o <ASA's IP>la URL en un navegador en la máquina del cliente, que lo llevará a la página del portal de *WebVPN*.

Nota: Si se utiliza Internet Explorer (IE), la instalación se realiza principalmente a través de ActiveX, a menos que se vea obligado a utilizar Java. Todos los demás navegadores utilizan Java.

Una vez iniciada la sesión en la página, la instalación debe comenzar en la máquina del cliente y el cliente debe conectarse a ASA una vez finalizada la instalación.

Nota: Es posible que se le solicite permiso para ejecutar ActiveX o Java. Esto debe permitirse para continuar con la instalación.

Logon	
Group SSLClient 🔻	
Username	
Password	
Logon	



AnyConnect Secure Mobility Client						
 WebLaunch Platform Detection - ActiveX - Java Detection 	Attempting to use Java for Installation Sun Java applet has started. This could take up to 60 seconds. Please wait					
 Download Connected 	Help Download					

Implementación independiente

Complete estos pasos para utilizar los menús:

- Descargue la imagen de AnyConnect Client del sitio web de Cisco. Para elegir la imagen correcta para descargar, consulte la página web de <u>Cisco AnyConnect Secure Mobility</u> <u>Client</u>. En esta página se proporciona un vínculo de descarga. Desplácese a la página de descarga y seleccione la versión adecuada. Realice una búsqueda por **Paquete de** instalación completo - Ventana / Instalador independiente (ISO). Nota: Luego se descarga una imagen de instalador ISO (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
- 2. Utilice WinRar o 7-Zip para extraer el contenido del paquete ISO:

A 1070				
anyconnect-win-3.1.070		Burn disc image		
		7-Zip	- +	Open archive
	2	Edit with Notepad++		Open archive
		Open with		Extract files
		Share with	•	Extract Here
				Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"

3. Una vez extraído el contenido, ejecute el archivo **Setup.exe** y elija los módulos que deben instalarse junto con Cisco AnyConnect Secure Mobility Client.

Consejo: Para configurar parámetros adicionales para la VPN, consulte la sección <u>Configuración de conexiones de cliente VPN de AnyConnect</u> de la *Guía de configuración de Cisco ASA serie 5500 con la CLI 8.4 y 8.6*.

Configuración de CLI

En esta sección se proporciona la configuración de la CLI para Cisco AnyConnect Secure Mobility Client con fines de referencia.

ASA Version 9.3(2) ! hostname PeerASA-29 enable password 8Ry2YjIyt7RRXU24 encrypted ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0 1 interface GigabitEthernet0/0 nameif outside security-level 0 ip address 172.16.21.1 255.255.255.0 1 interface GigabitEthernet0/1 nameif inside security-level 100 ip address 10.10.10.1 255.255.255.0 1 boot system disk0:/asa932-smp-k8.bin ftp mode passive object network NETWORK_OBJ_10.10.10.0_24 subnet 10.10.10.0 255.255.255.0 object network NETWORK_OBJ_10.10.11.0_27 subnet 10.10.11.0 255.255.255.224 access-list all extended permit ip any any !*********Split ACL configuration********* access-list Split-ACL standard permit 10.10.10.0 255.255.255.0 no pager logging enable logging buffered debugging mtu outside 1500 mtu inside 1500 mtu dmz 1500 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-721.bin no asdm history enable arp timeout 14400 no arp permit-nonconnected !This will exempt traffic from Local LAN(s) to the !Remote LAN(s) from getting NATted on any dynamic NAT rule. nat (inside, outside) source static NETWORK OBJ 10.10.10.0 24 NETWORK OBJ 10.10.0.24 destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp route-lookup access-group all in interface outside route outside 0.0.0.0 0.0.0.0 172.16.21.2 1 timeout xlate 3:00:00 timeout pat-xlate 0:00:30 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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute timeout tcp-proxy-reassembly 0:01:00 timeout floating-conn 0:00:00 dynamic-access-policy-record DfltAccessPolicy

user-identity default-domain LOCAL aaa authentication ssh console LOCAL http server enable http 0.0.0.0 0.0.0.0 outside no snmp-server location no snmp-server contact !******** Trustpoint for Selfsigned certificate********* !Genarate the key pair and then configure the trustpoint !Enroll the trustpoint genarate the self-signed certificate crypto ca trustpoint SelfsignedCert enrollment self subject-name CN=anyconnect.cisco.com keypair sslcert crl configure crypto ca trustpool policy crypto ca certificate chain SelfsignedCert certificate 4748e654 308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105 0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e 170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d 06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0 55a975ec alf2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4 ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0 7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c 75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93 5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7 53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34 03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36 19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001 300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296 c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1 64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41 daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928 f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9 4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833 900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206 3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8 quit telnet timeout 5 ssh timeout 5 ssh key-exchange group dh-group1-shal console timeout 0 management-access inside threat-detection basic-threat threat-detection statistics access-list no threat-detection statistics tcp-intercept ssl server-version tlsv1-only ssl encryption des-shal 3des-shal aes128-shal aes256-shal !******* Bind the certificate to the outside interface******* ssl trust-point SelfsignedCert outside !*******Configure the Anyconnect Image and enable Anyconnect*** webvpn enable outside

anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1 anyconnect enable tunnel-group-list enable

```
!*****Group Policy configuration*******
!Tunnel protocol, Spit tunnel policy, Split
!ACL, etc. can be configured.
group-policy GroupPolicy_SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com
username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15
!*****Tunnel-Group (Connection Profile) Configuraiton****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
1
class-map inspection_default
match default-inspection-traffic
1
1
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
1
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

Verificación

Complete estos pasos para verificar la conexión del cliente y los diversos parámetros que están asociados a esa conexión:

1. Vaya a Monitoreo> VPN en ASDM:



2. Puede utilizar la opción **Filtrar por** para filtrar el tipo de VPN. Seleccione **AnyConnect Client** del menú desplegable y todas las sesiones de AnyConnect Client. **Consejo:** Las sesiones se pueden filtrar aún más con otros criterios, como *Nombre de usuario* y *Dirección*

N 27 Q	Filter By: AnyC	onnact Client 🔹	All Sessions	•	Filtar		
VEN Cluster Loads	Usemane	Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Encryption	Login Time Duration	Bytes TX Bytes RX	Inactivity
Compression Statistics Encryption Statistics Gobal RE/IPson Statistics	ciaco	GroupPolicy_SSLCIIen SSLCIIent	10.10.11.1 172.16.21	AnyConnect-Parent SSI-Tunnel AnyConnect-Parent (1)none S.	. 16 58:56 UTC . Dr. 12m:55a	. 11472 22738	01.00m:00
- VLAN Mapping Sessions Clientless SSL VPN VPN Connection Creater							
WSA Sessions							
Interfaces							
VPN							

3. Haga doble clic en una sesión para obtener más detalles sobre esa sesión en particular:

essio	on Details —								
Username		Group Policy Connection Profile	Assigned IP Address Public IP Address	Protocol Login Time Encryption Duration		Sytes Tx Sytes Rx	Inactivity		
isco		GroupPolicy_SSLClier SSLClient	10.10.11.1 172.16.21.1	AnyConnect-F AnyConnect-F	Parent SSL-Tunnel . Parent: (1)none S	16:58:56 UTC 1 0h:21m:09s 2	1472 6653	0h:00m:00s	
ID	Туре	Local Addr. / Subnet Mask / Protocol / Port Remote Addr. / Subnet Mask / Protocol / Port		Encryption	Other		Bytes Tx Bytes Rx		More
ID	Type AnyConn	Remote Addr. / Subnet	Mask / Protocol / Port	none	Other Tunnel ID: 14.1		Bytes Rx 5954		

4. Ingrese el comando **show vpn-sessiondb anyconnect** en la CLI para obtener los detalles de la sesión:

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1 Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. Puede utilizar las otras opciones de filtro para refinar los resultados:

show vpn-sessiondb detail anyconnect filter name cisco Session Type: AnyConnect Detailed Username : cisco Index : 19 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1 Bytes Tx : 11036 Bytes Rx : 4977 Pkts Tx : 8 Pkts Rx : 60 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : GroupPolicy_SSLClient Tunnel Group : SSLClient Login Time : 20:33:34 UTC Mon Apr 6 2015 Duration : 0h:01m:19s AnyConnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 AnyConnect-Parent: Tunnel ID : 19.1 Public IP : 10.106.44.243 Encryption : none Hashing : none TCP Src Port : 58311 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : AnyConnect Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 5518 Bytes Rx : 772 Pkts Tx : 4 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 19.2 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Encryption : 3DES Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 58315 TCP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 5518 Bytes Rx : 190 Pkts Tx : 4 Pkts Rx : 2 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 19.3 Assigned IP : 10.10.11.1 Public IP : 10.106.44.243 Encryption : DES Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 58269 UDP Dst Port : 443 Auth Mode : userPassword Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : DTLS VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.06073 Bytes Tx : 0 Bytes Rx : 4150 Pkts Tx : 0 Pkts Rx : 59

Troubleshoot

Puede utilizar la herramienta de diagnóstico e informes de AnyConnect (DART) para recopilar los datos que son útiles para solucionar los problemas de instalación y conexión de AnyConnect. El asistente de DART se utiliza en el equipo que ejecuta AnyConnect. La DART reúne los registros, el estado y la información de diagnóstico para el análisis de Cisco Technical Assistance Center (TAC) y no requiere privilegios de administrador para ejecutarse en la máquina del cliente.

Instalación de la DART

Complete estos pasos para instalar la DART:

- Descargue la imagen de AnyConnect Client del sitio web de Cisco. Para elegir la imagen correcta para descargar, consulte la página web de <u>Cisco AnyConnect Secure Mobility</u> <u>Client</u>. En esta página se proporciona un vínculo de descarga. Desplácese a la página de descarga y seleccione la versión adecuada. Realice una búsqueda por Paquete de instalación completo - Ventana / Instalador independiente (ISO). Nota: Luego se descarga una imagen de instalador ISO (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
- 2. Utilice WinRar o 7-Zip para extraer el contenido del paquete ISO:

anyconnect-win-3.1.070	r-	Burn disc image		
		7-Zip		Open archive
	2	Edit with Notepad++		Open archive
		Open with	•	Extract files
		Share with	•	Extract Here
				Extract to "anyconnect-win-3.1.07021-pre-deploy-k9\"

- 3. Navegue hasta la carpeta a la que se extrajo el contenido.
- 4. Ejecute el archivo **Setup.exe** y seleccione solo **Herramienta de diagnóstico e informes de Anyconnect**:



Ejecución de la DART

Aquí hay información importante que debe tener en cuenta antes de ejecutar la DART:

- El problema se debe recrear al menos una vez antes de ejecutar la DART.
- La fecha y hora en la máquina del usuario deben tenerse en cuenta cuando se vuelve a crear el problema.

Ejecute la DART desde el menú Inicio en la máquina del cliente:



Se puede seleccionar el modo *Predeterminado* o *Personalizado*. Cisco recomienda ejecutar la DART en el modo predeterminado para que toda la información se pueda capturar en una sola toma.

Cisco DART 3.1.05170	<u>;</u>							
Bundle Creation Option								
Select "Default" to include the typical log files and diagnostic information in the bundle. Select "Custom" to choose the list of log files and diagnostic information to be included in the bundle.								
 Default (Bundle will be saved to Desktop) 								
Custom								
Clear logs after DART finshes								
Back Next Cancel								

Una vez completada, la herramienta guarda el archivo *.zip* del paquete de la DART en el escritorio del cliente. El paquete se puede enviar por correo electrónico a TAC (después de abrir un caso en TAC) para su posterior análisis.

Información Relacionada

- Guía de solución de problemas de AnyConnect VPN Client: problemas comunes
- Problemas de Java 7 con AnyConnect, CSD/Hostscan y WebVPN: guía de solución de problemas
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).