IOS VPN(Router): Agregue un nuevo túnel o el Acceso Remoto L2L a un L2L existente VPN

Contenido

Introducción

Este documento proporciona los pasos requeridos para agregar un nuevo túnel VPN L2L o VPN de acceso remoto a una configuración VPN L2L que ya exista en un router IOS.

prerrequisitos

Requisitos

Asegúrese de que usted configure correctamente el túnel del IPSec VPN L2L que es actualmente operativo antes de que usted intente esta configuración.

Componentes Utilizados

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

- Dos routeres IOS que funcionan con las versiones de software 12.4 y 12.2
- Un dispositivo de seguridad adaptante de Cisco (ASA) ese funciona con la versión de

software 8.0

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Estas salidas son las Configuraciones actuales de ejecución. del router y de la sucursal 1 (BO1) ASA HQ (CONCENTRADOR). En esta configuración, hay un túnel del IPSec L2L configurado entre HQ y BO1 ASA.

Configuración del router actual HQ (CONCENTRADOR)

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 1680 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!--- Output is suppressed. ! ip cef ! ! crypto isakmp
policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 192.168.11.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
!
!
!
!
```

```
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside


interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
interface Serial2/1
 no ip address
 shutdown
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Configuración BO1 ASA

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
```

```
!--- Output is suppressed. ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive access-list 100 extended
permit ip 172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list nonat extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0
access-list ICMP extended permit icmp any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-602.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 10.10.10.0 255.255.255.0
access-group ICMP in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.11.1 1
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 192.168.10.10
crypto map map1 5 set transform-set newset
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
```

```
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
CiscoASA#
```

Antecedentes

Actualmente, hay una configuración de túnel existente L2L entre la oficina HQ y la oficina BO1. Su compañía ha abierto recientemente una nueva sucursal (BO2). Esta nueva oficina requiere la Conectividad a los recursos locales que están situados en la oficina HQ. Además, hay un requisito adicional de no prohibir a los empleados la oportunidad de trabajar del hogar y de acceder con seguridad los recursos que están situados en la red interna remotamente. En este ejemplo, se configura un nuevo túnel VPN así como un servidor del VPN de acceso remoto que está situado en el oficina HQ.

Agregue un túnel adicional L2L a la configuración

Éste es el diagrama de la red para esta configuración:

Instrucciones Paso a Paso

Esta sección proporciona los procedimientos requeridos que se deben realizar en el router HQ del CONCENTRADOR.

Complete estos pasos:

1. Cree esta nueva lista de acceso que se utilizará por la correspondencia de criptografía para definir el tráfico interesante:`HQ_HUB(config)#`**`ip access-list extended VPN_BO2`**
   `HQ_HUB(config-ext-nacl)#`**`permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255`**
   `HQ_HUB(config-ext-nacl)#`**`exit`**
   Advertencia: Para que la comunicación ocurra, el otro lado del túnel debe tener el contrario de esta entrada del Access Control List (ACL) para esa red determinada.
2. Agregue estas entradas a la ninguna sentencia NAT para eximir nating entre estas redes:`HQ_HUB(config)#`**`ip access-list extended NAT_Exempt`**
   `HQ_HUB(config-ext-nacl)#`**`deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255`**
   `HQ_HUB(config-ext-nacl)#`**`permit ip 10.10.10.0 0.0.0.255 any`**
   Agregue estos ACL al **nonat de la** correspondencia de ruta existente:`HQ_HUB(config)#`**`route-map nonat permit 10`**
   `HQ_HUB(config-route-map)#`**`match ip address NAT_Exempt`**
   `HQ_HUB(config)#`**`ip nat inside source route-map nonat interface Serial2/0 overload`**
   Advertencia: Para que la comunicación ocurra, el otro lado del túnel debe tener el contrario de esta entrada ACL para esa red determinada.
3. Especifique a la dirección de peer en la configuración de la fase 1 como se

muestra:`HQ_HUB(config)#crypto isakmp key cisco123 address 192.168.12.2`
Nota: La clave previamente compartida debe hacer juego exactamente a ambos lados del túnel.

4. Cree la configuración de la correspondencia de criptografía para el nuevo túnel VPN. Utilice lo mismo transforman el conjunto que fue utilizado en la primera configuración VPN, como todas las configuraciones de la fase 2 son lo mismo.
```
HQ_HUB(config)#crypto map map1 10 ipsec-isakmp
 HQ_HUB(config-crypto-map)#set peer 192.168.12.2
 HQ_HUB(config-crypto-map)#set transform-set newset
 HQ_HUB(config-crypto-map)#match address VPN_BO2
```
5. Ahora que usted ha configurado el nuevo túnel, usted debe enviar el tráfico interesante a través del túnel para traerlo para arriba. Para realizar esto, publique el comando extended ping de hacer ping un host en la red interna del túnel remoto.En este ejemplo, un puesto de trabajo en el otro lado del túnel con el direccionamiento 10.20.20.16 se hace ping. Esto trae el túnel para arriba entre el HQ y BO2. Ahora, hay dos túneles conectados con la oficina HQ. Si usted no tiene acceso a un sistema detrás del túnel, refiera a la mayoría del IPSec VPN común L2L y del Acceso Remoto que resuelve problemas las soluciones para encontrar una solución alternativa usando el `Acceso de administración`.

Ejemplo de configuración

HUB_HQ - Agregó una nueva configuración del túnel L2L VPN

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 2230 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_HUB
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef

!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.11.2
crypto isakmp key cisco123 address 192.168.12.2
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
```

```
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!

interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!

ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.10.0 0.0.0.255 any
ip access-list extended VPN_BO1
  permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255




!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Configuración del túnel BO2 L2L VPN

```
BO2#show running-config
Building configuration...
```

```
3w3d: %SYS-5-CONFIG_I: Configured from console by
console
Current configuration : 1212 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname BO2
!
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 group 2
crypto isakmp key cisco123 address 192.168.10.10
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.10.10
 set transform-set newset
 match address 100
!
!
!
!
interface Ethernet0
 ip address 10.20.20.10 255.255.255.0
 ip nat inside
!

!
interface Ethernet1
 ip address 192.168.12.2 255.255.255.0
 ip nat outside
 crypto map map1
!
interface Serial0
 no ip address
 no fair-queue
!
interface Serial1
 no ip address
 shutdown
!
ip nat inside source route-map nonat interface Ethernet1
overload
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.12.1
ip http server
!
access-list 100 permit ip 10.20.20.0 0.0.0.255
```

```
10.10.10.0 0.0.0.255
access-list 150 deny ip 10.20.20.0 0.0.0.255 10.10.10.0
0.0.0.255
access-list 150 permit ip 10.20.20.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 150
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end

BO2#
```

Agregue un VPN de acceso remoto a la configuración

Éste es el diagrama de la red para esta configuración:

En este ejemplo, la característica llamada **Túnel dividido** se utiliza. Esta característica permite que un cliente IPSec del acceso remoto dirija condicional los paquetes sobre un túnel IPsec en la forma encriptada, o a una interfaz de la red en la forma de texto claro. Con el Túnel dividido habilitado, los paquetes no limitados para los destinos en el otro lado del túnel IPsec no tienen que ser cifrados, enviado a través del túnel, desencriptaron, y entonces ruteado a un destino final. Este concepto aplica la directiva del Túnel dividido a una red específicada. El valor por defecto es hacer un túnel todo el tráfico. Para fijar una directiva del Túnel dividido, especifique un ACL donde el tráfico significado para Internet puede ser mencionado.

Instrucciones Paso a Paso

Esta sección proporciona los procedimientos requeridos para agregar la capacidad de Acceso Remoto y para permitir que los usuarios remotos accedan todos los sitios.

Complete estos pasos:

1. Cree un pool de la dirección IP que se utilizará para los clientes que conectan vía el túnel VPN. También, cree a un usuario básico para acceder el VPN una vez que se completa la configuración.`HQ_HUB(config)#`**`ip local pool ippool 10.10.120.10 10.10.120.50`**
   `HQ_HUB(config)#`**`username vpnuser password 0 vpnuser123`**
2. Exima el tráfico específico de nated.`HQ_HUB(config)#`**`ip access-list extended NAT_Exempt`**
   `HQ_HUB(config-ext-nacl)#`**`deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255`**
   `HQ_HUB(config-ext-nacl)#`**`deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255`**
   `HQ_HUB(config-ext-nacl)#`**`deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255`**
   `HQ_HUB(config-ext-nacl)#`**`permit ip host 10.10.10.0 any`**
   `HQ_HUB(config-ext-nacl)#`**`exit`**
   Agregue estos ACL al **nonat de la** correspondencia de ruta existente:`HQ_HUB(config)#`**`route-map nonat permit 10`**
   `HQ_HUB(config-route-map)#`**`match ip address NAT_Exempt`**
   `HQ_HUB(config)#`**`ip nat inside source route-map nonat interface Serial2/0 overload`**
   Note que la comunicación nacional entre los túneles VPN está eximida en este ejemplo.
3. Permita la comunicación entre los túneles L2L y los usuarios existentes del VPN de acceso remoto.`HQ_HUB(config)#`**`ip access-list extended VPN_BO1`**

```
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
HQ_HUB(config)#ip access-list extended VPN_BO2
HQ_HUB(config-ext-nacl)#permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```

Esto no prohibe a usuarios de acceso remoto la capacidad de comunicar con las redes detrás de los túneles especificados.**Advertencia:** Para que la comunicación ocurra, el otro lado del túnel debe tener el contrario de esta entrada ACL para esa red determinada.

4. **Túnel dividido de la configuración**Para habilitar el Túnel dividido para las conexiones VPN, aseegurese le configurar un ACL en el router. En este ejemplo, el comando del **split_tunnel de la lista de acceso** se asocia al grupo para los fines de tunelización dividida, y el túnel se forma a 10.10.10.0 /24 y 10.20.20.0/24 y 172.16.1.0/24 redes. Flujos de tráfico unencrypted a los dispositivos no en el túnel dividido ACL (por ejemplo, Internet).
```
HQ_HUB(config)#ip access-list extended split_tunnel
HQ_HUB(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255
HQ_HUB(config-ext-nacl)#exit
```
5. Configure la autenticación local, la autorización y la información de la configuración del cliente, tal como triunfos, dns. tráfico interesante acl y pool del IP, para los clientes VPN.
```
HQ_HUB(config)#aaa new-model
HQ_HUB(config)#aaa authentication login userauthen local
HQ_HUB(config)#aaa authorization network groupauthor local
HQ_HUB(config)#crypto isakmp client configuration group vpngroup
HQ_HUB(config-isakmp-group)#key cisco123
HQ_HUB(config-isakmp-group)#dns 10.10.10.10
HQ_HUB(config-isakmp-group)#wins 10.10.10.20
HQ_HUB(config-isakmp-group)#domain cisco.com
HQ_HUB(config-isakmp-group)#pool ippool
HQ_HUB(config-isakmp-group)#acl split_tunnel
HQ_HUB(config-isakmp-group)#exit
```
6. Configure el mapa dinámico y la información de mapa del cryto requeridos a la creación de túnel VPN.
```
HQ_HUB(config)#crypto isakmp profile vpnclient
HQ_HUB(config-isakmp-group)#match identity group vpngroup
HQ_HUB(config-isakmp-group)#client authentication list userauthen
HQ_HUB(config-isakmp-group)#isakmp authorization list groupauthor
HQ_HUB(config-isakmp-group)#client configuration address respond
HQ_HUB(config-isakmp-group)#exit
HQ_HUB(config)#crypto dynamic-map dynmap 10
HQ_HUB(config-crypto-map)#set transform-set newset
HQ_HUB(config-crypto-map)#set isakmp-profile vpnclient
HQ_HUB(config-crypto-map)#reverse-route
HQ_HUB(config-crypto-map)#exit
HQ_HUB(config)#crypto map map1 65535 ipsec-isakmp dynamic dynmap
HQ_HUB(config)#interface serial 2/0
HQ_HUB(config-if)#crypto map map1
```

Ejemplo de configuración

Ejemplo de configuración 2

```
HQ_HUB#show running-config
Building configuration...

Current configuration : 3524 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname HQ_HUB ! boot-start-marker boot-end-marker ! !
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network groupauthor local
!
aaa session-id common
!
resource policy
!
!
!
ip cef
!
!
!--- Output is suppressed ! username vpnuser password 0
vpnuser123 ! ! ! crypto isakmp policy 10 authentication
pre-share encryption 3des group 2 crypto isakmp key
cisco123 address 192.168.11.2 crypto isakmp key cisco123
address 192.168.12.2 ! crypto isakmp client
configuration group vpngroup
 key cisco123
 dns 10.10.10.10
 wins 10.10.10.20
 domain cisco.com
 pool ippool
 acl split_tunnel
crypto isakmp profile vpnclient
   match identity group vpngroup
   client authentication list userauthen
   isakmp authorization list groupauthor
   client configuration address respond
!
!
crypto ipsec transform-set newset esp-3des esp-md5-hmac
crypto ipsec transform-set remote-set esp-3des esp-md5-
hmac
!
crypto dynamic-map dynmap 10
 set transform-set remote-set
 set isakmp-profile vpnclient
 reverse-route
!
!
crypto map map1 5 ipsec-isakmp
 set peer 192.168.11.2
 set transform-set newset
 match address VPN_BO1
crypto map map1 10 ipsec-isakmp
 set peer 192.168.12.2
 set transform-set newset
 match address VPN_BO2
crypto map map1 65535 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
```

```
interface Serial2/0
 ip address 192.168.10.10 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 clock rate 64000
 crypto map map1
!
!
ip local pool ippool 10.10.120.10 10.10.120.50
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.1
!
ip nat inside source route-map nonat interface Serial2/0
overload
!
ip access-list extended NAT_Exempt
 deny ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
 deny ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip host 10.10.10.0 any
ip access-list extended VPN_BO1
 permit ip 10.10.10.0 0.0.0.255 172.16.1.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 172.16.1.0 0.0.0.255
ip access-list extended VPN_BO2
 permit ip 10.10.10.0 0.0.0.255 10.20.20.0 0.0.0.255
 permit ip 10.10.120.0 0.0.0.255 10.20.20.0 0.0.0.255
ip access-list extended split_tunnel
 permit ip 10.10.10.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 10.20.20.0 0.0.0.255 10.10.120.0 0.0.0.255
 permit ip 172.16.1.0 0.0.0.255 10.10.120.0 0.0.0.255



!
route-map nonat permit 10
 match ip address NAT_Exempt
!
!
control-plane
!
line con 0
line aux 0
line vty 0 4
!
!
end
HQ_HUB#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

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.

- **ping** — Este comando permite que usted inicie el túnel L2L VPN como se muestra.

Troubleshooting

Refiera a estos documentos para la información que usted puede utilizar para resolver problemas su configuración:

- Soluciones a los Problemas más frecuentes de IPSec VPN L2L y de Acceso Remoto
- Resolución de problemas de seguridad de IP – Información y uso de los comandos de depuración

Consejo: Cuando usted borra las asociaciones de seguridad, y no resuelve un problema del IPSec VPN, después quite y reaplique la correspondencia de criptografía relevante para resolver una amplia variedad de problemas.

Advertencia: Si usted quita una correspondencia de criptografía de una interfaz, derriba cualquier túnel IPsec asociado a esa correspondencia de criptografía. Siga estos pasos con cautela y considere la política del control de cambios de su organización antes proceder.

Ejemplo:

```
HQ_HUB(config)#interface s2/0
HQ_HUB(config-if)#no crypto map map1
*Sep 13 13:36:19.449: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
HQ_HUB(config-if)#crypto map map1
*Sep 13 13:36:25.557: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Información Relacionada

- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Página de Soporte de IPSec Negotiation/IKE Protocols
- Configurar un par dinámico y a los clientes VPN del LAN a LAN del router IPSec
- Soporte Técnico y Documentación - Cisco Systems