Contenido

Introducción

Esta guía explica la configuración inicial del concentrador del Cisco VPN 5000, específicamente cómo configurarlo para conectar con la red usando el IP, y ofrece la Conectividad del cliente remoto.

Usted puede instalar el concentrador en cualquiera de dos configuraciones, dependiendo de donde usted lo conecta con la red en relación con un Firewall. El concentrador 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 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 específicos para este documento.

Componentes Utilizados

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

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

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 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 para completar la configuración. Usted puede también generar un archivo de configuración en un editor de textos apropiado, y lo envía al concentrador 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 esto:

```
*[ 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.

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. Evite usar un direccionamiento en la misma red TCP/IP que el ethernet0, pues esto inhabilitará el TCP/IP en el concentrador VPN.

Ingrese los **comandos configure ip ethernet 1**, respondiendo a los prompts con su información del sistema. La secuencia de prompts debe parecer esto:

```
*[ 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 la ruta predeterminado.

Ruta predeterminada

Usted necesita configurar una ruta predeterminado que el concentrador 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. Más adelante, usted configurará 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 esto:

```
*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#
```

Ahora usted necesita configurar el gateway IPSec.

Gateway IPSec

El los controles del gateway IPSec donde el concentrador envía todo el IPSec, o tunneled, tráfico. Ésta es independiente de la ruta predeterminado que usted acaba de configurar. Comience ingresando el **comando configure general**, respondiendo a los prompts con su información del sistema. La secuencia de prompts debe parecer esto:

```
* 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#
```

Después, configure la política IKE.

Política IKE

Fije los parámetros del protocolo internet security association key management/del intercambio de claves de Internet (ISAKMP/IKE) para el concentrador. Estas configuraciones controlan cómo el concentrador 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 las cliente administra la sesiones de túnel individual. Los parámetros de la negociación IKE de la fase 2 para el concentrador VPN y el cliente se fijan en el dispositivo del [VPN Group <Name>]

El sintaxis para la política IKE es 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. Esta palabra clave puede aparecer las

épocas múltiples dentro de esta sección, en este caso el concentrador propone a todos los conjuntos de protección específica. El cliente valida una de las opciones para la negociación. El primer pedazo de cada opción, MD-5 (el message-digest 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.

```
* 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 se configuran los fundamentos, ingrese los parámetros del grupo.

Configuración de grupo VPN

Al ingresar los parámetros del grupo, recuerde que el nombre del grupo VPN no debe contener los espacios, aunque el analizador de sintaxis de la línea de comandos permite que usted ingrese los espacios en el nombre del grupo VPN. El nombre del grupo VPN puede contener las cartas, los números, las rociadas, y los caracteres de subrayado.

Hay cuatro parámetros básicos que se requieren en cada grupo VPN para la operación IP:

- Maxconnections
- StartIPaddress o LocalIPNet
- Transforme
- IPNet

El parámetro Maxconnections es el número máximo de sesiones de cliente simultáneas permitidas en esta configuración de grupo VPN determinada. Tenga este número presente, como trabaja conjuntamente con el StartIPAddress o el parámetro LocalIPNet.

El concentrador VPN asigna los IP Addresses a los clientes remotos por dos diversos esquemas, StartIPAddress y LocalIPNet. El StartIPAddress asigna los números IP de la subred conectada con el ethernet0 y los proxy-ARP para los clientes conectados. El LocalIPNet asigna los números IP a los clientes remotos de una subred única a los clientes VPN, y requiere que el resto de la red está hecho enterado de la existencia de la subred VPN con el Static o Dynamic Routing. El StartIPAddress ofrece una configuración más fácil, pero puede limitar el tamaño del espacio de la dirección. El LocalIPNet ofrece la mayor flexibilidad de la dirección para los usuarios remotos, pero requiere levemente más trabajo configurar la encaminamiento necesaria.

Para el StartIPAddress, utilice la primera dirección IP asignada a una sesión de túnel del cliente entrante. En una configuración de la configuración básica, esto debe ser una dirección IP en la red interna TCP/IP (la misma red que el puerto del ethernet0). En nuestro ejemplo abajo, asignan la primera sesión de cliente el direccionamiento de 192.168.233.50, la sesión de cliente simultánea siguiente se asigna 192.168.233.51, y así sucesivamente. Hemos asignado un valor de Maxconnections de 30, que significa que necesitamos tener un bloque de 30 IP Addresses inusitados (servidores DHCP incluyendo si usted tiene ningunos) que comienzan con

192.168.233.50 y que terminan con 192.168.233.79. Avoid que solapa los IP Addresses usados en diversas configuraciones de grupo VPN.

El LocalIPNet asigna los IP Addresses a los clientes remotos de una subred que deba ser inusitada a otra parte en el LAN. Por ejemplo, si usted especifica el parámetro el "LocalIPNet=182.168.1.0/24" en la configuración de grupo VPN, el concentrador asigna los IP Addresses a los clientes que comienzan con 192.168.1.1. Por lo tanto, usted necesita asignar el "Maxconnections=254", pues el concentrador no prestará atención a los límites de subred al asignar el IP numera con el LocalIPNet.

La palabra clave de la transformación especifica los tipos de protección y los algoritmos que el concentrador utiliza para las sesiones de cliente IKE. Las opciones son 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#
```

Cada opción es una pieza de protección que especifica la autenticación y los parámetros de encripción. Esta palabra clave puede aparecer las épocas múltiples dentro de esta sección, en este caso el concentrador 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.

El ESP (SHA, DES), ESP(SHA,3DES), ESP(MD5,DES), y ESP(MD5,3DES) denotan la encabezado del Encapsulating Security Payload (ESP) 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, y 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 instalaciones. Uso de ESP(MD5) y ESP(SHA) el encabezado ESP de autenticar los paquetes sin el cifrado. Uso de AH(MD5) y AH(SHA) el Encabezado de autenticación de autenticar los paquetes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), y AH(SHA)+ESP(3DES) uso el encabezado de autenticación de autenticar los paquetes y el encabezado ESP para cifrar los paquetes.

Nota: El software de cliente del Mac OS no soporta AH la opción. Usted debe especificar por lo menos una opción ESP si usted utiliza el software de cliente del Mac OS.

El campo de IPNet es importante, puesto que controla donde los clientes concentradores pueden ir. Los valores que usted ingresa en este campo determinan qué tráfico TCP/IP es tunneled, o generalmente, donde un cliente que pertenece a este grupo VPN puede ir en su red.

Cisco recomienda el configurar de la red interna (en este ejemplo 192.168.233.0/24), así que todo el tráfico de un cliente que va a la red interna se envía a través del túnel, y por lo tanto se autentica y se cifra (si usted Enable Encryption). En este escenario, no hay otro tráfico tunneled; en lugar, ha ruteado normalmente. Usted puede tener entradas múltiples, incluyendo solo o las direcciones de host. El formato es el direccionamiento (en nuestro ejemplo, la dirección de red 192.168.233.0) y entonces la máscara asociada a ese direccionamiento en los bits (/24, que es una máscara del C de la clase).

Comience a esta parte de la configuración ingresando el **comando configure VPN group basic-**

user, y después responda a los prompts con su información del sistema. Aquí está un ejemplo de la secuencia de la configuración completa:

```
*IntraPort2+_A56CB700# configure VPN group basic-user      Section 'VPN Group basic-user' 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 "?"      *[ VPN Group "basic-user" ]# startipaddress=192.168.233.50
or      *[ VPN Group "basic-user" ]# localipnet=192.168.234.0/24      *[ VPN Group "basic-user"
]# maxconnections=30      *[ VPN Group "basic-user" ]# Transform=ESP(SHA,DES)      *[ VPN Group
"basic-user" ]# ipnet=192.168.233.0/24      *[ VPN Group "basic-user" ]# exit      Leaving
section editor.      *IntraPort2_A51EB700#
```

El siguiente paso es definir la base de datos de usuario.

Configuración del usuario VPN

En esta sección de la configuración, usted define la base de datos de usuarios de VPN. Cada línea define a un usuario de VPN junto con la configuración de grupo VPN y la contraseña de ese usuario. Las entradas multilínea deben tener saltos de línea que terminan con una barra. Sin embargo, los saltos de línea incluidos en las comillas dobles se preservan.

Cuando un cliente VPN comienza a una sesión de túnel, el nombre de usuario del cliente se transmite al dispositivo. Si el dispositivo encuentra al usuario en esta sección, utiliza la información en la entrada para configurar el túnel. (Usted puede también utilizar a un servidor de RADIUS para la autenticación de usuarios VPN). Si el dispositivo no encuentra el nombre de usuario, y usted no ha configurado a un servidor de RADIUS para realizar la autenticación, no abren a la sesión de túnel y un error se vuelve al cliente.

Comience la configuración ingresando el **comando edit config VPN users**. Miremos un ejemplo que agregue a un usuario nombrado el "User1" al grupo VPN “básico-usuario”.

```
*IntraPort2+_A56CB700# edit config VPN users      Section 'VPN users' not found in the config.
Do you want to add it to the config? y      <Name> <Config> <SharedKey>      Editing "[ VPN
Users ]"...      1: [ VPN Users ]      End of buffer      Edit [ VPN Users ]> append 1
Enter lines at the prompt. To terminate input, enter      a . on a line all by itself.
Append> User1 Config="basic-user" SharedKey="Burnt"      Append> .      Edit [ VPN Users ]> exit
Saving section...      Checking syntax...      Section checked successfully.
*IntraPort2+_A56CB700#
```

“Se quema” el SharedKey de este usuario. Todos estos valores de configuración son con diferenciación entre mayúsculas y minúsculas; si usted configura el "User1", el usuario debe ingresar el "User1" en el software de cliente. Ingresar el "user1" da lugar a un mensaje de error inválido o del usuario no autorizado. Usted puede continuar ingresando a los usuarios en vez de salir el editor, sino recordar, usted debe ingresar un período para salir el editor. El error hacer tan puede causar las Entradas no válidas en la configuración.

Terminar

Su paso más reciente está guardando la configuración. Cuando está preguntado si usted está seguro que usted quiere descargar la configuración y recomenzar el dispositivo, el tipo y y presionar tecla Enter (Intro). No apague el concentrador 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 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 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