

PIX/ASA 7.x y IOS: Fragmentación VPN

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Productos Relacionados](#)

[Convenciones](#)

[Antecedentes](#)

[Problemas con la fragmentación](#)

[Tarea principal](#)

[Descubra la fragmentación](#)

[Soluciones a los problemas de Fragmentation](#)

[Verificación](#)

[Troubleshooting](#)

[Error de encriptación VPN](#)

[Problemas RDP y del Citrix](#)

[Información Relacionada](#)

[Introducción](#)

Este documento le guía en los pasos necesarios para solventar los problemas que pueden ocurrir con la fragmentación de un paquete. Un ejemplo de problemas de fragmentación es la capacidad de hacer ping en un recurso conectado a la red, pero la incapacidad de conectar con ese mismo recurso con una aplicación específica, tal como el correo electrónico o las bases de datos.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

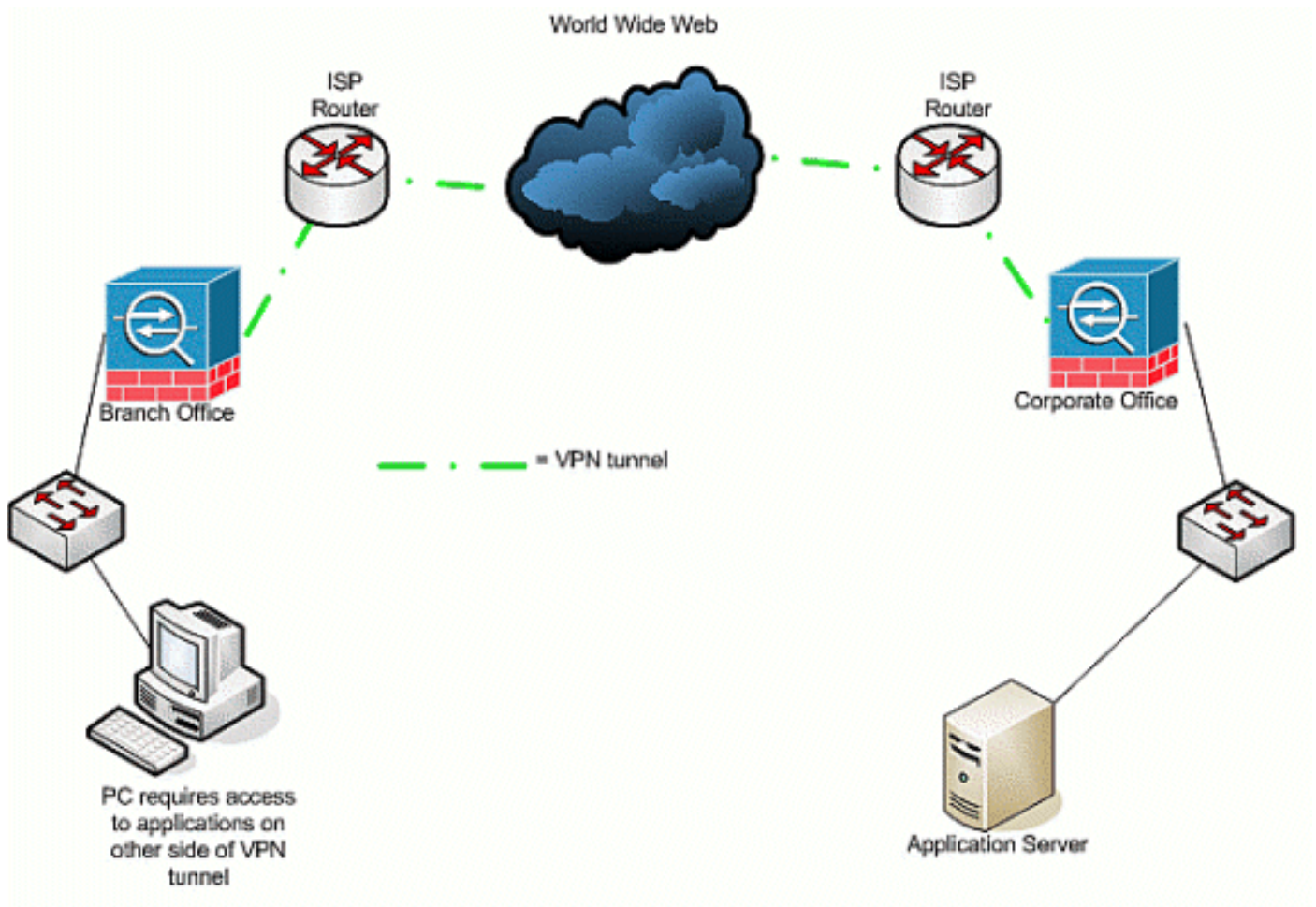
- Conectividad entre los pares VPN

[Componentes Utilizados](#)

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Productos Relacionados

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

- Routers IOS
- Dispositivos de seguridad del PIX/ASA

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El IP soporta un Largo máximo de 65,536 bytes para un paquete del IP, pero la mayoría de los protocolos de la capa de link de datos soportan una longitud mucho más pequeña, llamada una Unidad máxima de transmisión (MTU) (MTU). De acuerdo con el MTU soportado, puede ser necesario romper para arriba (fragmento) un paquete del IP para transmitirlo a través de un tipo de media determinado de la capa del link de datos. El destino entonces tiene que volver a montar los fragmentos nuevamente dentro del paquete del IP original, completo.

Protocol	Additional Bytes
ESP (encryption and hash)	56
AH	24+
GRE	24
NAT-T/IPsec over UDP (UDP part)	8
IPsec over TCP (TCP part)	20
L2TP	12
PPTP	48
Outer IP header in IPsec tunnel mode or PPTP/L2TP	20
PPPoE	8

Cuando usted utiliza un VPN para proteger los datos entre dos pares VPN, los gastos indirectos adicionales se agregan a las informaciones originales, que pueden requerir que ocurra la fragmentación. Campos de esta lista de la tabla que potencialmente tienen que ser agregados a los datos protegidos para soportar una conexión VPN. Observe que los protocolos múltiples pueden ser necesarios, que aumenta el tamaño del paquete original. Por ejemplo, si usted utiliza un L2L DMVPN conexión IPsec entre dos routers Cisco, donde usted ha implementado un túnel GRE, usted necesita estos gastos indirectos adicionales: ESP, GRE, y el encabezado IP externo. Si usted tiene una conexión del software cliente del IPsec a un gateway de VPN cuando el tráfico pasa a través de un dispositivo del direccionamiento, usted necesita estos gastos indirectos adicionales para el Traversal de la traducción de la dirección de red (NAT-T), así como el encabezado IP externo para la conexión del modo túnel.

[Problemas con la fragmentación](#)

Cuando la fuente envía un paquete a un destino, pone un valor en el campo de los indicadores de control de los encabezados IP que afecta a la fragmentación del paquete por los dispositivos intermedios. El indicador de control es tres bits de largo, pero solamente el primeros dos se utilizan en la fragmentación. Si el segundo bit se fija a 0, el paquete se permite ser hecho fragmentos; si se fija a 1, el paquete no se permite ser hecho fragmentos. El segundo bit se llama comúnmente el bit del *don't fragment (DF)*. El tercer bit especifica cuando ocurre la fragmentación, independientemente de si este paquete fragmentado es el fragmento más reciente (fije a 0), o si hay más fragmentos (fije a 1) que componen el paquete.

Hay cuatro áreas que pueden crear los problemas cuando se requiere la fragmentación:

- Los gastos indirectos adicionales en los ciclos de la CPU y la memoria son requeridos por los dos dispositivos que realizan la fragmentación y el nuevo ensamble.
- Si un fragmento se cae en la manera al destino, el paquete no puede ser vuelto a montar y el paquete entero se debe hacer fragmentos y enviar otra vez. Esto crea los problemas de caudal adicionales, especialmente en las situaciones donde está tarifa limitada el tráfico en la pregunta, y la fuente envía el tráfico sobre el límite permisible.
- El filtrado de paquetes y los escudos de protección con estado pueden tener dificultad que

procesa los fragmentos. Cuando ocurre la fragmentación, el primer fragmento contiene un encabezado IP externo, el encabezado interno, tal como TCP, UDP, ESP y otros, y parte del payload. Los fragmentos subsiguientes del paquete original contratan un encabezado IP externo y la continuación del payload. El problema con este proceso es que ciertos Firewall necesitan ver la información de encabezado interno en cada paquete para tomar las decisiones de filtración inteligentes; si esa información falta, pueden caer inadvertidamente todos los fragmentos, a excepción primer.

- La fuente en el encabezado IP del paquete puede fijar el tercer control mordido al *Don't Fragment*, así que significa que, si un dispositivo intermedio recibe el paquete y debe hacer fragmentos de él, el dispositivo intermedio no puede hacer fragmentos de él. En lugar, el dispositivo intermedio cae el paquete.

Tarea principal

Descubra la fragmentación

La mayoría de las redes utilizan los Ethernetes, con un valor del MTU predeterminado de 1,500 bytes, que se utiliza típicamente para los paquetes del IP. Para descubrir si la fragmentación ocurre o es necesaria pero no puede ser hecha (se fija el bit DF), primero saque a colación a su sesión de VPN. Entonces usted puede utilizar de estos cuatro procedimientos para descubrir la fragmentación.

1. Haga ping un dispositivo localizado en el otro extremo. Éste es bajo suposición que el hacer ping está permitido a través del túnel. Si esto es acertado, intente acceder una aplicación a través del mismo dispositivo; por ejemplo, si un servidor del email o del Escritorio Remoto de Microsoft está a través del túnel, la perspectiva abierta e intenta descargar su email, o intenta al Escritorio Remoto al servidor. Si esto no trabaja, y usted tiene la resolución de nombre correcta, hay una buena ocasión que la fragmentación es el problema.
2. De un dispositivo de Windows utilice esto: `C:\ > ping - f - l destination_IP_address de los packet_size_in_bytes`. - La opción **f** se utiliza para especificar que el paquete no puede ser hecho fragmentos. - La opción **L** se utiliza para especificar la longitud del paquete. Primero intente esto con un tamaño de paquetes de 1,500. Por ejemplo, `ping - f - l 1500 192.168.100`. Si la fragmentación se requiere pero no puede ser realizada, usted recibe un mensaje tal como esto: *Los paquetes necesitan ser hechos fragmentos pero conjunto DF*.
3. En los routers Cisco, ejecute el **comando debug ip icmp** y utilice el **comando extended ping**. Si usted ve el *ICMP: dst (x.x.x.x) la fragmentación necesaria y el DF para fijar, inalcanzable enviado al y.y.y.y*, donde está un dispositivo de destino x.x.x.x, y el y.y.y.y es su router, un dispositivo intermedio le dice que la fragmentación es necesaria, pero porque usted fija el DF mordido en el pedido de eco, un dispositivo intermedio no puede hacer fragmentos de él para remitirlo al salto siguiente. En este caso, disminuya gradualmente la talla del MTU de los ping hasta que usted encuentre uno que trabaje.
4. En los dispositivos del Cisco Security, utilice un filtro de la captura.
el permiso más
`outside_test tcp ninguno de la ciscoasa(config)#access-lista` recibe el eq 80 de
172.22.1.1 **Note:** Cuando usted deja la fuente como *ningunos*, permite que el administrador monitoree cualquier traducción de direcciones de red (NAT).
el eq más `outside_test 80 de`
172.22.1.1 del `host tcp del permiso de la ciscoasa(config)#access-lista` **Note:** Cuando usted invierte la información de origen y destino, permite que el tráfico de retorno sea capturado.
la
interfaz más `outside_test` de la lista de acceso del `outside_interface` de la captura del

```
ciscoasa(config)# afuera
```

El usuario necesita iniciar una nueva sesión con la aplicación X. Después de que el usuario haya iniciado una sesión de la nueva aplicación X, el administrador ASA necesita publicar el comando del **outside_interface de la captura de la demostración**.

Soluciones a los problemas de Fragmentation

Hay maneras diferentes que usted puede solucionar los problemas con la fragmentación. Éstos se discuten en esta sección.

Método 1: Configuración de MTU estática

La configuración de MTU estática puede solucionar los problemas con la fragmentación.

1. **El MTU cambia en el router:** Observe que si usted fija manualmente el MTU en el dispositivo, dice el dispositivo, que actúa como gateway de VPN, para hacer fragmentos de los paquetes recibidos antes de que los proteja y envíe a través del túnel. Esto es preferible al tener el router protege el tráfico y después hace fragmentos de él, pero el dispositivo hace fragmentos de él. **Advertencia:** Si usted cambia la talla del MTU en cualquier interfaz de dispositivo, causa todos los túneles terminados en esa interfaz que se derribará y reconstruida. En los routers Cisco, utilice el **mtucommand del IP** para ajustar la talla del MTU en la interfaz donde se termina el VPN:

```
router (config)# interface type [slot_#/] port_#  
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **El MTU cambia en ASA/PIX:** En ASA/PIX los dispositivos, utilice el **mtucommand** para ajustar la talla del MTU en el modo de configuración global. Por abandono, el MTU se fija a 1500. Por ejemplo, si usted tenía una interfaz en su dispositivo de seguridad que fue nombrado *Outside (donde se termina el VPN)*, y usted determinó (con las medidas enumeradas en la sección de la [fragmentación del descubrimiento](#)) que usted quiso utilizar 1380 como el tamaño del fragmento, utiliza este comando:

```
security appliance (config)# mtu Outside 1380
```

Método 2: Maximum Segment Size TCP

El Maximum Segment Size TCP puede solucionar los problemas con la fragmentación.

Note: Esta característica trabaja solamente con el TCP; otros protocolos IP tienen que utilizar otra solución para solucionar fragmentación de IP los problemas. Incluso si usted fija el MTU del IP en el router, no afecta a lo que negocian los hosts de los dos extremos dentro de la entrada en contacto de tres vías TCP con TCP MSS.

1. **El MSS cambia en el router:** La fragmentación ocurre con tráfico TCP porque tráfico TCP se utiliza normalmente para transportar una gran cantidad de datos. El TCP soporta una característica llamada el Maximum Segment Size TCP (MSS) que permita que los dos dispositivos negocien un tamaño conveniente para tráfico TCP. El valor MSS se configura estáticamente en cada dispositivo y representa el tamaño de almacén intermedio para utilizar para un paquete previsto. Cuando dos dispositivos establecen las conexiones TCP

comparan el valor local MSS con el valor local MTU dentro de la entrada en contacto de tres vías; cualquiera es más bajo se envía al peer remoto. Los dos pares entonces utilizan el más bajo de los dos valores intercambiados. Para configurar esta característica, haga esto: En los routers Cisco, utilice el **tcp adjust-mss** el comando en la interfaz en la cual se termina el VPN.

```
router (config)# interface type [slot_#/] port_#  
router (config-if)# ip tcp adjust-mss MSS_size_in_bytes
```

2. **El MSS cambia en ASA/PIX:** Para asegurarse de que el tamaño del segmento del máximo TCP no exceda el valor que usted fija y de que el máximo es no menos que al tamaño especificado, utilice el **comando connection del sysopt** en el modo de configuración global. Para restablecer la configuración predeterminada, utilice la forma del theno de este comando. El valor máximo predeterminado es 1380 bytes. La característica mínima se inhabilita por abandono (fije a 0). Para cambiar el máximo predeterminado del límite MSS, haga esto:

```
security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
```

Note: Si usted fija el tamaño máximo para ser mayor de 1380, los paquetes pueden hacerse fragmentos, dependiente sobre la talla del MTU (que es 1500 por abandono). Un gran número de fragmentos pueden afectar el funcionamiento del dispositivo de seguridad cuando utiliza la función de protección del Frag. Si usted fija el tamaño mínimo, evita que el servidor TCP el envío de muchos pequeños paquetes de datos de TCP al cliente y afecte el funcionamiento del servidor y de la red. Para cambiar el límite del mínimo MSS, haga esto:

```
security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
```

dispositivo de seguridad (config) # mínimo MSS_size_in_bytes de TCP-mss de la conexión del sysopt **Note:** Refiera a la [configuración MPF para permitir los paquetes que exceden la sección MSS del problema del PIX/ASA 7.X del documento: MSS excedido - Los clientes HTTP no pueden hojear a algunos sitios web](#) para más información para no prohibir a los paquetes excedidos MSS otro método.

[Método 3: Detección de MTU de trayecto \(PMTUD\)](#)

El PMTUD puede solucionar los problemas con la fragmentación.

El problema principal con TCP MSS es que el administrador tiene que saber qué valor a configurar en su router para prevenir el acontecimiento de la fragmentación. Esto puede ser un problema si más de una trayectoria existe entre usted y la ubicación del telecontrol VPN, o, cuando usted hace su interrogación inicial, usted encuentra que segundo-o un MTU tercero-más pequeño, en vez del más pequeño, está basado en la decisión de ruteo usada dentro de su interrogación inicial. Con el PMTUD, usted puede determinar un valor MTU para los paquetes del IP que evite la fragmentación. Si los mensajes ICMP son bloqueados por un router, el mtu de trayectoria está quebrado, y los paquetes con el conjunto de bits DF se desechan. Utilice el **comando df del IP del conjunto** de borrar el DF mordido y de permitir que envíen el paquete sea hecho fragmentos y. La fragmentación puede reducir la velocidad del reenvío de paquete en la red, pero las Listas de acceso se pueden utilizar para limitar el número de paquetes en los cuales se borre el bit DF.

1. Tres problemas pueden hacer el PMTUD no funcionar: Un router intermedio puede caer el paquete y no responder con un mensaje ICMP. Esto no es muy común en Internet, sino

puede ser común dentro de una red donde configuran al Routers para no responder con los mensajes inalcanzables de ICMP. Un router intermedio puede responder con un mensaje inalcanzable de ICMP, pero, en el flujo de vuelta, un Firewall bloquea este mensaje. Esto es un acontecimiento más común. El mensaje inalcanzable de ICMP hace su manera de nuevo a la fuente, pero la fuente ignora el mensaje de la fragmentación. Esto es el más infrecuente de los tres problemas. Si usted experimenta el primer problema, usted podría cualquiera borrar el DF mordido en el encabezado IP que la fuente puesta allí o manualmente ajusta el tamaño TCP MSS. Para borrar el bit DF, un router intermedio tiene que cambiar el valor a partir de la 1 a 0. que esto es hecha normalmente por un router en su red antes de que el paquete salga de la red. Ésta es una configuración simple del código que hace esto en router basado en el IOS:

```
Router (config) # access-list ACL_# permit tcp any any
Router (config) # route-map route_map_name permit seq#
Router (config-route-map) # match ip address ACL_#
Router (config-route-map) # set ip df 0
Router (config-route-map) # exit
Router (config) # interface type [slot#/]port #
Router (config-if) # ip policy router-map route_map_name
```

2. **PMTUD y túneles GRE** Por abandono, un router no realiza el PMTUD en los paquetes de túnel GRE que genera sí mismo. Para habilitar el PMTUD en las interfaces de túnel GRE y tener el router participar en el MTU que ajusta el proceso para la fuente/los dispositivos de destino para el tráfico que atraviesa el túnel, utilice esta configuración: Router (config) # tunnel_# del túnel de la interfaz Router (config-if) # trayectoria-MTU-detección del túnel El comando **tunnel path-mtu-discovery** habilita el PMTUD para la interfaz de túnel GRE de un router. El parámetro opcional del temporizador de edad especifica el número de minutos después de lo cual la interfaz del túnel reajusta el tamaño del MTU máximo descubierto, menos 24 bytes para el encabezado GRE. Si usted especifica *infinito* para el temporizador, el temporizador no se utiliza. El parámetro minuto-MTU especifica el número mínimo de bytes que comprende el valor MTU.
3. **PIX/ASA 7.x - Borre el don't fragment (DF)** o la manipulación de los archivos o de los paquetes grandes. Usted no puede todavía acceder correctamente Internet, los archivos grandes, o las aplicaciones a través del túnel porque da este mensaje de tamaño-error MTU:

```
PMTU-D packet 1440 bytes greater than effective mtu 1434,
dest_addr=10.70.25.1, src_addr=10.10.97.55, prot=TCP
```

Para resolver esto, esté seguro de borrar el DF mordido de la interfaz exterior del dispositivo. Configure la directiva del DF-bit para los paquetes IPsec con el comando **crypto del DF-bit del IPsec** en el modo de configuración global.

```
pix(config)# crypto ipsec df-bit clear-df outside
```

El bit DF con la característica de los túneles IPsec le deja especificar si el dispositivo de seguridad puede borrar, fijar, o copiar el bit del don't fragment (DF) de la encabezado encapsulada. El bit DF dentro del encabezado IP determina si un dispositivo está permitido hacer fragmentos de un paquete. Utilice el comando **crypto del DF-bit del IPsec** en el modo de configuración global de configurar el dispositivo de seguridad para especificar el bit DF en una encabezado encapsulada. Cuando usted encapsula el tráfico IPsec del modo túnel, utilice la configuración **clear-df** para el bit DF. Esta configuración deja el dispositivo enviar los paquetes más grandes que la talla del MTU disponible. También esta configuración es

apropiada si usted no conoce la talla del MTU disponible.

Note: Si usted todavía experimenta los problemas de fragmentación y los paquetes perdidos, opcionalmente, usted puede ajustar manualmente la talla del MTU con el comando de la **interfaz del túnel MTU del IP**. En este caso, el router hace fragmentos del paquete antes de que lo proteja. Este comando se puede utilizar conjuntamente con PMTUD y/o TCP MSS.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshooting

Error de encriptación VPN

Asuma que el túnel IPsec ha establecido entre el router y el PIX. Si usted ve los mensajes de error de encriptación que los paquetes están caídos, complete estos pasos para resolver el problema:

1. Realice una traza de sniffer del cliente al lado del servidor para descubrir que es el mejor MTU a utilizar. Usted puede también utilizar la prueba de ping:

```
ping -l 1400 192.168.1.1 -f
```

192.168.1.1 es la dirección IP de la máquina remota.

2. Continúe reduciendo el valor de 1400 por 20 hasta que haya una contestación. **Note:** El valor mágico, que trabaja en la mayoría de los casos, es 1300.
3. Después de que se alcance el Maximum Segment Size apropiado, ajústelo apropiadamente para que haya los dispositivos funcionando: En el firewall PIX:

```
sysopt connection tcpmss 1300
```

En el router:

```
ip tcp adjust-mss 1300
```

Problemas RDP y del Citrix

Problema:

Usted puede hacer ping entre las redes VPN, pero las conexiones del protocolo del Escritorio Remoto (RDP) y del Citrix no se pueden establecer a través del túnel.

Solución:

El problema puede ser la talla del MTU en el PC detrás del PIX/ASA. Fije la talla del MTU como 1300 para la máquina del cliente e intente establecer la conexión del Citrix a través del túnel VPN.

Información Relacionada

- [Resolución fragmentación de IP, problemas MTU, MSS, y PMTUD con el GRE y el IPSEC](#)
- [Problema de PIX/ASA 7.0: MSS excedido - Los clientes HTTP no pueden navegar a algunos Web site](#)
- [Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto](#)
- [Porqué no puedo hojear Internet al usar un túnel GRE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)