

Configuración de la tunelización dividida dinámica de ASA/AnyConnect

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configuración](#)

[Diagrama de la red](#)

[Paso 1. Crear atributos personalizados de AnyConnect](#)

[Paso 2. Crear nombre personalizado de AnyConnect y configurar valores](#)

[Paso 3. Agregar tipo y nombre a la directiva de grupo](#)

[Ejemplo de configuración CLI](#)

[Limitaciones](#)

[Verificación](#)

[Troubleshoot](#)

[En caso de que se utilice el carácter comodín en el campo Valores](#)

[En caso de que no se vean las rutas no seguras en la pestaña Detalles de ruta](#)

[Resolución general de problemas](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar AnyConnect Secure Mobility Client para la tunelización de exclusión de división dinámica a través de ASDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de ASA.
- Conocimientos básicos de Cisco AnyConnect Security Mobility Client.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- ASA 9.12(3)9
- Adaptive Security Device Manager (ASDM) 7.13(1)
- AnyConnect 4.7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La tunelización dividida de AnyConnect permite a Cisco AnyConnect Secure Mobility Client acceder de forma segura a los recursos corporativos a través de IKEV2 o Secure Sockets Layer (SSL).

Antes de la versión 4.5 de AnyConnect, basada en la política configurada en el dispositivo de seguridad adaptable (ASA), el comportamiento del túnel dividido podía ser Tunnel Specified (Túnel especificado), Tunnel All (Túnel especificado) o Exclude Specified (Excluir especificado).

Con la llegada de los recursos informáticos alojados en la nube, a veces los servicios se resuelven en una dirección IP diferente en función de la ubicación del usuario o de la carga de los recursos alojados en la nube.

Dado que AnyConnect Secure Mobility Client proporciona una tunelización dividida al rango de subred estática, host o conjunto de IPV4 o IPV6, a los administradores de red les resulta difícil excluir dominios/FQDN mientras configuran AnyConnect.

Por ejemplo, un administrador de red desea excluir el dominio Cisco.com de la configuración del túnel de división, pero la asignación DNS para Cisco.com cambia, ya que está alojado en la nube.

Mediante la tunelización Dynamic Split Exclude, AnyConnect resuelve dinámicamente la dirección IPv4/IPv6 de la aplicación alojada y realiza los cambios necesarios en la tabla de routing y los filtros para permitir que la conexión se realice fuera del túnel.

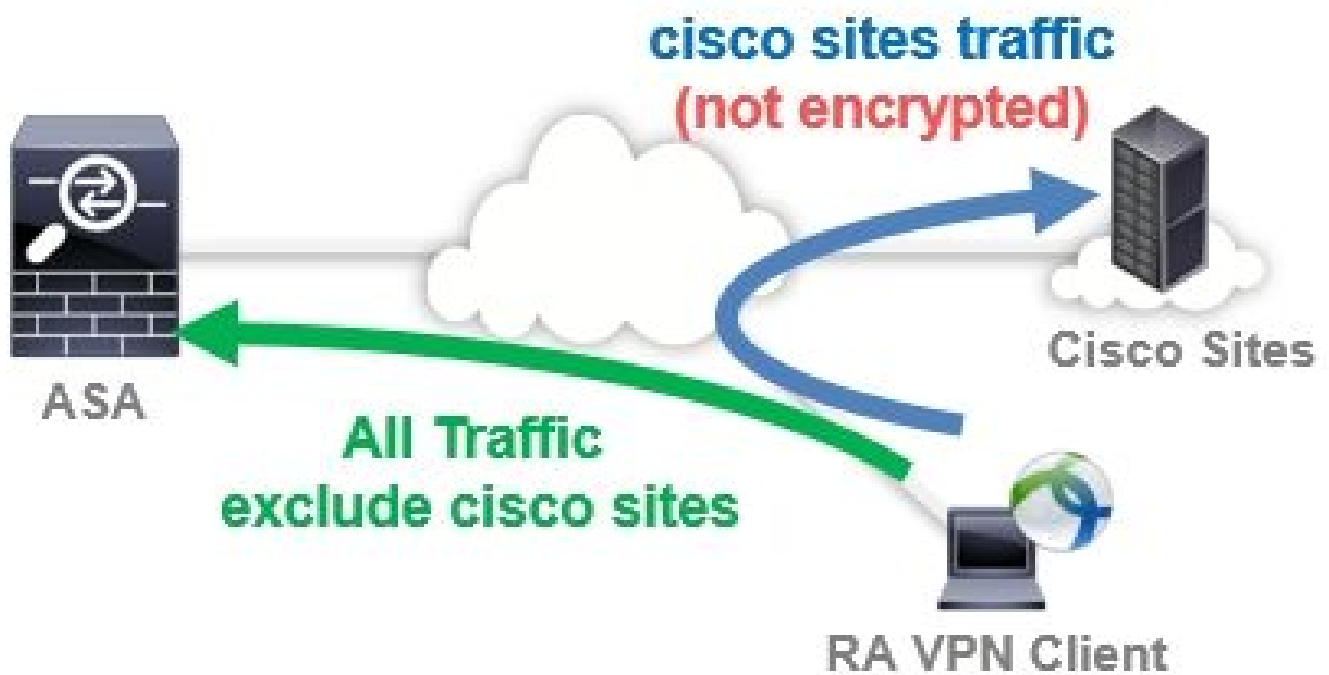
A partir de AnyConnect 4.5, se puede utilizar la tunelización dinámica de escupir en la que AnyConnect resuelve dinámicamente la dirección IPv4/IPv6 de la aplicación alojada y realiza los cambios necesarios en la tabla de routing y los filtros para permitir que la conexión se realice fuera del túnel

Configuración

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

Diagrama de la red

Esta imagen muestra la topología utilizada para los ejemplos de este documento.



Paso 1. Crear atributos personalizados de AnyConnect

Desplácese hasta **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom**

Attributes. Haga clic en el **Add** botón, y establezca el **dynamic-split-exclude-domains** atributo y la descripción opcional, como se muestra en la imagen:

The screenshot shows the Cisco configuration interface. The breadcrumb trail is **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes**. Below the breadcrumb, there is a description: "Declarations of custom attribute types and these attributes are enforced in [AnyConnect](#) group policy, [AnyConnect](#) dynamic access policy and [AnyConnect](#) custom attribute names". There are buttons for **Add**, **Edit**, and **Delete**. Below these buttons is a table with two columns: **Type** and **Description**.

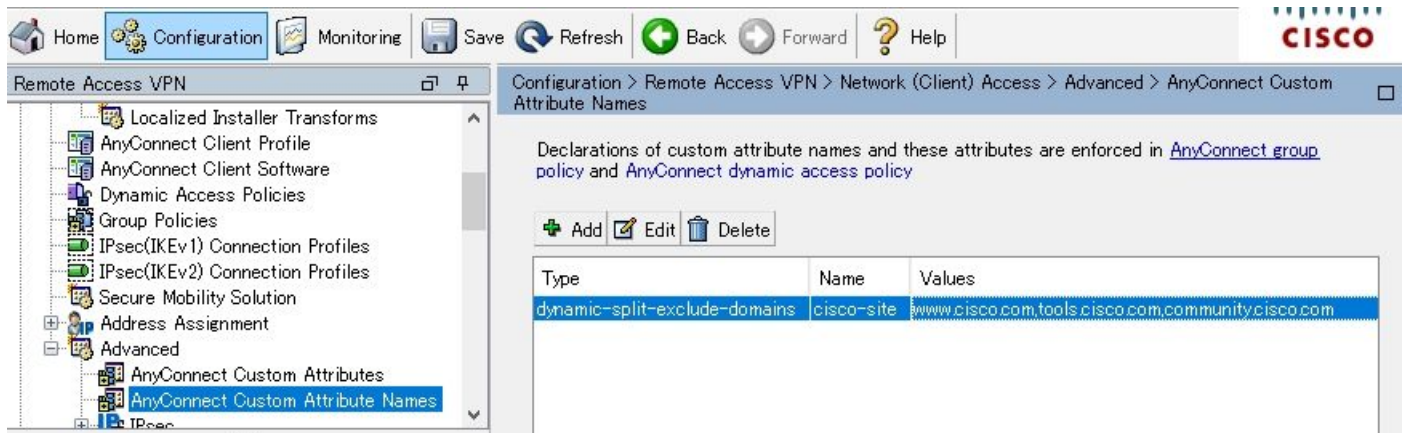
Type	Description
dynamic-split-exclude-domains	Dynamic Split Tunneling

Paso 2. Crear nombre personalizado de AnyConnect y configurar valores

Desplácese hasta **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names**.

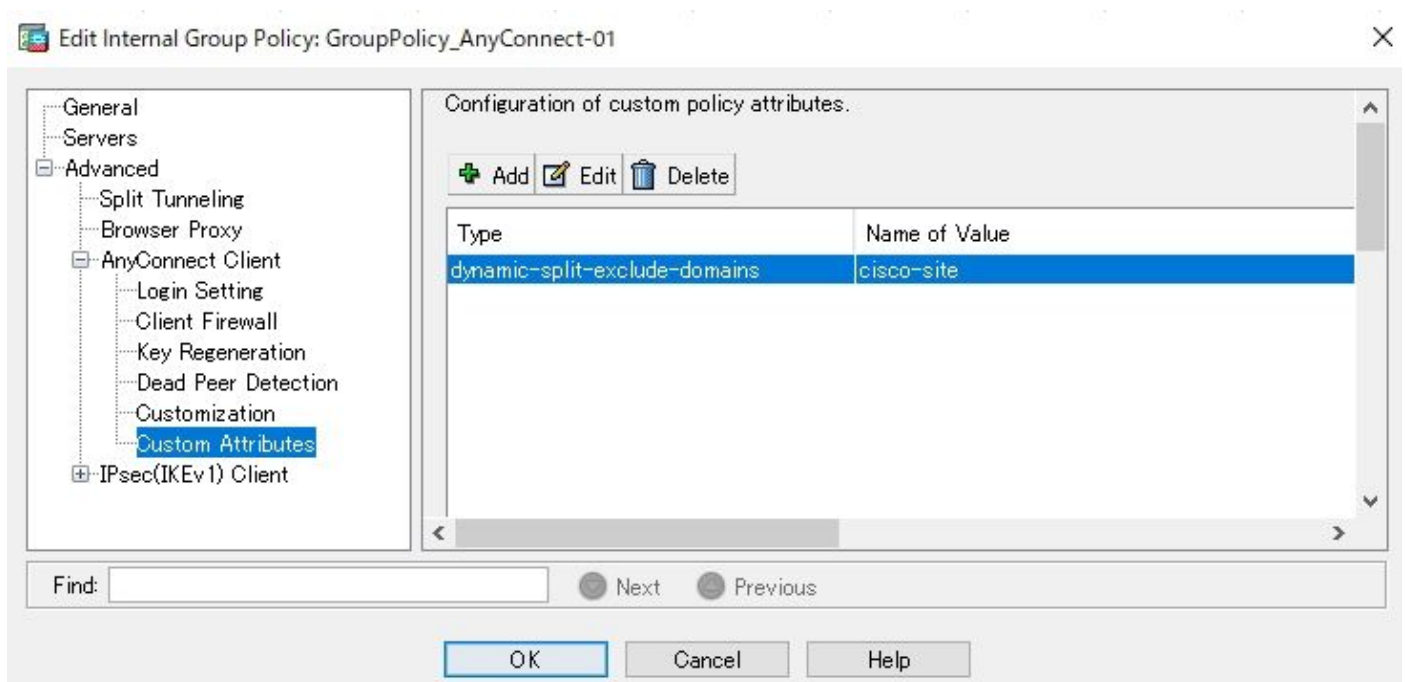
Haga clic en el **Add** botón, y establezca el **dynamic-split-exclude-domains** atributo creado anteriormente de Tipo, un nombre arbitrario y Valores, como se muestra en la imagen:

Tenga cuidado de no introducir espacios en Nombre. (Por ejemplo: Posible sitio de Cisco, Sitio de Cisco imposible) Cuando se registran varios dominios o FQDN en Valores, sepárelos con una coma (,).



Paso 3. Agregar tipo y nombre a la directiva de grupo

Desplácese hasta **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** y seleccione una directiva de grupo. A continuación, navegue hasta **Advanced > AnyConnect Client > Custom Attributes** y agregue el **Type** y **Name**, tal como se muestra en la imagen:



Ejemplo de configuración CLI

Esta sección proporciona la configuración CLI de Dynamic Split Tunneling para fines de referencia.

<#root>

```
ASAv10# show run
```

```
--- snip ---
```

```
webvpn
```

```
enable outside
```

```
AnyConnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling
```

```
hsts
```

```
enable
```

```
max-age 31536000
```

```
include-sub-domains
```

```
no preload
```

```
AnyConnect image disk0:/AnyConnect-win-4.7.04056-webdeploy-k9.pkg 1
```

```
AnyConnect enable
```

```
tunnel-group-list enable
```

```
cache
```

```
disable
```

```
error-recovery disable
```

```
AnyConnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community
```

```
group-policy GroupPolicy_AnyConnect-01 internal
```

```
group-policy GroupPolicy_AnyConnect-01 attributes
```

```
wins-server none
```

```
dns-server value 10.0.0.0
```

```
vpn-tunnel-protocol ssl-client
```

```
split-tunnel-policy tunnelall
```

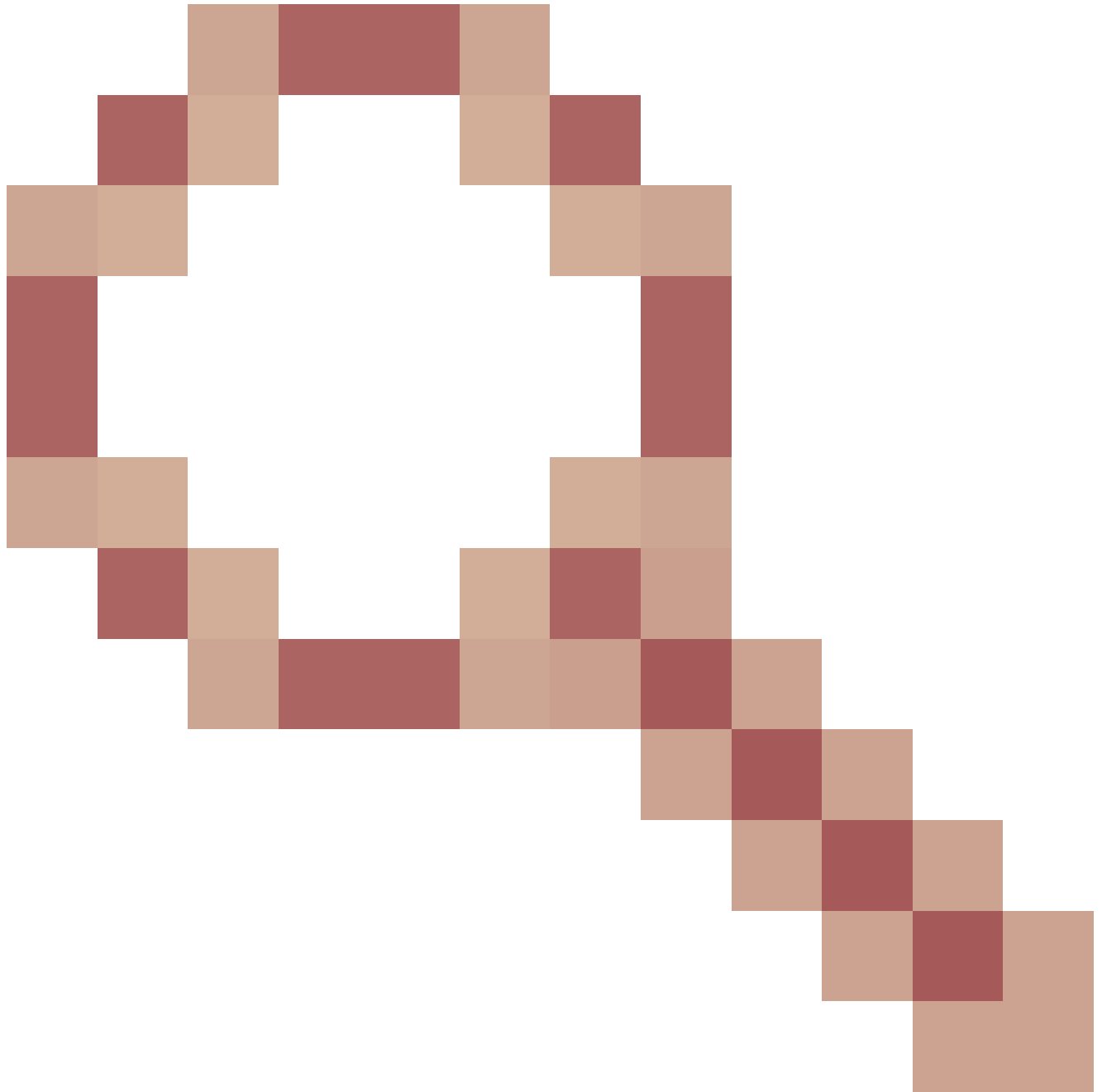
```
split-tunnel-network-list value SplitACL
```

```
default-domain value cisco.com
```

```
AnyConnect-custom dynamic-split-exclude-domains value cisco-site
```

Limitaciones

- ASA versión 9.0 o posterior es necesario para utilizar los atributos personalizados de Dynamic Split Tunneling.
- No se admite el carácter comodín del campo Valores.
- La tunelización dividida dinámica no es compatible con los dispositivos iOS (Apple) (petición de mejora: ID de error de Cisco [CSCvr54798](#))



).

Verificación

Para verificar el **Dynamic Tunnel Exclusions**, AnyConnectsoftware de inicio configurado en el cliente, haga clic en **Advanced Window>Statistics**, como se muestra en la imagen:



Virtual Private Network (VPN)

Preferences Statistics **Route Details** Firewall Message History

Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Tunnel All Traffic
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	www.cisco.com tools.cisco.com community.cisco.com
Dynamic Tunnel Inclusion:	None
Duration:	00:00:43
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information	
Client (IPv4):	1.176.100.101
Client (IPv6):	Not Available
Server:	100.0.0.254

Bytes

Reset Export Stats...

También puede navegar hasta **Advanced Window > Route Details** pestaña donde puede verificar **Dynamic Tunnel Exclusions** que se enumeran **Non-Secured Routes**, debajo, como se muestra en la imagen.



Virtual Private Network (VPN)

Preferences | Statistics | Route Details | **Firewall** | Message History

Non-Secured Routes (IPv4)

- 72.163.4.38/32 (tools.cisco.com)
- 173.37.145.84/32 (www.cisco.com)
- 208.74.205.244/32 (community.cisco.com)

Secured Routes (IPv4)

- 0.0.0.0/0

En este ejemplo, ha configurado www.cisco.com Dynamic Tunnel Exclusion listdebajo y la captura de Wireshark recopilada en la interfaz física del cliente AnyConnect confirma que el tráfico a www.cisco.com (198.51.100.0) no está cifrado por DTLS.

Capturing from ローカル エリア接続 [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help


Filter: Expression... Clear Apply Save

No.	Time	Source	S.Port	Destination	D.Port	Length	Info
17	2.991100000	100.0.0.1	56319	100.0.0.254	443	569	CID: 254, Seq: 0
18	3.092024000	100.0.0.1	2095	173.37.145.84	443	66	2095+443 [SYN] Seq=0
19	3.128694000	173.37.145.84	443	100.0.0.1	2093	60	443+2093 [SYN, ACK] Seq=1
20	3.128697000	173.37.145.84	443	100.0.0.1	2094	60	443+2094 [SYN, ACK] Seq=1
21	3.128848000	100.0.0.1	2093	173.37.145.84	443	54	2093+443 [ACK] Seq=1
22	3.128886000	100.0.0.1	2094	173.37.145.84	443	54	2094+443 [ACK] Seq=1
23	3.129667000	100.0.0.1	2093	173.37.145.84	443	296	client Hello
24	3.130049000	100.0.0.1	2094	173.37.145.84	443	296	client Hello

En caso de que se utilice el carácter comodín en el campo Valores

Si se configura un comodín en el campo Valores, por ejemplo, ***.cisco.com** se configura en Valores, la sesión de AnyConnect se desconecta, como se muestra en los registros:

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> N
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> First TCP SVC connection established for
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP SVC connection established without
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Client Type: Cisco AnyConnect VPN Ag
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv4 Address <172.16.0.0> IPv6 address
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (172.16.0.0/44868) to identity:203.0.113.0/44
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC closing connection: Transport closin
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC Message: 16/ERROR: Configuration
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> WebVPN session terminated: User Reque
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session disconnected. Session Type: AnyConnect-
```

 **Nota:** como alternativa, puede utilizar el dominio **cisco.com** en Valores para permitir FQDN como www.cisco.com y tools.cisco.com.

En caso de que no se vean las rutas no seguras en la pestaña Detalles de ruta

El cliente AnyConnect detecta y agrega automáticamente la dirección IP y el FQDN en la ficha Detalles de ruta, cuando el cliente inicia el tráfico para los destinos excluidos.

Para verificar que los usuarios de AnyConnect están asignados a la política de grupo de Anyconnect correcta, puede ejecutar el comando **show vpn-sessiondb anyconnect filter name <username>**

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco
```

```
Session Type: AnyConnect
```

```
Username : cisco Index : 7
```

```
Assigned IP : 172.16.0.0 Public IP : 10.0.0.0
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
```

```
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx : 7795373 Bytes Rx : 390956
```

```
Group Policy : GroupPolicy_AnyConnect-01
```

```
Tunnel Group : AnyConnect-01
```

```
Login Time : 13:20:48 UTC Tue Mar 31 2020
```

```
Duration : 20h:19m:47s
```

```
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
```

```
Audt Sess ID : 019600a9000070005e8343b0
```

```
Security Grp : none
```

Resolución general de problemas

Puede utilizar la herramienta de diagnóstico e informes (DART) de AnyConnect para recopilar los datos que son útiles para solucionar los problemas de instalación y conexión de AnyConnect. El asistente de la DART se utiliza en la computadora 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.

Información Relacionada

- [Guía del administrador de Cisco AnyConnect Secure Mobility Client, versión 4.7 - Acerca de la tunelización dividida dinámica](#)
- [ASDM Book 3: Guía de configuración de ASDM de VPN de la serie ASA de Cisco, 7.13 - Configuración de la tunelización dividida dinámica](#)

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).