Configuración inicial del Concentrador VPN 5000 de Cisco y para Acceso a cliente remoto.

Contenido

Introducción

Esta guía explica la configuración inicial del Cisco VPN 5000 Concentrator, específicamente cómo configurarlo para conectarse a la red mediante IP y ofrecer conectividad de cliente remoto.

Puede instalar el concentrador en cualquiera de las dos configuraciones, dependiendo de dónde lo conecte a la red en relación con un firewall. El concentrador 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 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 específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

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 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 para completar la configuración. También puede generar un archivo de configuración en un editor de texto apropiado y enviarlo al concentrador usando 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 tener el siguiente aspecto:

```
*[ 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.

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. Evite utilizar una dirección en la misma red TCP/IP que Ethernet 0, ya que esto desactivará TCP/IP en el concentrador VPN.

Ingrese los comandos **configure ip ethernet 1**, respondiendo a las indicaciones con la información del sistema. La secuencia de avisos debe tener el siguiente aspecto:

```
*[ 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 la ruta predeterminada.

Ruta predeterminada

Debe configurar una ruta predeterminada que el concentrador 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. Más adelante, configurará 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 tener el siguiente aspecto:

```
*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 debe configurar la puerta de enlace IPSec.

Gateway IPSec

La puerta de enlace IPSec controla dónde el concentrador envía todo el tráfico IPSec o tunelizado. Esto es independiente de la ruta predeterminada que acaba de configurar. Comience ingresando el comando **configure general**, respondiendo a las indicaciones con la información del sistema. La secuencia de avisos debe tener el siguiente aspecto:

```
* 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#
```

A continuación, configure la política IKE.

Política IKE

Establezca los parámetros del protocolo de administración de claves de la asociación de seguridad de Internet/intercambio de claves de Internet (ISAKMP/IKE) para el concentrador. Estos parámetros controlan cómo el concentrador 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 determinada. 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 fase 2 de negociación IKE controla cómo el VPN Concentrator y el cliente manejan las sesiones de túnel individuales. Los parámetros de negociación IKE de fase 2 para el concentrador VPN y el cliente 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 concentrador VPN y el cliente. Esta palabra clave puede aparecer varias veces en esta sección, en cuyo caso el concentrador propone todos los conjuntos de protección especificados. El cliente acepta una de las opciones para la negociación. La primera parte de cada opción, MD-5 (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.

```
* 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 han configurado los conceptos básicos, introduzca los parámetros de grupo.

Configuración de grupo VPN

Al ingresar parámetros de grupo, recuerde que el nombre del grupo VPN no debe contener espacios, aunque el analizador de línea de comandos le permita introducir espacios en el nombre del grupo VPN. El nombre del grupo VPN puede contener letras, números, guiones y guiones bajos.

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

- Maxconnections
- StartIPaddress o LocalIPNet
- Transformación
- IPNet

El parámetro Maxconnections es el número máximo de sesiones de cliente simultáneas permitidas en esta configuración de grupo de VPN en particular. Tenga en cuenta este número, ya que funciona junto con el parámetro StartIPAddress o LocalIPNet.

El concentrador VPN asigna direcciones IP a los clientes remotos mediante dos esquemas diferentes, StartIPAddress y LocalIPNet. Start(Inicio) La dirección IP asigna números IP de la subred conectada a Ethernet 0 y barras proxy para los clientes conectados. LocalIPNet asigna números IP a los clientes remotos desde una subred exclusiva para los clientes VPN, y requiere que el resto de la red sea consciente de la existencia de la subred VPN a través de un ruteo estático o dinámico. Start(Dirección IP de inicio) ofrece una configuración más sencilla, pero puede limitar el tamaño del espacio de direcciones. LocalIPNet ofrece una mayor flexibilidad de direccionamiento para los usuarios remotos, pero requiere un poco más de trabajo para configurar el ruteo necesario.

Para StartIPAddress, utilice la primera dirección IP asignada a una sesión de túnel de cliente entrante. En una configuración básica, debe ser una dirección IP en la red TCP/IP interna (la misma red que el puerto Ethernet 0). En nuestro ejemplo a continuación, a la primera sesión de cliente se le asigna la dirección 192.168.233.50, la siguiente sesión de cliente simultánea se asigna 192.168.233.51, y así sucesivamente. Hemos asignado un valor de Maxconnections de 30, lo que significa que necesitamos un bloque de 30 direcciones IP no utilizadas (incluidos los servidores DHCP, si los tiene) a partir de 192.168.233.50 y hasta 192.168.233.79. Evite la superposición de las direcciones IP usadas en diferentes configuraciones de grupo VPN.

LocalIPNet asigna direcciones IP a los clientes remotos desde una subred que se debe utilizar en otra parte de la LAN. Por ejemplo, si especifica el parámetro "LocalIPNet=182.168.1.0/24" en la configuración del grupo VPN, el concentrador asigna direcciones IP a los clientes que comienzan por 192.168.1.1. Por lo tanto, debe asignar "Maxconnections=254", ya que el concentrador no tendrá en cuenta los límites de subred al asignar números IP mediante LocalIPNet.

La palabra clave Transform especifica los tipos de protección y algoritmos que el concentrador utiliza para las sesiones de cliente IKE. Las opciones son las siguientes:

```
Transform = [ 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) ]
```

Cada opción es una pieza de protección que especifica los parámetros de autenticación y cifrado. Esta palabra clave puede aparecer varias veces dentro de esta sección, en cuyo caso el concentrador 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.

ESP(SHA,DES), ESP(SHA,3DES), ESP(MD5,DES) y ESP(MD5,3DES) denotan el encabezado de carga de seguridad de encapsulación (ESP) 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 y 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 instalaciones. ESP(MD5) y ESP(SHA) utilizan el encabezado ESP para autenticar los paquetes sin cifrado. AH(MD5) y AH(SHA) utilizan el encabezado de autenticación (AH) para autenticar los paquetes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) y AH(SHA)+ESP(3DES) utilizan el encabezado de autenticación para autenticar los paquetes y el encabezado ESP para cifrar los paquetes.

Nota: El software Mac OS Client no soporta la opción AH. Debe especificar al menos una opción ESP si utiliza el software Mac OS Client.

El campo IPNet es importante, ya que controla dónde pueden ir los clientes del concentrador. Los valores introducidos en este campo determinan qué tráfico TCP/IP se tuneliza, o más comúnmente, dónde un cliente que pertenece a este grupo de VPN puede conectarse a su red.

Cisco recomienda configurar la red interna (en este ejemplo 192.168.233.0/24), de modo que todo el tráfico de un cliente que va a la red interna se envíe a través del túnel y, por lo tanto, se autentique y se cifre (si habilita el cifrado). En esta situación, no se tuneliza ningún otro tráfico; en su lugar, se rutea normalmente. Puede tener varias entradas, incluidas direcciones únicas o de host. El formato es la dirección (en nuestro ejemplo, la dirección de red 192.168.233.0) y luego la máscara asociada con esa dirección en bits (/24, que es una máscara de clase C).

Inicie esta parte de la configuración ingresando el comando **configure VPN group basic-user** y luego responda a las indicaciones con la información del sistema. Este es un ejemplo de la secuencia de 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 del usuario.

Configuración del usuario VPN

En esta sección de la configuración, define la base de datos de usuarios de VPN. Cada línea define un usuario VPN junto con la configuración y contraseña del grupo VPN de ese usuario. Las entradas de varias líneas deben tener saltos de línea que terminen con una barra invertida. Sin embargo, se conservan los saltos de línea entre comillas dobles.

Cuando un cliente VPN inicia 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 de la

entrada para configurar el túnel. (También puede utilizar un servidor RADIUS para la autenticación de usuarios de VPN). Si el dispositivo no encuentra el nombre de usuario y no ha configurado un servidor RADIUS para realizar la autenticación, la sesión del túnel no se abre y se devuelve un error al cliente.

Inicie la configuración ingresando el comando **edit config VPN users**. Veamos un ejemplo que agrega un usuario denominado "User1" al grupo VPN "basic-user".

```
*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#
```

La clave compartida de este usuario es "Quemada". Todos estos valores de configuración distinguen entre mayúsculas y minúsculas; si configura "User1", el usuario debe introducir "User1" en el software cliente. Al ingresar "user1", aparece un mensaje de error de usuario no válido o no autorizado. Puede seguir introduciendo usuarios en lugar de salir del editor, pero recuerde que debe introducir un período para salir del editor. Si no lo hace, pueden producirse entradas no válidas en la configuración.

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 la tecla Intro. No apague el concentrador durante el proceso de arranque. Después de que el concentrador se haya reiniciado, los usuarios pueden conectarse mediante el software concentrador VPN Client.

Para guardar la configuración, ingrese el comando **save**, de la siguiente manera:

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

Si está conectado al concentrador 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 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