Contenido

Introducción

Este documento explica la configuración inicial del concentrador del Cisco VPN 5000 y demuestra cómo conectar con la red usando el IP y cómo ofrecer la conectividad VPN del LAN a LAN del modo principal IPSec.

Usted puede instalar el concentrador VPN en cualquiera de dos configuraciones, dependiendo de donde usted lo conecta con la red en relación con un Firewall. El concentrador VPN tiene dos accesos de Ethernet, uno de los cuales (el Ethernet 1) pasa solamente el tráfico IPSec. El otro puerto (ethernet0) rutea todo el tráfico IP. Si usted planea instalar el concentrador VPN paralelamente al Firewall, usted debe utilizar ambos puertos de modo que el ethernet0 haga frente al LAN protegido, y el Ethernet1 haga frente a Internet a través del router de gateway de Internet de la red. Usted puede también instalar el concentrador VPN detrás del Firewall en el LAN protegido y conectarlo a través del puerto del ethernet0, para pasar el tráfico IPSec que pasa entre Internet y el concentrador con el Firewall.

prerrequisitos

Requisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el concentrador del Cisco VPN 5000.

La información que se presenta en este documento se originó a partir de dispositivos dentro de 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 un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Configuración de conectividad básica

La manera más fácil de establecer la conectividad de red básica es conectar un cable serial con el puerto de la consola en el concentrador VPN y utilizar el de software de terminal para configurar la dirección IP en el puerto del ethernet0. Después de configurar la dirección IP en el puerto del ethernet0, usted puede utilizar Telnet para conectar con el concentrador VPN para completar la configuración. Usted puede también generar un archivo de configuración en un editor de textos apropiado, y lo envía al concentrador VPN usando el TFTP.

Usando el de software de terminal a través del puerto de la consola, le indican inicialmente para una contraseña. Utilice la contraseña “letmein.” Después de responder con la contraseña, publique el **comando configure ip ethernet 0**, respondiendo a los prompts con su información del sistema. La secuencia de prompts debe parecer el 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 ]#
```

Usted está listo ahora para configurar el puerto del Ethernet1.

Configuración del puerto Ethernet 1

La información de direccionamiento TCP/IP en el puerto del Ethernet1 es el externo, direccionamiento del Enrutable por Internet TCP/IP que usted asignó para el concentrador VPN. Evite usar un direccionamiento en la misma red TCP/IP que el ethernet0, pues esto inhabilitará el TCP/IP en el concentrador.

Ingrese los **comandos configure ip ethernet 1**, respondiendo a los prompts con su información del sistema. La secuencia de prompts debe parecer el 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 usted necesita configurar el gateway IPSec.

Configuración de la puerta de enlace IPSec

El los controles del gateway IPSec donde el concentrador VPN envía todo el IPSec, o tunneled, tráfico. Ésta es independiente de la ruta predeterminado que usted configura más adelante. Comience ingresando el **comando configure general**, respondiendo a los prompts con su información del sistema. La secuencia de prompts debe parecer el ejemplo mostrado abajo.

```
* 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 posterior, han cambiado al **comando ipsecgateway al comando vpngateway**.

Ahora configuremos la directiva del Internet Key Exchange (IKE).

Configuración de la política IKE

El control de parámetros del protocolo internet security association key management (ISAKMP) /IKE cómo el concentrador VPN y el cliente identifican y se autentican para establecer a las sesiones de túnel. Se refiere esta negociación inicial pues fase 1. los parámetros de la fase 1 son globales al dispositivo y no se asocian a una interfaz particular. Las palabras claves reconocidas en esta sección son descritas más abajo. Los parámetros de negociación de la fase 1 para los túneles de LAN a LAN se pueden fijar en la sección del [Tunnel Partner <Section ID>]. Controles de la negociación IKE de la fase 2 cómo el concentrador VPN y el cliente VPN manejan las sesiones de túnel individual. Los parámetros de la negociación IKE de la fase 2 para el concentrador VPN y el cliente VPN se fijan en el dispositivo del [VPN Group <Name>].

El sintaxis para la política IKE está como sigue.

```
* 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#
```

La contraseña de protección especifica a un conjunto de protección para la negociación ISAKMP/IKE entre el concentrador VPN y el cliente VPN. Esta palabra clave puede aparecer las épocas múltiples dentro de esta sección, en este caso el concentrador VPN propone a todos los conjuntos de protección específica. El cliente VPN valida una de las opciones para la negociación. El primer pedazo de cada opción, MD5 (la publicación de mensaje 5), es el algoritmo de autenticación usado para la negociación. Algoritmo de troceo seguro de la significa SHA, que se considera ser más seguro que el MD5. El segundo pedazo de cada opción es el algoritmo de encripción. El DES (Data Encryption Standard) utiliza una clave 56-bit para revolver los datos. El tercer pedazo de cada opción es el grupo Diffie-Hellman, usado para el intercambio de claves. Porque números más grandes son utilizados por el algoritmo del group2 (G2), es más seguro que el group1 (G1).

Para comenzar la configuración, ingrese el **comando configure IKE policy**, respondiendo a los prompts con su 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 usted ha configurado los fundamentos, es hora de definir el túnel y los parámetros de

comunicación IP.

Configuración de sitio a sitio de modo principal

Para configurar el concentrador VPN para soportar las conexiones de LAN a LAN, usted necesita definir la configuración del túnel, así como los parámetros de comunicación IP que se utilizarán en el túnel. Usted hará esto en dos secciones, la sección del [Tunnel Partner VPN x], y la sección del [IP VPN x]. Para cualquier configuración dada del sitio a localizar, el *x* definido en estas dos secciones debe hacer juego, para asociar la configuración del túnel correctamente a la configuración del protocolo.

Miremos cada uno de estas secciones detalladamente.

Configuración de la sección de socio de túnel

En la sección del partner de túnel, usted debe definir por lo menos los ocho parámetros siguientes.

- Transforme
- Partner
- KeyManage
- SharedKey
- Modo
- LocalAccess
- Par
- BindTo

Transforme

La palabra clave de la transformación especifica los tipos de protección y los algoritmos usados para las sesiones de cliente IKE. Cada opción asociada a este parámetro es una pieza de protección que especifica la autenticación y los parámetros de encripción. El parámetro de la transformación puede aparecer las épocas múltiples dentro de esta sección, en este caso el concentrador VPN propone las piezas de protección específicada en la orden que se analizan, hasta que una sea validado por el cliente para el uso durante la sesión. En la mayoría de los casos, solamente uno transforma la palabra clave es necesario.

Las opciones para la palabra clave de la transformación están como sigue.

```
* 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#
```

Significa Encapsulating Security Payload ESP y AH encabezado de autenticación de la significa. Ambas estas encabezados se utilizan para cifrar y para autenticar los paquetes. El DES (Data Encryption Standard) utiliza una clave 56-bit para revolver los datos. El 3DES utiliza tres diversas claves y tres aplicaciones del algoritmo DES para revolver los datos. El MD5 es el algoritmo de troceo del message-digest 5. El SHA es el algoritmo de troceo seguro, que se considera ser algo más seguro que el MD5.

ESP(MD5,DES) es la configuración predeterminada, y se recomienda para la mayoría de las configuraciones. Uso ESP de ESP(MD5) y ESP(SHA) de autenticar los paquetes (sin el cifrado). Uso de AH(MD5) y AH(SHA) AH de autenticar los paquetes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), y AH(SHA)+ESP(3DES) uso AH de autenticar los paquetes y el ESP para cifrar los paquetes.

Partner

La palabra clave de socio define la dirección IP del otro terminador de túnel en la sociedad del túnel. Este número debe ser un público, el IP Address ruteable con el cual el concentrador VPN local puede crear conexión IPSec.

KeyManage

La palabra clave KeyManage define cómo los dos concentradores VPN en una sociedad del túnel determinan qué dispositivo inicia el túnel y qué tipo de procedimiento de establecimiento del túnel a seguir. Las opciones son Automático, Iniciar, Responder y Manual. Usted puede utilizar las primeras tres opciones para configurar los túneles IKE, y la palabra clave manual para configurar los túneles de encripción corregidos. Este documento no cubre cómo configurar los túneles de encripción corregidos. El auto especifica que el partner de túnel puede iniciar y responder a las peticiones de la configuración de túnel. El iniciado especifica que el partner de túnel envía solamente las peticiones de la configuración de túnel, él no responde a ellas. Responda especifica que el partner de túnel responde a los pedidos de configuración de túnel, pero nunca los inicia.

SharedKey

La palabra clave de SharedKey se utiliza como el secreto compartido de IKE. Usted debe fijar el mismo valor de SharedKey en ambos partners de túnel.

Modo

La palabra clave de Modo define el protocolo de la negociación IKE. La configuración predeterminada es agresiva, así que fijar el concentrador VPN para el modo de interoperabilidad, usted debe fijar la palabra clave de Modo a la tubería.

LocalAccess

El LocalAccess define los números IP que se pueden acceder a través del túnel, de una máscara del host a una ruta predeterminado. La palabra clave LocalProto define que protocolo IP numera se puede acceder a través del túnel, tal como ICMP(1), TCP(6), UDP(17), y así sucesivamente. Si usted quiere pasar todos los números IP, después usted debe fijar LocalProto=0. LocalPort determina qué números del puerto se pueden alcanzar a través del túnel. LocalProto y LocalPort omiten 0, o el todo-acceso.

Par

La palabra clave del par especifica qué subredes se encuentran a través de un túnel. PeerProto especifica qué protocolos se permiten con el punto final del túnel remoto, y PeerPort fija qué números del puerto se pueden acceder en el otro extremo del túnel.

BindTo

El BindTo especifica qué acceso de Ethernet termina las conexiones del sitio a localizar. Usted debe fijar siempre este parámetro al Ethernet1, excepto cuando el concentrador VPN se está ejecutando en el modo de puerto único.

Configurar los parámetros

Para configurar estos parámetros, ingrese el **comando configure Tunnel Partner VPN 1**, respondiendo a los prompts con su información del sistema.

La secuencia de prompts debe parecer el ejemplo abajo.

```
*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 hora de configurar la sección IP.

Configuración de Sección IP

Usted puede utilizar las conexiones con o sin número (como en configuración IP en las conexiones WAN) en la sección de configuración IP de cada sociedad del túnel. Aquí, utilizamos innumerable.

La configuración mínima para una conexión sitio a sitio sin numerar requiere dos declaraciones: numbered=false y mode=routed. Comience ingresando los **comandos configure ip vpn 1**, y responda a los prompts del sistema como sigue.

```
*[ 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 hora de configurar una ruta predeterminado.

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

Usted necesita configurar una ruta predeterminado que el concentrador VPN pueda utilizar para enviar todo el tráfico TCP/IP destinado para las redes con excepción de las redes con las cuales está conectado directamente, o para cuáles tiene rutas dinámico. Las puntas de la ruta predeterminado de nuevo a todas las redes encontradas en el puerto interno. Usted configuró ya el Intraport para enviar el tráfico IPSec a y desde Internet usando el parámetro de gateway de IPSec. Para comenzar la configuración de la ruta predeterminado, ingrese el comando edit config ip static, respondiendo a los prompts con su información del sistema. La secuencia de prompts debe parecer el ejemplo abajo.

```
*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 paso más reciente es salvar la configuración. Cuando está preguntado si usted está seguro que usted quiere descargar la configuración y recomenzar el dispositivo, el tipo **y** y el Presione ENTER. No apague el concentrador VPN durante el proceso de arranque. Después de que el concentrador haya reiniciado, los usuarios pueden conectar usando el software cliente VPN del concentrador.

Para salvar la configuración, ingrese el **comando save**, como sigue.

```
*IntraPort2+_A56CB700# save      Save configuration to flash and restart device? y
```

Si usted está conectado con el concentrador VPN usando Telnet, la salida antedicha es toda lo que usted verá. Si usted está conectado a través de una consola, usted verá la salida similar al siguiente, solamente mucho más de largo. En el extremo de esta salida, el concentrador VPN vuelve “Hello Console (Saludo a la consola)…” y pide una contraseña. Éste es cómo usted sabe que le acaban.

```
*IntraPort2+_A56CB700# save      Save configuration to flash and restart device? y
```

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