Configuración de L2TP a través de IPSec entre Windows 8 PC y ASA mediante clave previamente compartida

Contenido

Introducción **Prerequisites Requirements Restricciones Componentes Utilizados Convenciones Antecedentes** Configurar Diagrama de la red Configuración de túnel completo Configuración de ASA con Adaptive Security Device Manager (ASDM) Configuración ASA con CLI Configuración del cliente Windows 8 L2TP/IPsec Configuración del túnel dividido Configuración en ASA Configuración en el cliente L2TP/IPsec Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe cómo configurar el protocolo de túnel de capa 2 (L2TP) sobre IPsec usando una clave previamente compartida entre Cisco Adaptive Security Appliance (ASA) y el cliente nativo de Windows 8.

L2TP sobre seguridad de protocolo de Internet (IPsec) proporciona la capacidad de implementar y administrar una solución de red privada virtual (VPN) L2TP junto con los servicios de firewall y VPN IPsec en una única plataforma.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

• Conectividad IP de la máquina cliente al ASA. Para probar la conectividad, intente hacer ping

a la dirección IP del ASA desde el punto final del cliente y viceversa

• Asegúrese de que los puertos UDP 500 y 4500 y el protocolo de carga de seguridad de encapsulación (ESP) no se bloqueen ninguna parte a lo largo de la ruta de la conexión

Restricciones

- L2TP sobre IPsec soporta solamente IKEv1. IKEv2 no es compatible.
- L2TP con IPsec en el ASA permite que el LNS interopere con clientes VPN nativos integrados en sistemas operativos como Windows, MAC OS X, Android y Cisco IOS. Sólo se soporta L2TP con IPsec, el L2TP nativo no se soporta en ASA.
- La duración mínima de asociación de seguridad IPSec admitida por el cliente de Windows es de 300 segundos. Si el tiempo de vida en el ASA se establece en menos de 300 segundos, el cliente de Windows lo ignora y lo reemplaza con una vida útil de 300 segundos.
- El ASA solo admite las versiones 1 y 2 del Protocolo punto a punto (PPP) de autenticación de contraseña (PAP) y el Protocolo de autenticación por desafío mutuo de Microsoft (CHAP) en la base de datos local. Los servidores de autenticación proxy realizan el protocolo de autenticación extensible (EAP) y el CHAP. Por lo tanto, si un usuario remoto pertenece a un grupo de túnel configurado con los comandos authentication eap-proxy o authentication chap, y el ASA se configura para utilizar la base de datos local, ese usuario no puede conectarse.

Tipos de Autenticación PPP Soportados

L2TP sobre conexiones IPsec en el ASA soporta solamente los tipos de autenticación PPP mostrados en la Tabla

	Soporte d	e Servidor AAA y Tipos de Autenticación PPP
Tipo de servidor AAA		Tipos de Autenticación PPP Soportados
L	LOCAL	PAP, MSCHAPv1, MSCHAPv2
F	RADIUS	PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-Proxy
TA	ACACS+	PAP, CHAP, MSCHAPv1
	LDAP	PAP
	NT	PAP
K	erberos	PAP
	SDI	SDI
Característic	cas del Tipo d	e Autenticación PPP
Palabra	Tipo de	
clave	autenticación	Características
chap	CHAP	En respuesta al desafío del servidor, el cliente devuelve el [desafío más contraseña] cifrado con un nombre de usuario de texto sin cifrar. Este protocolo es más seguro que el PAP, pero no cifra los datos.
eap-proxy EAP		Habilita EAP que permite que el dispositivo de seguridad proxy el proceso de autenticación PPP a un servidor de autenticación RADIUS externo.
	CHAP de	
ms-chap-v1 ms-chap-v2	Microsoft, Versión 1 Microsoft CHAP, versión, 2	Similar a CHAP pero más seguro en que el servidor almacena y compara solamente contraseñas cifradas en lugar de borrar contraseñas de texto como en CHAP. Este protocolo también genera una clave para el cifrado de datos por parte de MPPE.
pap	PAP	Pasa el nombre de usuario y la contraseña de texto sin cifrar durante la autenticación y no es seguro.

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

- Cisco 5515 Series ASA que ejecuta la versión de software 9.4(1)
- Cliente L2TP/IPSec (Windows 8)

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Esta configuración puede también se utilizar con Cisco ASA 5500 Series Security Appliance 8.3(1) o posterior.

Convenciones

Consulte <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones de los documentos

Antecedentes

El protocolo de túnel de capa 2 (L2TP) es un protocolo de tunelación VPN que permite a los clientes remotos utilizar la red IP pública para comunicarse de forma segura con los servidores de red corporativos privados. L2TP utiliza PPP sobre UDP (puerto 1701) para tunelizar los datos.

El protocolo L2TP se basa en el modelo cliente/servidor. La función se divide entre el servidor de red L2TP (LNS) y el concentrador de acceso L2TP (LAC). El LNS normalmente se ejecuta en un gateway de red como el ASA en este caso, mientras que el LAC puede ser un servidor de acceso a la red (NAS) de acceso telefónico o un dispositivo terminal con un cliente L2TP agrupado como Microsoft Windows, Apple iPhone o Android.

Configurar

Esta sección se presenta con la información necesaria para configurar las funciones descritas en este documento.

Nota: Use la herramienta <u>Command Lookup Tool (clientes registrados solamente) para</u> encontrar más información sobre los comandos usados en este documento.

Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

Diagrama de la red



Configuración de túnel completo

Configuración de ASA con Adaptive Security Device Manager (ASDM)

Complete estos pasos:

Paso 1. Inicie sesión en el ASDM y navegue hasta **Asistentes > Asistentes VPN > Asistente VPN** de Acceso Remoto Ipsec (IKEv1).

🔂 Cisco ASDM 7.2 for ASA - 10.106.44.216					
File View Tools	File View Tools Wizards Window Help				
Home 🖧 Conf	Startup Wizard		Back 🕐 Forward 🤣 Help		
Device List	VPI	N Wizards		Site-to-site VPN Wizard	
	Hig	h Availability and Scalability Wizard		AnyConnect VPN Wizard	
P Add Delete	Uni	ified Communication Wizard		Clientless SSL VPN Wizard	
Find:	Pac	ket Capture Wizard		IPsec (IKEv1) Remote Access VPN Wizard	
Image:					

Paso 2. Aparecerá una ventana de configuración de VPN de acceso remoto. En la lista desplegable, elija la interfaz en la que debe terminar el túnel VPN. En este ejemplo, la interfaz externa está conectada a la WAN y, por lo tanto, terminan los túneles VPN en esta interfaz. Mantenga el cuadro Enable inbound IPSec sessions to bypass interface access lists. La política de grupo y las listas de acceso de autorización por usuario todavía se aplican al tráfico verificado para que no sea necesario configurar una nueva lista de acceso en la interfaz externa para permitir que los clientes accedan a los recursos internos. Haga clic en Next (Siguiente).



Paso 3. Como se muestra en esta imagen, elija el tipo de cliente como **cliente de Microsoft Windows que usa L2TP sobre IPSec** y **MS-CHAP-V1** y **MS-CHAP-V2** como protocolo de autenticación PPP ya que PAP no es seguro y otros tipos de autenticación no son compatibles con la base de datos LOCAL como servidor de autenticación y haga clic en **Siguiente**.

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

Paso 4. Elija el método de autenticación como **Pre-shared-key** y escriba la clave previamente compartida que también debe ser la misma en el lado del cliente y haga clic en **Next**, como se muestra en esta imagen.

📑 VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
VPN WIZard	White Cleant Authentication Precision and Tunnel Group Name (Step 3 or) The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client. Authentication Method Pre-shared key Pre-Shared Key: Clsc0@123 Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK) Tunnel Group For VPN clients using L2TP over IPsec with pre-shared key authentication, DefaultRAGroup tunnel group must be used.
- 6-	Tunnel Group Name: DefaultRAGroup
	< Back Next > Finish Cancel Help

Paso 5. Especifique un método para autenticar los usuarios que intenten el L2TP a través de conexiones del IPSec. Se puede utilizar un servidor de autenticación AAA externo o su propia base de datos local. Elija **Authenticate using the local user database** si desea autenticar los clientes con la base de datos local de ASA y haga clic en **Next**.

Nota: Consulte <u>Configuración de la Autenticación RADIUS para los usuarios de VPN</u> para autenticar a los usuarios usando el servidor AAA externo.

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

Paso 6. Para agregar nuevos usuarios a la base de datos local para la autenticación de usuario, introduzca el nombre de usuario y la contraseña y, a continuación, haga clic en **ADD** o se pueden utilizar las cuentas de usuario existentes en la base de datos, como se muestra en esta imagen. Haga clic en Next (Siguiente).

To VPN Wizard		x
VPN Wizard	User Accounts (Step 5 of 11) Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.	
Home	User to Be Added Username: test Add >> Password (optional): Confirm Password (optional):	
	<pre><back next=""> Finish Cancel Help</back></pre>	2

Paso 7. En la lista desplegable, elija el conjunto de direcciones que se utilizará para asignar la dirección IP a los clientes. Para crear un nuevo conjunto de direcciones, haga clic en **Nuevo**, como se muestra en esta imagen.

VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch Fr	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN dients.
Corporate Network	Tunnel Group Name : DefaultRAGroup
THE THE	Pool Name: New
	Pool Settings
	Range Start Address:
The	Range End Address:
	Subnet Mask:
	< Back Next > Finish Cancel Help

Paso 8. Aparece el cuadro de diálogo Agregar agrupación IPv4.

- 1. Ingrese el nombre del nuevo pool de dirección IP.
- 2. Ingrese las direcciones IP de inicio y de finalización.
- 3. Introduzca la máscara de subred y haga clic en OK.

iii VPN Wizard			
VPN Wizard	Address Pool (Step 6 o	of 11)	
Branch	Enter a pool of local a clients.	addresses to be used for assigning dynamic IP addresses to remo	ite VPN
Home	a Add IPv4 Pool		
Corporate Network	Name: Ad	ddress-pool	
Genting you	Starting IP Address: 19	92.168.1.1 New	
	Ending IP Address: 19	92.168.1.254	
LUU III	Subnet Mask: 25	55.255.255.0	
The	ОК	Cancel Help	
	500	DIECTROSK.	
		< Back Next > Finish Cancel	Help

Paso 9. Verifique la configuración del conjunto y haga clic en Next (Siguiente).

VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate Network	Tunnel Group Name : DefaultRAGroup
THE THE	Pool Name: Address-pool New
	Pool Settings
2444111III	Range Start Address: 192.168.1.1
T	Range End Address: 192.168.1.254
	Subnet Mask: 255.255.255.0
	<pre>< Back Next > Finish Cancel Help</pre>

Paso 10. Configure los atributos que se enviarán a los clientes o déjelos vacíos y haga clic en Siguiente.

T VPN Wizard		×	
VPN Wizard	Attributes Pushed to Client (Optional) (S	itep 7 of 11)	
Branch	Attributes you configure below are pushed ASA. If you do not want an attribute push	d to the VPN client when the client connects to the ned to the client, leave the corresponding field blank.	
Corporate Home	Tunnel Group:	DefaultRAGroup	
No.	Primary DNS Server:	8.8.8.8	
	Secondary DNS Server:	4.4.4.2	
- Internet	Primary WINS Server:		
	Secondary WINS Server:		
	Default Domain Name:	cisco.com	
		< Back Next > Finish Cancel Help	

Paso 11: Asegúrese de que la casilla Enable Perfect Forwarding Secrecy (PFS) no esté marcada, ya que algunas plataformas cliente no admiten esta función. Habilite la tunelización dividida para permitir que los usuarios remotos tengan acceso cifrado simultáneo a los recursos definidos anteriormente, y el acceso no cifrado a la casilla de Internet está desmarcado, lo que significa que la tunelización completa está habilitada en la cual todo el tráfico (incluido el tráfico de Internet) de la máquina cliente se enviará al ASA a través del túnel VPN. Haga clic en Next (Siguiente).

Te VPN Wizard	×
VPN Wizard	IPsec Settings (Optional) (Step 8 of 11)
Branch Br	Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN. To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the Exempt Networks field blank.
Corporate Network	Interface: outside Exempt Networks: .
6	Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.
	Enable Perfect Forwarding Secrecy (PFS) Diffie-Hellman Group:
	< <u>Back</u> <u>Next</u> > <u>Finish</u> <u>Cancel</u> <u>Help</u>

Paso 12. Revise la información de resumen y, a continuación, haga clic en Finalizar.



Configuración ASA con CLI

Paso 1. Configure los parámetros de política IKE Fase 1.

Esta política se utiliza para proteger el tráfico de control entre los pares (es decir, protege la clave previamente compartida y las negociaciones de la fase 2)

```
ciscoasa(config)#crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)#authentication pre-share
ciscoasa(config-ikev1-policy)#encryption 3des
ciscoasa(config-ikev1-policy)#hash sha
ciscoasa(config-ikev1-policy)#group 2
ciscoasa(config-ikev1-policy)#lifetime 86400
ciscoasa(config-ikev1-policy)#exit
Paso 2. Configure Transform-set.
```

Contiene los parámetros de política de la Fase 2 IKE que se utilizan para proteger el tráfico de datos. Dado que el cliente de Windows L2TP/IPsec utiliza el modo de transporte IPsec, configure el modo para transportar. El valor predeterminado es el modo de túnel

ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport **Paso 3. Configure el mapa dinámico.**

A medida que los clientes de Windows obtienen una dirección IP dinámica para el ISP o el

servidor DHCP local (ejemplo módem), ASA no conoce la dirección IP del par y esto plantea un problema en la configuración de un peer estático en el extremo ASA. Por lo tanto, debe abordarse la configuración criptográfica dinámica en la que no se definen necesariamente todos los parámetros y después se aprenden dinámicamente los que faltan, como resultado de la negociación IPSec del cliente.

ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA Paso 4. Enlazar mapa dinámico a mapa criptográfico estático y aplicar el mapa criptográfico y habilitar IKEv1 en la interfaz externa

El mapa criptográfico dinámico no se puede aplicar en una interfaz y, por lo tanto, enlazarlo a un mapa criptográfico estático. Los conjuntos criptográficos dinámicos deben ser los mapas criptográficos de menor prioridad en el conjunto de mapas criptográficos (es decir, deben tener los números de secuencia más altos) para que el ASA evalúe primero otros mapas criptográficos. Examina el conjunto de mapas criptográficos dinámicos sólo cuando las otras entradas de mapa (estáticas) no coinciden.

ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map ciscoasa(config)#crypto map outside_map interface outside ciscoasa(config)#crypto ikev1 enable outside Paso 5. Crear conjunto de direcciones IP

Cree un conjunto de direcciones desde las cuales las direcciones IP se asignan dinámicamente a los clientes VPN remotos. Ignore este paso para utilizar el conjunto existente en ASA.

```
ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0
Paso 6. Configurar la política de grupo
```

Identifique la política de grupo como interna, lo que significa que los atributos se extraen de la base de datos local.

ciscoasa(config)#group-policy L2TP-VPN internal

Nota: Las conexiones L2TP/IPsec se pueden configurar con una política de grupo predeterminada (DfltGrpPolicy) o con una política de grupo definida por el usuario. En cualquier caso, la política de grupo debe configurarse para utilizar el protocolo de tunelización L2TP/IPsec. configure l2tp-ipsec en el atributo de protocolo VPN en la política de grupo predeterminada que se heredará a la política de grupo definida por el usuario si el atributo vpn-protocol no está configurado en ella.

Configure atributos como el protocolo de túnel vpn (en nuestro caso, es l2tp-ipsec), el nombre de dominio, la dirección IP del servidor DNS y WINS y las nuevas cuentas de usuario

Configure los nombres de usuario y las contraseñas en el dispositivo además de utilizar AAA. Si el usuario es un cliente L2TP que utiliza Microsoft CHAP versión 1 o versión 2, y el ASA está configurado para autenticarse contra la base de datos local, se debe incluir la palabra clave mschap. Por ejemplo, username <username>password <password>mschap.

ciscoasa(config)#group-policy L2TP-VPN attributes

ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2

ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec

ciscoasa(config-group-policy)#default-domain value cisco.com

ciscoasa(config-group-policy)# username test password test mschap
Paso 7. Configure tunnel-group

Cree un grupo de túnel con el comando **tunnel-group**, y especifique el nombre del conjunto de direcciones local utilizado para asignar la dirección IP al cliente. Si el método de autenticación es una clave previamente compartida, el nombre del grupo de túnel debe ser DefaultRAGroup, ya que no hay opción en el cliente para especificar el grupo de túnel y, por lo tanto, sólo aterriza en el grupo de túnel predeterminado. Enlazar la política de grupo al grupo de túnel mediante el comando default-group-policy

```
ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes
ciscoasa(config-tunnel-general)#address-pool Address-pool
ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN
ciscoasa(config-tunnel-general)#exit
```

Nota: Se debe configurar el perfil de conexión predeterminado (grupo de túnel), DefaultRAGroup, si se realiza una autenticación previa basada en clave compartida. Si se realiza la autenticación basada en certificados, se puede elegir un perfil de conexión definido por el usuario basado en identificadores de certificado

Utilice el comando **tunnel-group ipsec-Attributes** para ingresar al modo de configuración ipsecattribute a fin de establecer la clave previamente compartida.

```
ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key C!sc0@123
ciscoasa(config-tunnel-ipsec)#exit
```

Configure el protocolo de autenticación PPP con el comando **authentication type** del modo de atributos ppp del grupo de túnel. Inhabilite CHAP que está habilitado de forma predeterminada ya que no se soporta si el servidor AAA está configurado como base de datos local.

ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes ciscoasa(config-ppp)#no authentication chap ciscoasa(config-ppp)#authentication ms-chap-v2 ciscoasa(config-ppp)#exit Paso 8. Configuración de NAT-Exemption

Configure la exención de NAT para que los clientes puedan acceder a los recursos internos conectados a las interfaces internas (en este ejemplo, los recursos internos están conectados a la interfaz interna).

```
ciscoasa(config)#object network L2TP-Pool
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#exit
ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-
Pool no-proxy-arp route-lookup
Ejemplo de Configuración Completo
```

crypto ikev1 policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 exit crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map crypto map outside_map interface outside crypto ikev1 enable outside ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0 group-policy L2TP-VPN internal group-policy L2TP-VPN attributes vpn-tunnel-protocol l2tp-ipsec default-domain value cisco.com username test password test mschap exit tunnel-group DefaultRAGroup general-attributes address-pool Address-pool default-group-policy L2TP-VPN exit tunnel-group DefaultRAGroup ipsec-attributes ikev1 pre-shared-key C!sc0@123 exit tunnel-group DefaultRAGroup ppp-attributes no authentication chap authentication ms-chap-v2 exit object network L2TP-Pool subnet 192.168.1.0 255.255.255.0 exit nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp route-lookup

Configuración del cliente Windows 8 L2TP/IPsec

1. Abra el panel Control y seleccione Centro de redes y recursos compartidos.



2. Elija Configurar una nueva opción de conexión o red.

¥	Network and Sharing Center	-		x
📀 🌛 🝷 🕇 🚆 « All Control P	anel Items 🔸 Network and Sharing Center	✓ C Search Control Panel		Q
Control Panel Home	View your basic network information and	l set up connections		
Change adapter settings	View your active networks			
Change advanced sharing settings	Network 2 Public network	Access type: No Internet access Connections:		
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connect Troubleshoot problems Diagnose and repair network problems, or g	tion; or set up a router or access point. et troubleshooting information.]	
See also				
Internet Options				
Windows Firewall				

3. Elija la opción Conectar a un lugar de trabajo y haga clic en Siguiente.

🔄 🔄 Set Up a Connection or Network	
Choose a connection option	
Connect to the Internet Set up a broadband or dial-up connection to the Internet.	
Set up a new network Set up a new router or access point.	
Connect to a workplace Set up a dial-up or VPN connection to your workplace.	
<u>!</u>	<u>V</u> ext Cancel

□ ×

4. Haga clic en la opción Usar mi conexión a Internet (VPN).



5. Introduzca la dirección IP de la interfaz WAN o FQDN de ASA y cualquier nombre para el adaptador VPN que tenga relevancia local y haga clic en **Crear**.

			-		<u>^</u>
€	Connect to a Workpl	ace			
	Type the Internet addre	ess to connect to			
	Your network administrator c	an give you this address.	_		
	Internet address:	172.16.1.2	1		
	Destination name:	L2TP VPN	L		
	Use a smart card				
	 Remember my creder 	ntials			
	🌏 🗌 Allow other people to	use this connection			
	This option allows any	yone with access to this computer to use this connection.			
		Creat	2	Cano	cel

6. En Network and Sharing Center, elija la opción **Cambiar configuración del adaptador** en el panel izquierdo de la ventana.

2	Network and Sharing Cente	er 🗕 🗆 🗙			
(→ ▼ ↑ 🖳 « All Control Panel Items → Network and Sharing Center ∨ C Search Control Panel					
Control Panel Home Change adapter settings	View your basic network information View your active networks	and set up connections			
Change advanced sharing settings	Network 2 Public network	Access type: No Internet access Connections: Up Ethernet			
	Change your networking settings				
 Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information. 					

7. Haga clic con el botón derecho del ratón en el adaptador recientemente creado para VPN L2TP y elija **Propiedades.**



8. Vaya a la ficha **Seguridad**, elija el tipo de VPN como **protocolo de túnel de capa 2 con IPsec (L2TP/IPsec)** y, a continuación, haga clic en **Parámetros avanzados.**

L2TP VPN Properties				
General Options Security Networking Sharing				
Type of VPN:				
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)				
Advanced settings				
Require encryption (disconnect if server declines)				
Authentication				
O Use Extensible Authentication Protocol (EAP)				
✓				
Properties				
O Allow these protocols				
Unencrypted password (PAP)				
Challenge Handshake Authentication Protocol (CHAP)				
Microsoft CHAP Version 2 (MS-CHAP v2)				
Automatically use my Windows logon name and password (and domain, if any)				
OK Cancel				

9. Ingrese la clave previamente compartida como la misma mencionada en el grupo de túnel **DefaultRAGroup** y haga clic en **Aceptar**. En este ejemplo, C!sc0@123 se utiliza como clave previamente compartida.

Advanced Properties
L2TP
Use preshared key for authentication Key: C!sc0@123
○ Use certificate for authentication ✓ Verify the Name and Usage attributes of the server's certificate
OK Cancel

10. Elija el método de autenticación como Permitir estos protocolos y asegúrese de que solamente la casilla de verificación **Microsoft CHAP Version 2 (MS-CHAP v2)** esté marcada y haga clic en **Aceptar**.

L2TP VPN Properties
General Options Security Networking Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)
Advanced settings
Require encryption (disconnect if server declines)
O Use Extensible Authentication Protocol (EAP)
 Allow these protocols Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP) Microsoft CHAP Version 2 (MS-CHAP v2) Automatically use my Windows logon name and password (and domain, if any)
OK Cancel

11. En Conexiones de red, haga clic con el botón derecho del ratón en el adaptador VPN L2TP y elija Conectar/Desconectar.



12. Aparecerá el icono Networks y haga clic en Connect en la conexión VPN L2TP.



13. Introduzca las credenciales del usuario y haga clic en Aceptar.

Networks
Connecting to 172.16.1.2
Network Authentication
User name
Password
Domain:
OK Cancel

Si los parámetros requeridos coinciden en ambos extremos, se establecerá la conexión L2TP/IPsec.



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) asociada a esta función. El tráfico para las subredes o los hosts que se define en esta ACL se cifra a través del túnel desde el extremo del cliente, y las rutas para estas subredes se instalan en la tabla de ruteo del PC. ASA intercepta el mensaje DHCPINFORM de un cliente y responde con la máscara de subred, el nombre de dominio y las rutas estáticas sin clase.

Configuración en ASA

ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0 ciscoasa(config)# group-policy DefaultRAGroup attributes ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable

Configuración en el cliente L2TP/IPsec

1. Haga clic con el botón derecho del ratón en el adaptador VPN L2TP y elija Propiedades.



2. Vaya a la ficha Networking (Redes), elija Internet Protocol Version 4 (TCP/IPv4) (Protocolo de Internet versión 4 [TCP/IPv4]) y, a continuación, haga clic en **Properties (Propiedades).**

L2TP VPN Properties	×				
General Options Security Networking Sharing					
This connection uses the following items:					
Internet Protocol Version 6 (TCP/IPv6)	11				
Internet Protocol Version 4 (TCP/IPV4) Image: A standard Control of	• •				
Client for Microsoft Networks					
Install Ninstall Properties	11				
Description	- 1				
Transmission Control Protocol /Internet Protocol The default					
wide area network protocol that provides communication					
across diverse interconnected networks.					
OK Cance	1				

3. Haga clic en la opción Avanzado.

Internet Protocol Version 4 (T	CP/IPv4) Properties ? ×
General	
You can get IP settings assigned auto supports this capability. Otherwise, yo administrator for the appropriate IP se	omatically if your network ou need to ask your network ttings.
Obtain an IP address automatica	ally
Use the following IP address:	
IP address:	· · ·
Obtain DNS server address auto Use the following DNS server ad Preferred DNS server:	ddresses:
Alternate DNS server:	
	Advanced OK Cancel

4. Desmarque la opción Usar gateway predeterminado en la red remota y haga clic en Aceptar.

Advanced TCP/IP Settings ? ×
IP Settings DNS WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network Disable class based route addition
Automatic metric Interface metric:
OK Cancel

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Nota: La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

• show crypto ikev1 sa - Muestra todas las SA IKE actuales en un par.

```
ciscoasa# show crypto ikev1 sa
IKEv1 SAs:
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
```

Total IKE SA: 1

1 IKE Peer:

10.1.1.2

Type : user Role : responder Rekey : no

State : MM_ACTIVE

• show crypto ipsec sa - Muestra todas las SA IPsec actuales en un par.

ciscoasa# show crypto ipsec sa interface: outside Crypto map tag:

outside_dyn_map

, seq num: 10, local addr: 172.16.1.2

local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

17/1701

)

remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/

17/1701

)

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

dynamic allocated peer ip(ipv6): 0.0.0.0

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0

```
#TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
 #send errors: 0, #recv errors: 0
 local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0
 path mtu 1500, ipsec overhead 58(36), media mtu 1500
 PMTU time remaining (sec): 0, DF policy: copy-df
 ICMP error validation: disabled, TFC packets: disabled
 current outbound spi: E8AF927A
 current inbound spi : 71F346AB
inbound esp sas:
 spi: 0x71F346AB (1911768747)
    transform: esp-3des esp-sha-hmac no compression
    in use settings ={RA, Transport, IKEv1, }
    slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
    sa timing: remaining key lifetime (kB/sec): (237303/3541)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x0000003
outbound esp sas:
  spi: 0xE8AF927A (3903820410)
    transform: esp-3des esp-sha-hmac no compression
    in use settings ={RA, Transport, IKEv1, }
    slot: 0, conn_id: 4096, crypto-map: outside_dyn_map
    sa timing: remaining key lifetime (kB/sec): (237303/3541)
    IV size: 8 bytes
    replay detection support: Y
    Anti replay bitmap:
     0x0000000 0x0000001
```

• show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverlpSec - Muestra información detallada sobre L2TP a través de conexiones IPSec.

ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed

Username : test

Index : 1

Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

Protocol	:	IKEv1 IPsec L2T	POverIPs	sec			
License	:	Other VPN					
Encryption	:	IKEv1: (1)3DES	IPsec:	(1)3DES	L2TPO	verIPsec:	(1)none
Hashing	:	IKEv1: (1)SHA1	IPsec:	(1)SHA1	L2TPO	verIPsec:	(1)none
Bytes Tx	:	1574		Bytes Rx	:	12752	
Pkts Tx	:	29		Pkts Rx	:	118	
Pkts Tx Drop	:	0		Pkts Rx I	Drop :	0	

```
Group Policy : L2TP-VPN
```

Tunnel Group : DefaultRAGroup

Duration : 0h:04m:05s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a6a2577000010005557d3a0 Security Grp : none IKEv1 Tunnels: 1 IPsec Tunnels: 1

IKEv1:

L2TPOverIPsec Tunnels: 1

Tunnel ID : 1.1 UDP Src Port : 500 UDP Dst Port : 500 Auth Mode : preSharedKeys Hashing : SHA1 IKE Neg Mode : Main Encryption : 3DES Rekey Int (T): 28800 Seconds Rekey Left(T): 28555 Seconds D/H Group : 2 Filter Name :

IPsec:

Tunnel ID :	1.2		
Local Addr :	172.16.1.2/255.255.255	.255/17/1701	
Remote Addr :	10.1.1.2/255.255.255.2	55/17/1701	
Encryption :	3DES	Hashing :	SHA1
Encapsulation:	Transport		
Rekey Int (T):	3600 Seconds	Rekey Left(T):	3576 Seconds
Rekey Int (D):	250000 K-Bytes	Rekey Left(D):	250000 K-Bytes
Idle Time Out:	30 Minutes	Idle TO Left :	29 Minutes
Bytes Tx :	1574	Bytes Rx :	12752
Pkts Tx :	29	Pkts Rx :	118

L2TPOverIPsec:

Tunnel ID : 1.3

Username : test

Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

Idle Time	Out:	30 Minutes	Idle TO Left	:	27 Minutes
Client OS	:	Microsoft			
Client OS	Ver:	6.2			
Bytes Tx	:	475	Bytes Rx	:	9093
Pkts Tx	:	18	Pkts Rx	:	105

En ASDM, bajo **Monitoring > VPN > VPN Statistics > Sessions** se puede ver la información general relacionada con la sesión VPN. El **acceso remoto IPsec (IKEv1)** puede filtrar las sesiones L2TP a través de IPsec > Protocolo > L2TP a través de IPsec.

File View Tools Wizards Window Help						
🕙 home of Configuration 🔂 Monitores 💭 Monitores 🖓 Refeati 💿 State 💿 Formand 🦿 refe						
Device List 🗗 🕂 🛪	Monitoring > VPN > VPN Statistics > Sessions					
🗣 Add 📋 Delete 🚿 Connect						
Find: Go	Type Actve Comulative Peek Concurrent Inactive					
	VEv1 Prec(JZPP Prec 1 15 1 Fiter By: [Psec(JJE v1) Remote Access •] Protocol • [LZPP Over Prec •] Fiter					
VPN Statistics	Usemane Group Policy Assigned IP Address Protocol Logn Time Olent(Peer) Type Bytes Tx NAC Result Connection Profile Public/eper (Public/eper) Paddress Enroyston Duration Version Bytes Tx Potaure Token	Details				
VPN Curter Loads Compression Statistics Compression Statistics Compression Statistics Global DEC(Press: Statistics No.Coexino Summary Protocol Statistics Vi-N4 Mapping Seasions Vi-N4 Mapping Seasions	nez befuziek/kowo (1922-1843.1.1) Debut precit/2020-456.111/C Sattky 9 2015 Monzolt (422 Jakowon Defuziek/Kowo (44.103.208.179 Debut (1.03063 Preci (1.040.0306238 (4.1 Preci (1.040.0306238	Ping				

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un comando debug.

Precaución: En el ASA, puede establecer varios niveles de depuración; de forma predeterminada, se utiliza el nivel 1. Si cambia el nivel de depuración, la verbosidad de las depuraciones podría aumentar. Haga esto con precaución, especialmente en entornos de producción.

Utilice los siguientes **comandos debug con precaución** para resolver los problemas con el túnel VPN

- debug crypto ikev1 muestra información de depuración sobre IKE
- debug crypto ipsec muestra información de depuración sobre IPsec

Este es el resultado de debug para una conexión L2TP exitosa sobre IPSec:

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13)
```

May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group Description: Rcv'd: Unknown Cfg'd: Group 2 May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Oakley proposal is acceptable May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal RFC VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received Fragmentation VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group Description: Rcv'd: Unknown Cfg'd: Group 2 May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group Description: Rcv'd: Unknown Cfg'd: Group 2 May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended capabilities payload May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124 May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260 May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 2000001) May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash May 18 04:17:18 [IKEv1]IP = 10.1.1.2,

Connection landed on tunnel_group DefaultRAGroup

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for Responder... May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 304

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keepalives (type = None) May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds. May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500 May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300 May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

PSec SA Proposal # 2, Transform # 1 acceptable

Matches global IPSec SA entry # 10 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI! IPSEC: New embryonic SA created @ 0x00007fffe13ab260, SCB: 0xE1C00540, Direction: inbound SPI : 0x7AD72E0D Session ID: 0x00001000 VPIF num : 0x0000002 Tunnel type: ra Protocol : esp : 240 seconds Lifetime May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine: SPI = 0x7ad72e0dMay 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick mode May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce pavload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd
QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR
+ HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
```

encrypt_rule=00000000; tunnelFlow_rule=00000000 May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key! IPSEC: New embryonic SA created @ 0x00007fffe1c75c00, SCB: 0xE13ABD20, Direction: outbound SPT : 0x8C14FD70 Session ID: 0x00001000 VPIF num : 0x0000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x8C14FD70 IPSEC: Creating outbound VPN context, SPI 0x8C14FD70 Flags: 0x00000205 SA : 0x00007fffe1c75c00 SPI : 0x8C14FD70 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x0AC609F9 Channel: 0x00007fffed817200 IPSEC: Completed outbound VPN context, SPI 0x8C14FD70 VPN handle: 0x000000000028d4 IPSEC: New outbound encrypt rule, SPI 0x8C14FD70 Src addr: 172.16.1.2 Src mask: 255.255.255.255 Dst addr: 10.1.1.2 Dst mask: 255.255.255.255

Src ports

Upper: 1701

Lower: 1701

Op : equal

Dst ports

Upper: 1701

Lower: 1701

Op : equal

Protocol: 17

```
Use protocol: true
  SPI: 0x0000000
   Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
  Src addr: 172.16.1.2
   Src mask: 255.255.255.255
  Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
   Src ports
    Upper: 0
    Lower: 0
    Op : ignore
   Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x8C14FD70
   Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User () Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
   SCB: 0xE1C00540,
  Direction: inbound
  SPI
       : 0x7AD72E0D
  Session ID: 0x00001000
  VPIF num : 0x0000002
  Tunnel type: ra
  Protocol : esp
   Lifetime
             : 240 seconds
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
   Flags: 0x0000206
   SA : 0x00007fffe13ab260
  SPI : 0x7AD72E0D
  MTU : 0 bytes
   VCID : 0x0000000
  Peer : 0x000028D4
  SCB : 0x0AC5BD5B
   Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
   VPN handle: 0x000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x00000205
   SA : 0x00007fffe1c75c00
   SPI : 0x8C14FD70
  MTU : 1500 bytes
  VCID : 0x0000000
```

```
Peer : 0x00004174
  SCB : 0x0AC609F9
  Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
  VPN handle: 0x000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c76a00
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 1701
    Lower: 1701
    Op : equal
  Dst ports
    Upper: 1701
    Lower: 1701
    Op : equal
  Protocol: 17
  Use protocol: true
  SPI: 0x0000000
  Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
  Use protocol: true
  SPI: 0x7AD72E0D
  Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
   Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
   Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
   Use protocol: true
   SPI: 0x7AD72E0D
   Use SPI: true
```

```
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

PHASE 2 COMPLETED

```
(msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,
```

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1 En esta tabla se muestran algunos de los errores relacionados con VPN más frecuentes en el cliente de Windows

Código
de errorSoluciones posibles691Asegúrese de que el nombre de usuario y la contraseña introducidos sean correctos789,835Asegúrese de que la clave previamente compartida configurada en el equipo cliente sea la mis
que en ASA8001. Asegúrese de que el tipo de VPN esté configurado en "Layer 2 Tunneling Protocol (L2TP)"
2. Asegúrese de que la clave previamente compartida esté configurada correctamente809Asegúrese de que el puerto UDP 500, 4500 (en caso de que el cliente o el servidor se encuent
detrás del dispositivo NAT) y el tráfico ESP no se haya blogueado

Información Relacionada

- <u>Cisco ASA 5500 Series Adaptive Security Appliances</u>
- Soluciones y Troubleshooting para los Problemas más Comunes con VPN IPSec de Acceso Remoto y L2L
- Soporte Técnico y Documentación Cisco Systems