Configuración del concentrador Cisco VPN 5000 e implementación de la conectividad VPN de LAN a LAN de modo principal IPsec

Contenido

Introducción

Este documento explica la configuración inicial del Cisco VPN 5000 Concentrator y muestra cómo conectarse a la red mediante IP y cómo ofrecer conectividad VPN de LAN a LAN de modo principal IPSec.

Puede instalar el concentrador VPN en cualquiera de las dos configuraciones, dependiendo de dónde lo conecte a la red en relación con un firewall. El concentrador VPN tiene dos puertos Ethernet, uno de los cuales (Ethernet 1) sólo pasa tráfico IPSec. El otro puerto (Ethernet 0) enruta todo el tráfico IP. Si planea instalar el concentrador VPN en paralelo con el firewall, debe utilizar ambos puertos para que Ethernet 0 se enfrente a la LAN protegida y Ethernet 1 se enfrente a Internet a través del router de gateway de Internet de la red. También puede instalar el concentrador VPN detrás del firewall en la LAN protegida y conectarlo a través del puerto Ethernet 0, de modo que el tráfico IPSec que pasa entre Internet y el concentrador pase a través del firewall.

Prerequisites

Requirements

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el Cisco VPN 5000 Concentrator.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configuración de conectividad básica

La forma más sencilla de establecer la conectividad de red básica es conectar un cable serial al puerto de consola en el concentrador VPN y utilizar el software de terminal para configurar la dirección IP en el puerto Ethernet 0. Después de configurar la dirección IP en el puerto Ethernet 0, puede utilizar Telnet para conectarse al concentrador VPN para completar la configuración. También puede generar un archivo de configuración en un editor de texto adecuado y enviarlo al concentrador VPN mediante TFTP.

Al utilizar el software de terminal a través del puerto de la consola, inicialmente se le solicita una contraseña. Utilice la contraseña "letmein". Después de responder con la contraseña, ejecute el comando **configure ip ethernet 0**, respondiendo a las indicaciones con la información del sistema. La secuencia de avisos debe ser similar a la del siguiente ejemplo.

```
*[ IP Ethernet 0 ]# configure ip ethernet 0
      Section 'ip ethernet 0' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 0 ]# ipaddress=192.168.233.1
      *[ IP Ethernet 0 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 0 ]# ipbroadcast=192.168.233.255
      *[ IP Ethernet 0 ]# mode=routed
      *[ IP Ethernet 0 ]#
```

Ahora está listo para configurar el puerto Ethernet 1.

Configuración del puerto Ethernet 1

La información de direccionamiento TCP/IP en el puerto Ethernet 1 es la dirección TCP/IP enrutable a Internet externa que asignó al concentrador VPN. Evite utilizar una dirección en la misma red TCP/IP que Ethernet 0, ya que esto desactivará TCP/IP en el concentrador.

Ingrese los comandos **configure ip ethernet 1**, respondiendo a las indicaciones con la información del sistema. La secuencia de avisos debe ser similar a la del siguiente ejemplo.

```
*[ IP Ethernet 0 ]# configure ip ethernet 1
      Section 'ip ethernet 1' not found in the config.
```

```
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP Ethernet 1 ]# ipaddress=206.45.55.1
      *[ IP Ethernet 1 ]# subnetmask=255.255.255.0
      *[ IP Ethernet 1 ]# ipbroadcast=206.45.55.255
      *[ IP Ethernet 1 ]# mode=routed
      *[ IP Ethernet 1 ]#
```

Ahora necesita configurar el gateway IPSec.

Configuración de la puerta de enlace IPSec

El gateway IPSec controla dónde el concentrador VPN envía todo el tráfico IPSec o tunelizado. Esto es independiente de la ruta predeterminada que configure más adelante. Comience ingresando el comando **configure general**, respondiendo a las indicaciones con la información del sistema. La secuencia de avisos debe ser similar al ejemplo que se muestra a continuación.

```
* IntraPort2+_A56CB700# configure general
      Section 'general' not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ General ]# ipsecgateway=206.45.55.2
      *[ General ]# exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Nota: En las versiones 6.x y posteriores, el comando **ipsecgateway** se ha cambiado al comando **vpngateway**.

Ahora configuremos la política de intercambio de claves de Internet (IKE).

Configuración de la política IKE

Los parámetros del protocolo de administración de claves de asociación de seguridad de Internet (ISAKMP)/IKE controlan cómo el concentrador VPN y el cliente se identifican y autentican entre sí para establecer sesiones de túnel. Esta negociación inicial se denomina Fase 1. Los parámetros de la Fase 1 son globales para el dispositivo y no están asociados a una interfaz en particular. A continuación se describen las palabras clave reconocidas en esta sección. Los parámetros de negociación de la fase 1 para los túneles de LAN a LAN se pueden establecer en la sección [Tunnel Partner <Section ID>]. La negociación IKE de fase 2 controla cómo el VPN Concentrator y el VPN Client manejan las sesiones de túnel individuales. Los parámetros de negociación IKE de fase 2 para el VPN Concentrator y el VPN Client se establecen en el dispositivo [VPN Group <Name>].

La sintaxis de la política IKE es la siguiente.

```
Protection = [ MD5_DES_G1 | MD5_DES_G2 | SHA_DES_G1 | SHA_DES_G2 ]
```

La palabra clave protection especifica un conjunto de protección para la negociación ISAKMP/IKE entre el VPN Concentrator y el VPN Client. Esta palabra clave puede aparecer varias veces dentro de esta sección, en cuyo caso el concentrador VPN propone todos los conjuntos de protección especificados. El cliente VPN acepta una de las opciones para la negociación. La

primera parte de cada opción, MD5 (Message Digest 5), es el algoritmo de autenticación utilizado para la negociación. SHA significa algoritmo hash seguro, que se considera más seguro que MD5. La segunda parte de cada opción es el algoritmo de cifrado. DES (estándar de cifrado de datos) utiliza una clave de 56 bits para codificar los datos. La tercera parte de cada opción es el grupo Diffie-Hellman, utilizado para el intercambio de claves. Dado que el algoritmo del grupo 2 (G2) utiliza números más grandes, es más seguro que el grupo 1 (G1).

Para iniciar la configuración, ingrese el comando **configure IKE policy**, respondiendo a las indicaciones con la información del sistema. Se presenta un ejemplo a continuación:

```
* IntraPort2+_A56CB700# configure IKE Policy
      Section 'IKE Policy' was not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IKE Policy ] Protection = MD5_DES_G1
      *[ IKE Policy ] exit
      Leaving section editor.
      * IntraPort2+_A56CB700#
```

Ahora que ha configurado los conceptos básicos, ha llegado el momento de definir los parámetros de túnel y comunicación IP.

Configuración de sitio a sitio de modo principal

Para configurar el concentrador VPN para que admita conexiones de LAN a LAN, debe definir la configuración del túnel, así como los parámetros de comunicación IP que se utilizarán en el túnel. Hará esto en dos secciones, la sección [Tunnel Partner VPN x] y la sección [IP VPN x]. Para cualquier configuración de sitio a sitio dada, la *x* definida en estas dos secciones debe coincidir, de modo que la configuración del túnel se asocie correctamente con la configuración del protocolo.

Veamos cada una de estas secciones en detalle.

Configuración de la sección de socio de túnel

En la sección partner de túnel, debe definir al menos los ocho parámetros siguientes.

- Transformación
- Partner
- KeyManage
- SharedKey
- Modo
- LocalAccess
- Entidad par
- Enlazar

Transformación

La palabra clave Transform especifica los tipos de protección y algoritmos utilizados para las sesiones de cliente IKE. Cada opción asociada a este parámetro es una pieza de protección que

especifica los parámetros de autenticación y cifrado. El parámetro Transform puede aparecer varias veces dentro de esta sección, en cuyo caso el VPN Concentrator propone las piezas de protección especificadas en el orden en que se analizan, hasta que el cliente acepte una para usarla durante la sesión. En la mayoría de los casos, sólo se necesita una palabra clave Transform.

Las opciones para la palabra clave Transform son las siguientes.

```
[ ESP(SHA,DES) | ESP(SHA,3DES) | ESP(MD5,DES) | ESP(MD5,3DES) | ESP(MD5) |
ESP(SHA) | AH(MD5) | AH(SHA) |AH(MD5)+ESP(DES) | AH(MD5)+ESP(3DES) |
AH(SHA)+ESP(DES) | AH(SHA)+ESP(3DES) ]
```

ESP significa Encapsulating Security Payload y AH significa Authentication Header. Ambos encabezados se utilizan para cifrar y autenticar paquetes. DES (estándar de cifrado de datos) utiliza una clave de 56 bits para codificar los datos. 3DES utiliza tres claves diferentes y tres aplicaciones del algoritmo DES para codificar los datos. MD5 es el algoritmo hash del resumen de mensajes 5. SHA es el algoritmo hash seguro, que se considera un poco más seguro que MD5.

ESP(MD5,DES) es el valor predeterminado y se recomienda para la mayoría de las configuraciones. ESP(MD5) y ESP(SHA) utilizan ESP para autenticar paquetes (sin cifrado). AH(MD5) y AH(SHA) utilizan AH para autenticar paquetes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) y AH(SHA)+ESP(3DES) utilizan AH para autenticar paquetes y ESP para cifrar paquetes.

Partner

La palabra clave Partner define la dirección IP del otro terminador de túnel en la asociación de túnel. Este número debe ser una dirección IP pública enrutable con la que el concentrador VPN local pueda crear una conexión IPSec.

KeyManage

La palabra clave KeyManage define cómo los dos Concentradores VPN en una asociación de túnel determinan qué dispositivo inicia el túnel y qué tipo de procedimiento de establecimiento de túnel seguir. Las opciones son Auto (Automático), Initiate (Iniciar), Respond (Responder) y Manual (Manual). Puede utilizar las primeras tres opciones para configurar túneles IKE y la palabra clave Manual para configurar túneles de cifrado fijo. Este documento no trata sobre cómo configurar túneles de cifrado fijo. Auto especifica que el partner de túnel puede iniciar y responder a las solicitudes de configuración del túnel. Initiate especifica que el partner de túnel sólo envía solicitudes de configuración de túnel, no les responde. Respond especifica que el partner de túnel responde a las solicitudes de configuración de túnel, pero nunca las inicia.

SharedKey

La palabra clave SharedKey se utiliza como secreto compartido IKE. Debe establecer el mismo valor de SharedKey en ambos partners de túnel.

Modo

La palabra clave Mode define el protocolo de negociación IKE. El valor predeterminado es Agresivo, por lo que para configurar el concentrador VPN para el modo de interoperabilidad, debe

establecer la palabra clave Mode en Main.

LocalAccess

LocalAccess define los números IP a los que se puede acceder a través del túnel, desde una máscara de host a una ruta predeterminada. La palabra clave LocalProto define a qué números de protocolo IP se puede acceder a través del túnel, como ICMP(1), TCP(6), UDP(17), etc. Si desea pasar todos los números IP, debe establecer LocalProto=0. LocalPort determina a qué números de puerto se puede alcanzar a través del túnel. Tanto LocalProto como LocalPort tienen el valor predeterminado de 0 o de acceso completo.

Entidad par

La palabra clave Peer especifica qué subredes se encuentran a través de un túnel. PeerProto especifica qué protocolos se permiten a través del extremo del túnel remoto y PeerPort establece a qué números de puerto se puede acceder en el otro extremo del túnel.

Enlazar

BindTo especifica qué puerto Ethernet termina las conexiones de sitio a sitio. Siempre debe establecer este parámetro en Ethernet 1, excepto cuando el concentrador VPN se está ejecutando en modo de puerto único.

Configuración de los Parámetros

Para configurar estos parámetros, ingrese el comando **configure Tunnel Partner VPN 1**, respondiendo a las indicaciones con la información de su sistema.

La secuencia de avisos debe ser similar a la del ejemplo siguiente.

```
*IntraPort2+_A56CB700# configure Tunnel Partner VPN 1
      Section ?config Tunnel Partner VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
       =
      To find a list of valid keywords and additional help enter "?"
      *[ Tunnel Partner VPN 1 ]# transform=ESP(MD5,DES)
      *[ Tunnel Partner VPN 1 ]# sharedkey=letmein
      *[ Tunnel Partner VPN 1 ]# partner=208.203.136.10
      *[ Tunnel Partner VPN 1 ]# mode=main
      *[ Tunnel Partner VPN 1 ]# peer=10.0.0.0/8
      *[ Tunnel Partner VPN 1 ]# localaccess=192.168.233.0/24
      *[ Tunnel Partner VPN 1 ]# bindto=Ethernet 1
      *[ Tunnel Partner VPN 1 ]# exit
      Leaving section editor.
```

Ahora es el momento de configurar la sección IP.

Configuración de Sección IP

Puede utilizar conexiones numeradas o sin numerar (como en la configuración IP en conexiones WAN) en la sección de configuración IP de cada asociación de túnel. Aquí usamos sin numerar.

La configuración mínima para una conexión sitio a sitio sin numerar requiere dos instrucciones: numbered=false y mode=routed. Comience ingresando los comandos **configure ip vpn 1** y responda a las indicaciones del sistema como se indica a continuación.

```
*[ IP Ethernet 0 ]# configure ip vpn 1
      Section ?IP VPN 1? not found in the config.
      Do you want to add it to the config? y
      Configure parameters in this section by entering:
      <Keyword> = <Value>
      To find a list of valid keywords and additional help enter "?"
      *[ IP VPN 1 ]# mode=routed
      *[ IP VPN 1 ]# numbered=false
```

Ahora es el momento de configurar una ruta predeterminada.

Configuración de la ruta predeterminada (tabla de rutas TCP/IP)

Debe configurar una ruta predeterminada que el concentrador VPN puede utilizar para enviar todo el tráfico TCP/IP destinado a redes distintas de las redes a las que está conectado directamente o para las que tiene rutas dinámicas. La ruta predeterminada señala a todas las redes encontradas en el puerto interno. Ya ha configurado Intraport para enviar tráfico IPSec desde y hacia Internet usando el parámetro IPSec Gateway. Para iniciar la configuración de ruta predeterminada, ingrese el comando edit config ip static, respondiendo a las indicaciones con la información del sistema. La secuencia de avisos debe ser similar a la del ejemplo siguiente.

```
*IntraPort2+_A56CB700# edit config ip static
      Section 'ip static' not found in the config.
      Do you want to add it to the config? y
      Configuration lines in this section have the following format:
      <Destination> <Mask> <Gateway> <Metric> [<Redist=(RIP|none)>]
      Editing "[ IP Static ]"...
      1: [ IP Static ]
      End of buffer
      Edit [ IP Static ]> append 1
      Enter lines at the prompt. To terminate input, enter
      a . on a line all by itself.
      Append> 0.0.0.0 0.0.0.0 192.168.233.2 1
      Append> .
      Edit [ IP Static ]> exit
      Saving section...
      Checking syntax...
      Section checked successfully.
      *IntraPort2+_A56CB700#
```

Terminar

El último paso es guardar la configuración. Cuando se le pregunte si está seguro de que desea descargar la configuración y reiniciar el dispositivo, escriba **y** y presione **Intro**. No apague el concentrador VPN durante el proceso de arranque. Después de que el concentrador se haya reiniciado, los usuarios pueden conectarse mediante el software VPN Client del concentrador.

Para guardar la configuración, ingrese el comando **save**, como se indica a continuación.

```
*IntraPort2+_A56CB700# save
```

```
      Save configuration to flash and restart device? y
```

Si está conectado al concentrador VPN mediante Telnet, el resultado anterior es todo lo que verá. Si está conectado a través de una consola, verá un resultado similar al siguiente, sólo mucho más. Al final de este resultado, el concentrador VPN devuelve "Hello Console..." y solicita una contraseña. Así es como sabes que has terminado.

```
Codesize => 0 pfree => 462
      Updating Config variables...
      Adding section '[ General ]' to config
      Adding -- ConfiguredFrom = Command Line, from Console
      Adding -- ConfiguredOn = Timeserver not configured
      Adding -- DeviceType = IntraPort2
      Adding -- SoftwareVersion = IntraPort2 V4.5
      Adding -- EthernetAddress = 00:00:a5:6c:b7:00
      Not starting command loop: restart in progress.
      Rewriting Flash....
```

Información Relacionada

- Anuncio de fin de venta de los concentradores Serie VPN 5000 de Cisco
- Página de soporte del concentrador VPN 5000 de Cisco
- Página de soporte para Cisco VPN 5000 Client
- Página de soporte de IPSec
- Soporte Técnico y Documentación - Cisco Systems