

Configuración de un túnel VPN de sitio a sitio entre routers de la serie RV y dispositivos de seguridad adaptable de la serie ASA 5500

Objetivo

La seguridad es esencial para proteger la propiedad intelectual de una empresa, a la vez que se garantiza la continuidad empresarial y se proporciona la capacidad de ampliar el espacio de trabajo corporativo a los empleados que necesitan acceso a los recursos de la empresa en cualquier momento y lugar.

Las soluciones de seguridad VPN son cada vez más importantes para las pequeñas y medianas empresas. Una VPN es una red privada construida dentro de una infraestructura de red pública, como Internet global. Una VPN extiende una red privada entre ubicaciones de oficina geográficamente separadas. Permite a un ordenador host enviar y recibir datos a través de redes públicas, ya que eran una parte integral de la red privada con toda la funcionalidad. Las VPN aumentan la seguridad de una organización distribuida, lo que facilita al personal trabajar desde diferentes sitios sin poner en peligro la red. Las motivaciones para utilizar VPN son los requisitos para "virtualizar" parte de las comunicaciones de una organización y la economía de las comunicaciones.

Hay diferentes topologías VPN: hub y spoke, punto a punto y malla completa. Este consejo inteligente incluye VPN de sitio a sitio (punto a punto), que proporciona una infraestructura basada en Internet para ampliar los recursos de red a oficinas remotas, oficinas domésticas y sitios de partners empresariales. Todo el tráfico entre los sitios se cifra mediante el protocolo de seguridad IP (IPsec) y se integran funciones de red como routing, calidad de servicio (QoS) y compatibilidad con multidifusión.

Los routers de la serie RV de Cisco ofrecen soluciones VPN sólidas y fáciles de gestionar a las pequeñas empresas preocupadas por los costes. Los Cisco ASA 5500 Series Adaptive Security Appliances ayudan a las organizaciones a equilibrar la seguridad y la productividad. Combina el firewall con inspección activa (stateful) más implementado del sector con servicios de seguridad de red de última generación integrales, que incluyen: visibilidad y control granular de aplicaciones y microaplicaciones, seguridad web, sistemas de prevención de intrusiones (IPS), acceso remoto altamente seguro y otros.

En esta breve guía se describe un ejemplo del diseño para crear una VPN IPsec de sitio a sitio entre routers de la serie RV y dispositivos de seguridad adaptable de la serie ASA 5500, y se proporcionan ejemplos de configuración.

Dispositivos aplicables

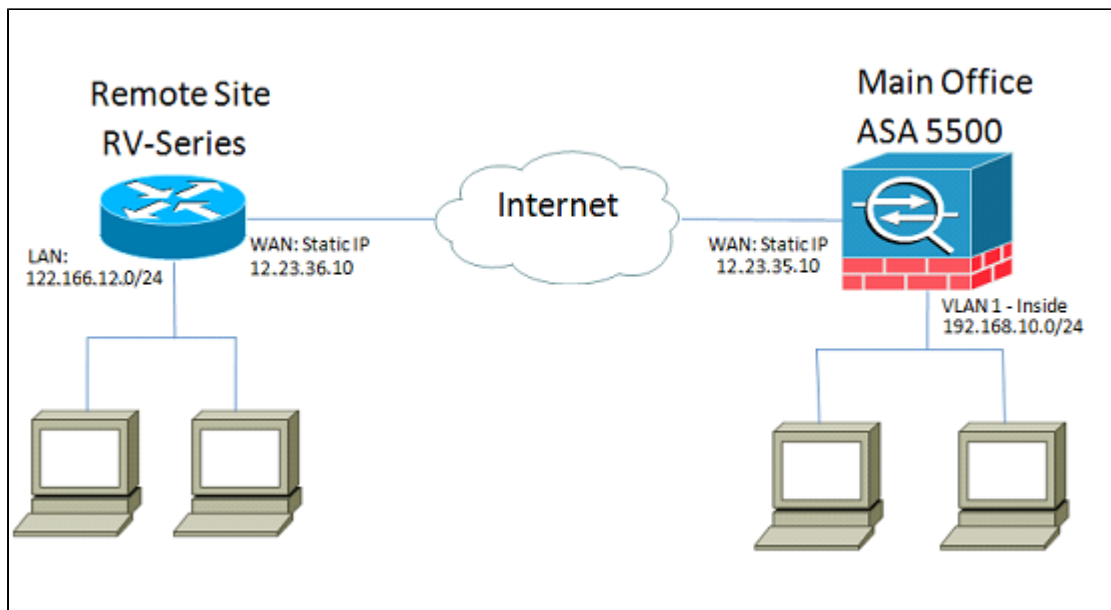
- Routers VPN de la serie RV0xx de Cisco
- Cisco ASA 5500 Series Adaptive Security Appliances

Versión del software

- 4.2.2.08 [Routers VPN de la serie Cisco RV0xx]

Preconfiguración

En la siguiente imagen se muestra un ejemplo de implementación de un túnel VPN de sitio a sitio mediante un router serie RV (sitio remoto) y un ASA 5500 (oficina principal).



Con esta configuración, un host en la red de sitio remoto de 122.166.12.x y un host en VLAN 1 en la oficina principal pueden comunicarse entre sí de forma segura.

Funciones esenciales

Intercambio de claves de Internet (IKE)

Intercambio de claves de Internet (IKE) es el protocolo utilizado para configurar una asociación de seguridad (SA) en el conjunto de protocolos IPsec. IKE se basa en el protocolo Oakley y en el protocolo ISAKMP (Internet Security Association and Key Management Protocol), y utiliza un intercambio de claves Diffie-Hellman para configurar un secreto de sesión compartido, del que se derivan las claves criptográficas. Se debe mantener manualmente una política de seguridad para cada par.

Seguridad de protocolo de Internet (IPSec)

IPSec utiliza servicios de seguridad criptográfica para proteger las comunicaciones a través de redes de protocolo de Internet (IP). IPSec admite la autenticación de peer en el nivel de red, la autenticación de origen de datos, la integridad de los datos, la confidencialidad de los datos (cifrado) y la protección de la reproducción. IPSec implica muchas tecnologías de componentes y métodos de cifrado. Sin embargo, el funcionamiento de IPSec se puede dividir en cinco pasos principales:

Paso 1. El "tráfico interesante" inicia el proceso IPSec: el tráfico se considera interesante cuando la política de seguridad IPSec configurada en los pares IPSec inicia el proceso IKE.

Paso 2. IKE fase 1: IKE autentica a los pares IPSec y negocia las SA IKE durante esta fase, configurando un canal seguro para negociar las SA IPSec en la fase 2.

Paso 3. IKE fase 2: IKE negocia los parámetros de SA IPSec y configura SA IPSec coincidentes en los pares.

Paso 4. Transferencia de datos: los datos se transfieren entre pares IPSec en función de los parámetros IPSec y las claves almacenadas en la base de datos SA.

Paso 5. Terminación del túnel IPsec: las SA IPsec terminan mediante eliminación o agotando el tiempo de espera.

ISAKMP

La Asociación de seguridad de Internet y el Protocolo de administración de claves (ISAKMP) se utilizan para negociar el túnel entre los dos terminales. Define los procedimientos de autenticación, comunicación y generación de claves, y es utilizado por el protocolo IKE para intercambiar claves de cifrado y establecer la conexión segura.

Consejos de diseño

Topología VPN: con una VPN de sitio a sitio, se configura un túnel IPsec seguro entre cada sitio y cada otro sitio. Una topología de varios sitios se suele implementar como una malla completa de túneles VPN de sitio a sitio (es decir, cada sitio ha establecido túneles para cada otro sitio). Si no se necesita comunicación entre las oficinas remotas, se utiliza una topología VPN de hub-spoke para reducir el número de túneles VPN (es decir, cada sitio establece un túnel VPN únicamente a la oficina principal).

Direccionamiento IP de WAN y DDNS: el túnel VPN debe establecerse entre dos direcciones IP públicas. Si los routers WAN reciben direcciones IP estáticas del proveedor de servicios de Internet (ISP), el túnel VPN se puede implementar directamente mediante direcciones IP públicas estáticas. Sin embargo, la mayoría de las pequeñas empresas utilizan servicios de Internet de banda ancha rentables, como módem por cable o DSL, y reciben direcciones IP dinámicas de sus ISP. En estos casos, se puede utilizar DDNS para asignar la dirección IP dinámica a un nombre de dominio completo (FQDN).

Direccionamiento IP de LAN: la dirección de red IP de LAN privada de cada sitio no debe tener solapamientos. La dirección de red IP de LAN predeterminada en cada sitio remoto siempre debe cambiarse.

Autenticación VPN: el protocolo IKE se utiliza para autenticar los pares VPN al establecer un túnel VPN. Existen varios métodos de autenticación IKE, y la clave previamente compartida es el método más conveniente. Cisco recomienda aplicar una clave previamente compartida segura.

Cifrado VPN: para garantizar la confidencialidad de los datos transportados a través de la VPN, se utilizan algoritmos de cifrado para cifrar la carga útil de paquetes IP. DES, 3DES y AES son tres estándares de encriptación comunes. AES se considera el más seguro en comparación con DES y 3DES. Cisco recomienda encarecidamente aplicar el cifrado AES-128 bits o superior (por ejemplo, AES-192 y AES-256). Sin embargo, cuanto más fuerte sea el algoritmo de cifrado, más recursos de procesamiento necesitará.

Consejos de Configuración

Lista de comprobación previa a la configuración

Paso 1. Asegúrese de que el ASA y el router RV están conectados al gateway de Internet (el router o módem ISP).

Paso 2. Encienda el router RV de Cisco y, a continuación, conecte los PC, servidores y otros dispositivos IP internos al conmutador LAN o a los puertos del conmutador del router RV.

Paso 3. Haga lo mismo con la red detrás del ASA. Paso 4. Asegúrese de que las direcciones de red IP LAN están configuradas en cada sitio y son subredes indiferentes. En este ejemplo, la LAN de la oficina principal utiliza 192.168.10.0/24, and la LAN del sitio remoto utiliza 122.166.12.0/24.

Paso 4. Asegúrese de que los PC y servidores locales pueden comunicarse entre sí y con el router.

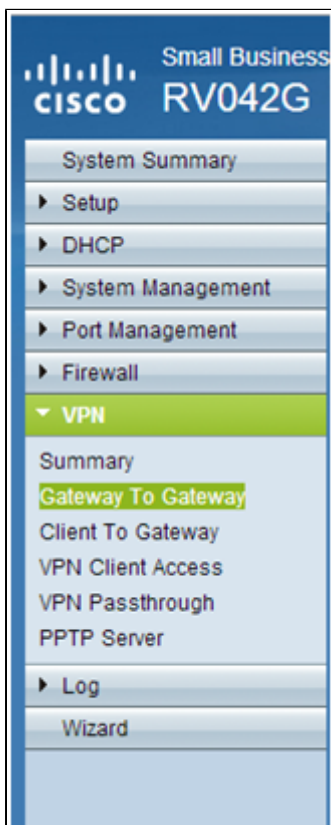
Identificación de la conexión WAN

Deberá saber si el ISP le proporciona una dirección IP dinámica o si ha recibido una dirección IP

estática. Por lo general, el ISP le proporcionará una IP dinámica, pero deberá confirmarlo para completar la configuración.

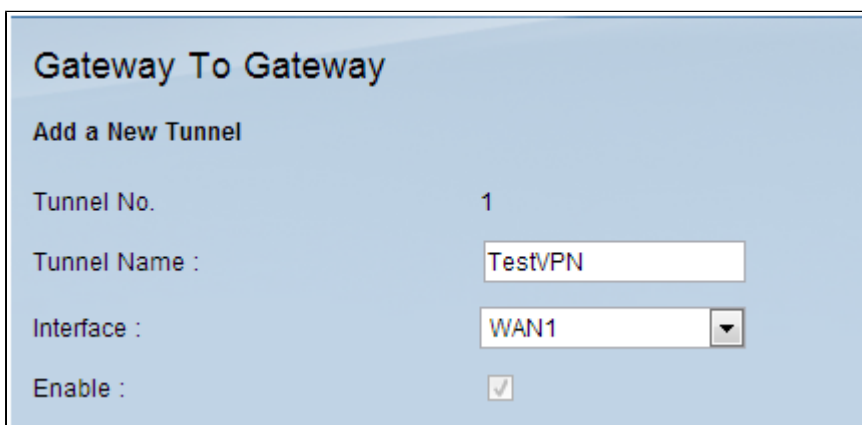
Configuración del RV042G en la oficina remota

Paso 1. Inicie sesión en la interfaz de usuario web y vaya a la sección **VPN > Gateway to Gateway**. Dado que estamos agregando una conexión de LAN a LAN, los terminales serán el gateway de cada red.



Paso 2. Configure los terminales locales y remotos en el router

a) Configure el nombre del túnel para identificarlo de cualquier otro túnel que ya haya configurado.

The image shows the 'Gateway To Gateway' configuration page. The title is 'Gateway To Gateway'. Below the title is the section 'Add a New Tunnel'. The configuration fields are: Tunnel No. (1), Tunnel Name (TestVPN), Interface (WAN1), and Enable (checked).

b) La configuración de grupo local configura los hosts locales que se permitirán en el túnel VPN. Asegúrese de que dispone de la subred y la máscara correctas para la red a la que desea que se le permita atravesar el túnel.

Local Group Setup	
Local Security Gateway Type :	IP Only
IP Address :	12.23.36.10
Local Security Group Type :	Subnet
IP Address :	122.166.12.0
Subnet Mask :	255.255.255.0

C) Remote Group Setup (Configuración de grupo remoto) configura el terminal remoto y el tráfico de red que debe buscar el router. Introduzca la IP estática del gateway remoto para establecer la conexión en el campo de dirección IP del gateway. A continuación, introduzca la subred permitida en la VPN desde el sitio remoto (la LAN de la oficina principal).

Remote Group Setup	
Remote Security Gateway Type :	IP Only
IP Address :	12.23.35.10
Remote Security Group Type :	Subnet
IP Address :	192.168.10.0
Subnet Mask :	255.255.255.0

Paso 3. Configure los parámetros del túnel.

a) Deberá configurar una clave previamente compartida para obtener resultados óptimos.

Las fases 1 y 2 son diferentes fases de autenticación, la fase 1 crea el túnel inicial y comienza la negociación, y la fase 2 finaliza la negociación de la clave de cifrado y protege la transmisión de datos una vez que se establece el túnel.

b) El grupo DH corresponderá al grupo de políticas crypto isakmp en el ASA, que verá en la siguiente sección. En ASA, el valor predeterminado es el Grupo 2, y las versiones más recientes del código ASA requieren al menos el Grupo 2 de DH. La contrapartida es que es un bit más alto y, por lo tanto, requiere más tiempo de CPU.

c) El cifrado de fase 1 define el algoritmo de cifrado utilizado. El valor predeterminado de la serie RV es DES, pero el valor predeterminado de ASA será 3DES. Sin embargo, se trata de estándares más antiguos y no son eficaces en la implementación actual. El cifrado AES es más rápido y seguro, y Cisco recomienda al menos AES-128 (o simplemente AES) para obtener los mejores resultados.

d) La autenticación de fase 1 verifica la integridad del paquete. Las opciones son SHA-1 y MD5, y cualquiera de ellas debería funcionar ya que producen resultados similares.

La configuración de la fase 2 sigue las mismas reglas que la fase 1. Al configurar los parámetros de IPsec, tenga en cuenta que los parámetros del ASA tendrán que COINCIDIR con los del RV042G. Si hay alguna discrepancia, los dispositivos no podrán negociar la clave de cifrado y la conexión fallará.

Nota: Asegúrese de guardar los parámetros antes de salir de esta página.

IPSec Setup	
Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 2 - 1024 bit
Phase 1 Encryption :	AES-128
Phase 1 Authentication :	SHA1
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	<input type="checkbox"/>
Phase 2 DH Group :	Group 2 - 1024 bit
Phase 2 Encryption :	AES-128
Phase 2 Authentication :	SHA1
Phase 2 SA Life Time :	28800 seconds
Preshared Key :	c12c0VPn3x4mPL3

Configuración de ASA 5500 en la oficina principal (CLI)

Nota: Asegúrese de utilizar el comando "write mem" con frecuencia para evitar la pérdida de configuraciones. En primer lugar, estas son las interfaces que hemos configurado en el ASA. El suyo puede ser diferente, por lo que debe asegurarse de modificar las configuraciones en consecuencia.

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
```

Paso 1. Configuración de la administración de cifrado (ISAKMP)

El primer paso será configurar la política ISAKMP, que es lo que se utiliza para negociar el cifrado del túnel. Esta configuración debe ser IDÉNTICA en ambos extremos. Aquí es donde configurará los parámetros de cifrado para que coincidan con la fase 1 de la configuración de RV.

```
ASA5505(config)# crypto isakmp policy 1
ASA5505(config-isakmp-policy)# authentication pre-share
ASA5505(config-isakmp-policy)# encryption aes
ASA5505(config-isakmp-policy)# hash sha
ASA5505(config-isakmp-policy)# group 2
ASA5505(config-isakmp-policy)# lifetime 28800
ASA5505(config-isakmp-policy)# exit
ASA5505(config)# █
```

Paso 2. Selección de tráfico

Es lo mismo que el grupo de seguridad local y remoto del RV042G. En el ASA, utilizamos listas de acceso para definir lo que la red considera "tráfico interesante" para permitir en la VPN. En primer lugar, configure los objetos de red para el sitio remoto y el sitio local:

```
object network insidenet
  subnet 192.168.10.0 255.255.255.0
object network rsite
  subnet 122.166.12.0 255.255.255.0
```

A continuación, configure la lista de acceso para utilizar estos objetos:

```
access-list vpn extended permit ip object insidenet object rsite
```

Alternativamente, puede utilizar las subredes mismas, pero en implementaciones más grandes es más fácil utilizar objetos y grupos de objetos.

Paso 3. Configuración del túnel IPsec (autenticación de fase 2)

Aquí configuraremos el "conjunto de transformación" y el grupo de túnel, que configurará la autenticación de fase 2. Si configura la Fase 2 para que sea diferente de la Fase 1, tendrá un conjunto de transformación diferente. Aquí esp-aes define el encriptación y esp-sha-hmac define el hash. El comando tunnel-group configura la información de túnel específica de la conexión, como la clave previamente compartida. Utilice la IP pública del par remoto como el nombre del grupo de túnel.

```
ASA5505(config)# crypto ipsec transform-set asarv esp-aes esp-sha-hmac
ASA5505(config)# tunnel-group 12.23.36.10 type ipsec-l2l
ASA5505(config)# tunnel-group 12.23.36.10 ipsec-attributes
ASA5505(config-tunnel-ipsec)# pre-shared-key c12c0VPn3x4mPL3
ASA5505(config-tunnel-ipsec)# exit
ASA5505(config)#
```

Paso 4. Configuración de mapa criptográfico

Ahora tenemos que aplicar la configuración de la fase 1 y la fase 2 a un "mapa criptográfico" que permitirá al ASA establecer la VPN y enviar el tráfico correcto. Piense en esto como la unión de las piezas de la VPN.

```
ASA5505(config)# crypto map asarv 1 match address vpn
ASA5505(config)# crypto map asarv 1 set peer 12.23.36.10
ASA5505(config)# crypto map asarv 1 set transform-set asarv
ASA5505(config)# crypto map asarv interface outside
ASA5505(config)#
```

Paso 5. Verificar el estado de VPN

Por último, compruebe los terminales para verificar que la conexión VPN esté activa y en funcionamiento. La conexión no se activará por sí sola; deberá pasar el tráfico para que ASA pueda detectarla e intentar establecer la conexión. En el ASA, utilice el comando "show crypto isakmpsa" para mostrar el estado.

```

ASA5505(config)# show crypto isakmp sa

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: 12.23.36.10
  Type    : L2L                Role    : responder
  Rekey   : no                 State   : MM_ACTIVE
ASA5505(config)#

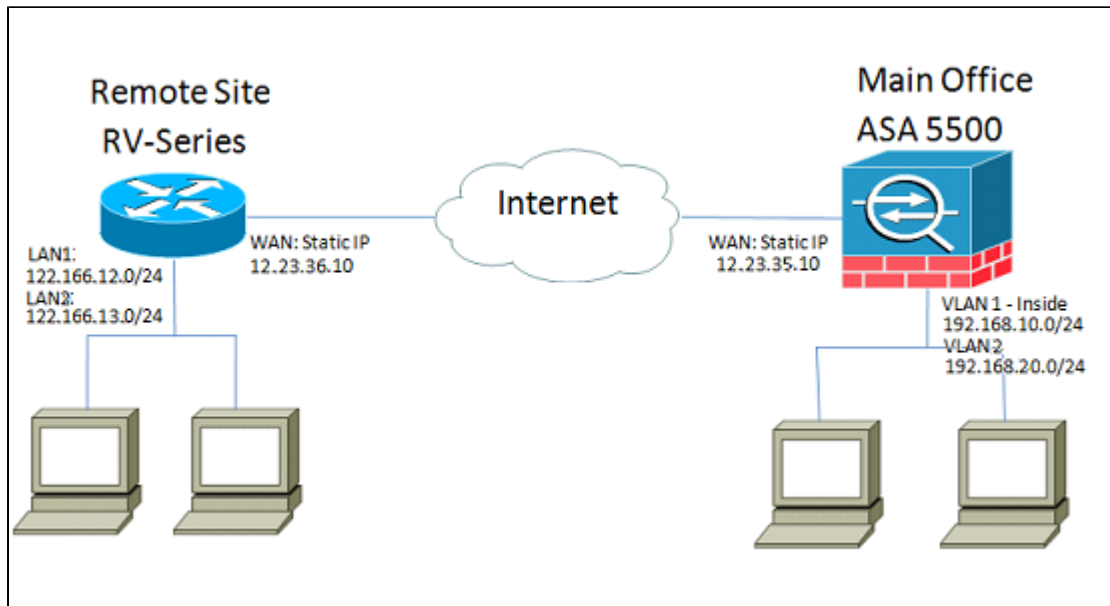
```

En el RV42G, vaya a la página **VPN > Summary (VPN > Resumen)** y compruebe el estado.

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	TestVPN	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	

Situación alternativa: varias subredes en la red

No entre en pánico. Puede parecer un proceso abrumadoramente complicado al configurar la red, pero ya ha realizado la parte difícil anterior. La configuración de la VPN para varias subredes requiere alguna configuración adicional, pero muy poca complejidad adicional (a menos que el esquema de subred sea extenso). En el ejemplo que hemos utilizado para esta sección se utilizan 2 subredes en cada sitio. La topología de red actualizada es muy similar:



Configuración del RV042G

Al igual que antes, configuraremos el RV042G en primer lugar. El RV042G no puede configurar varias subredes en un solo túnel, por lo que será necesario agregar una entrada adicional para la nueva subred. Esta sección sólo tratará la configuración de VPN para varias subredes, no ninguna configuración de configuración adicional para ellas.

Paso 1. Configuración del primer túnel

Utilizaremos la misma configuración para cada túnel que para el ejemplo de subred única. Como

antes, configure esto yendo a **VPN > Gateway to Gateway** y agregando un túnel nuevo, o si está usando un túnel existente vaya a la página **VPN > Summary** y edite el existente.

a) Configure el nombre del túnel, pero cámbielo ya que tendremos más de un cambio en el nombre para que sea más descriptivo.

Gateway To Gateway

Add a New Tunnel

Tunnel No. 1

Tunnel Name : VPNSubnet1

Interface : WAN1

Enable :

b) A continuación configuraremos el grupo local, igual que antes. Configure esto sólo para UNA de las subredes que necesitan acceso. Tendremos una entrada de túnel para 122.166.12.x y otra para la subred 122.166.13.x.

Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 12.23.36.10

Local Security Group Type : Subnet

IP Address : 122.166.12.0

Subnet Mask : 255.255.255.0

c) Ahora configure el sitio remoto, siguiendo el mismo procedimiento descrito anteriormente.

Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 12.23.35.10

Remote Security Group Type : Subnet

IP Address : 192.168.10.0

Subnet Mask : 255.255.255.0

d) Por último, configure los parámetros de encriptación. Recuerde estos parámetros, ya que deseará que sean iguales en ambos túneles que estamos configurando.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : AES-128

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 bit

Phase 2 Encryption : AES-128

Phase 2 Authentication : SHA1

Phase 2 SA Life Time : 28800 seconds

Preshared Key : c12c0VPn3x4mPL3

Paso 2. Configuración del segundo túnel

Ahora que la Subred 1 está configurada para el túnel VPN, debemos ir a **VPN > Gateway to Gateway** y agregar un segundo túnel. Esta segunda entrada se configurará de forma similar a la primera, pero con las subredes secundarias de cada sitio.

a) Asegúrese de darle un nombre distintivo para saber qué conexión es.

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name : VPNsubnet2

Interface : WAN1

Enable :

b) Utilice la segunda subred como el grupo "Seguridad local".

Local Group Setup

Local Security Gateway Type : IP Only

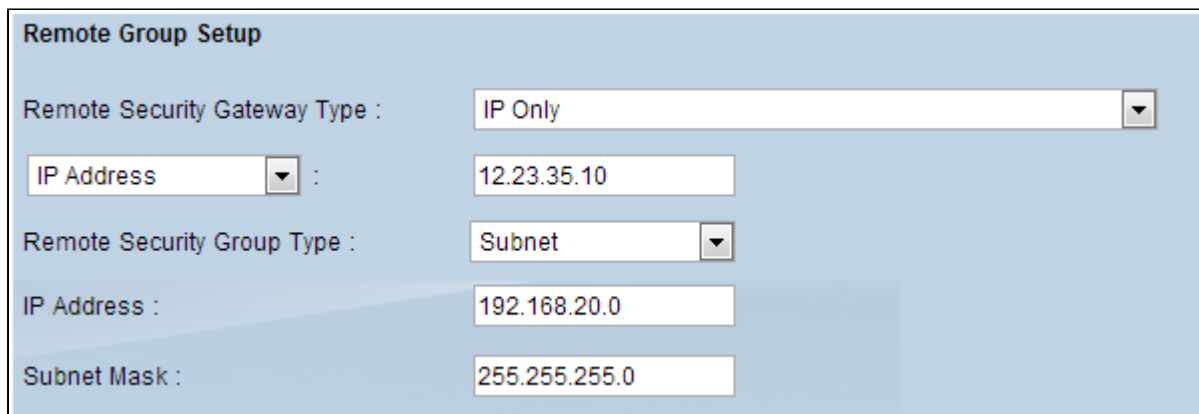
IP Address : 12.23.36.10

Local Security Group Type : Subnet

IP Address : 122.166.13.0

Subnet Mask : 255.255.255.0

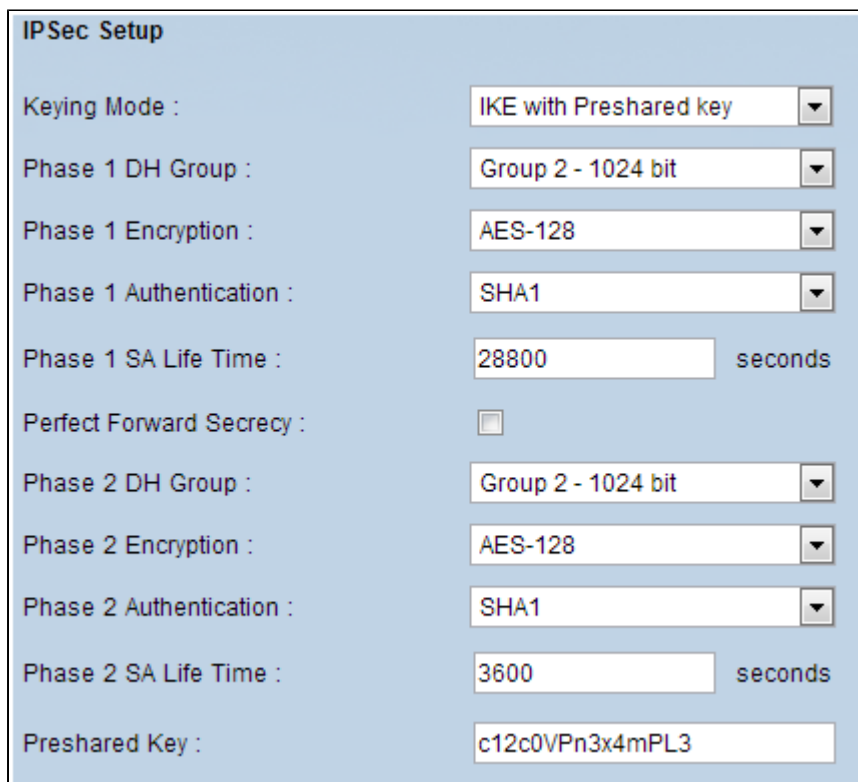
C) Y utilice la segunda subred remota como el grupo "Seguridad remota".



The screenshot shows the 'Remote Group Setup' configuration page. It includes the following fields and values:

- Remote Security Gateway Type : IP Only
- IP Address : 12.23.35.10
- Remote Security Group Type : Subnet
- IP Address : 192.168.20.0
- Subnet Mask : 255.255.255.0

d) Configure el cifrado para las fases 1 y 2 de la misma manera que para el primer túnel.



The screenshot shows the 'IPSec Setup' configuration page. It includes the following fields and values:

- Keying Mode : IKE with Preshared key
- Phase 1 DH Group : Group 2 - 1024 bit
- Phase 1 Encryption : AES-128
- Phase 1 Authentication : SHA1
- Phase 1 SA Life Time : 28800 seconds
- Perfect Forward Secrecy :
- Phase 2 DH Group : Group 2 - 1024 bit
- Phase 2 Encryption : AES-128
- Phase 2 Authentication : SHA1
- Phase 2 SA Life Time : 3600 seconds
- Preshared Key : c12c0VPn3x4mPL3

Configuración de ASA

Ahora modificaremos la configuración en el ASA. Esta configuración es increíblemente simple. Puede utilizar la misma configuración que la anterior, ya que utiliza todos los mismos parámetros de cifrado, con solo un pequeño cambio. Necesitamos etiquetar el tráfico adicional como "interesante" para que el firewall lo envíe a través de la VPN. Dado que utilizamos una lista de acceso para identificar el tráfico interesante, todo lo que tenemos que hacer es modificar esta lista de acceso.

Paso 1. Para empezar, elimine la lista de acceso anterior, de modo que podamos modificar los objetos en el ASA. Utilice la forma "no" del comando para eliminar configuraciones en la CLI.

Paso 2. Una vez que se elimina la ACL, queremos crear nuevos objetos para las nuevas subredes involucradas (suponiendo que aún no lo haya hecho al configurar esas subredes). También queremos que sean más descriptivos.

Según la configuración de VLAN que aparece a continuación:

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan2
 nameif engineering
 security-level 100
 ip address 192.168.20.1 255.255.255.0
!
interface Vlan10
 nameif outside
 security-level 0
 ip address 12.23.35.10 255.255.255.0
!
```

Necesitamos un grupo de objetos para la red interna principal (192.168.10.x) y la red de ingeniería (192.168.20.x). Configure los objetos de red de esta manera:

```
ASA5505(config)# show run object
object network ASAvlan1
 subnet 192.168.10.0 255.255.255.0
object network ASAvlan2
 subnet 192.168.20.0 255.255.255.0
object network RVvlan1
 subnet 122.166.12.0 255.255.255.0
object network RVvlan2
 subnet 122.166.13.0 255.255.255.0
```

Paso 3. Ahora que se han configurado los objetos de red relevantes, podemos configurar la lista de acceso para etiquetar el tráfico apropiado. Debe asegurarse de que tiene una entrada de lista de acceso para ambas redes detrás del ASA a ambas subredes remotas. El resultado final debería verse así.

```
ASA5505(config)# show run access-list
access-list vpn extended permit ip object ASAvlan1 object RVvlan1
access-list vpn extended permit ip object ASAvlan1 object RVvlan2
access-list vpn extended permit ip object ASAvlan2 object RVvlan1
access-list vpn extended permit ip object ASAvlan2 object RVvlan2
```

Paso 4. Ahora, debido a que eliminamos la lista de acceso antigua, necesitamos volver a aplicarla al mapa criptográfico usando el mismo comando que antes:

```
ASA5505(config)# crypto map asarv 1 match address vpn
```

Verifique la conexión





¡Y eso es todo! El túnel debe estar operativo ahora. Inicie la conexión y verifique el estado mediante el comando "show crypto isakmpsa" en el ASA.

```
ASA5505(config)# show crypto isakmp sa

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: 12.23.36.10
  Type    : L2L                Role    : responder
  Rekey   : no                 State   : MM_ACTIVE
ASA5505(config)#
```

En la serie RV, el estado se mostrará en la página VPN > Summary (VPN > Resumen).

No.	Name	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Tunnel Test	Config.
1	VPNSubnet1	Connected	AES/SHA1	122.166.12.0 255.255.255.0	192.168.10.0 255.255.255.0	12.23.35.10	Disconnect	 
2	VPNsubnet2	Connected	AES/SHA1	122.166.13.0 255.255.255.0	192.168.20.0 255.255.255.0	12.23.35.10	Disconnect	 

Add Page 1 of 1

Ver un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras charlas sobre tecnología de Cisco](#)

Acerca de esta traducción

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

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

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