Configurando o Cisco VPN 5000 Concentrator e implementando a conectividade VPN de LAN para LAN de modo principal de IPSec

Índice

Introdução

Este documento explica a configuração inicial do concentrador do Cisco VPN 5000 e demonstra como conectar à rede usando o IP e como oferecer a conectividade de VPN do LAN para LAN do modo principal IPSec.

Você pode instalar o concentrador VPN em qualquer uma de duas configurações, segundo onde você o conecta à rede com relação a um Firewall. O concentrador VPN tem duas portas Ethernet, uma de que (Ethernet1) passa somente o tráfego de IPSec. A outra porta (ethernet0) distribui todo o tráfego IP. Se você planeia instalar o concentrador VPN paralelamente ao Firewall, você deve usar ambas as portas de modo que o ethernet0 enfrente o LAN protegido, e Ethernet1 enfrente o Internet através do Internet Gateway Router da rede. Você pode igualmente instalar o concentrador VPN atrás do Firewall no LAN protegido e conectá-lo através da porta do ethernet0, de modo que o tráfego de IPSec que passa entre o Internet e o concentrador seja passado com o Firewall.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no concentrador do Cisco VPN 5000.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Configuração de conectividade básica

A maneira a mais fácil de estabelecer a conectividade de rede básica é conectar um cabo serial à porta de Console no concentrador VPN e usar o software terminal para configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT na porta do ethernet0. Após ter configurado o endereço IP de Um ou Mais Servidores Cisco ICM NT na porta do ethernet0, você pode usar o telnet para conectar ao concentrador VPN para terminar a configuração. Você pode igualmente gerar um arquivo de configuração em um editor de texto apropriado, e envia-o ao concentrador VPN usando o TFTP.

Usando o software terminal através da porta de Console, você é alertado inicialmente para uma senha. Use a senha “letmein.” Após a resposta com a senha, emita o **comando configure ip ethernet 0**, respondendo às alertas com sua informação de sistema. A sequência das alertas deve olhar como o exemplo seguinte.

```
*[ 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 ]#
```

Agora você está pronto para configurar a porta de Ethernet1.

Configurando a porta Ethernet 1

A informação de endereçamento TCP/IP na porta de Ethernet1 é a externo, endereço que do Internet roteável TCP/IP você atribuiu para o concentrador VPN. Evite usar um endereço na mesma rede TCP/IP que o ethernet0, porque isto desabilitará o TCP/IP no concentrador.

Inscreva os **comandos configure ip ethernet 1**, respondendo às alertas com sua informação de

sistema. A sequência das alertas deve olhar como o exemplo seguinte.

```
*[ 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 ]#
```

Agora você precisa de configurar o gateway IPSec.

Configurando o gateway IPSec

Os controles do gateway IPSec onde o concentrador VPN envia todo o IPsec, ou escavado um túnel, tráfego. Este é independente da rota padrão que você configura mais tarde. Comece inscrevendo o **comando configure general**, respondendo às alertas com sua informação de sistema. A sequência das alertas deve olhar como o exemplo mostrado abaixo.

```
* 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#
```

Note: Nas liberações 6.x e mais tarde, o **comando ipsecgateway** foi mudado ao **comando vpngateway**.

Deixe-nos agora configuram a política do Internet Key Exchange (IKE).

Configurando a política de IKE

O controle de parâmetros do protocolo internet security association key management (ISAKMP) /IKE como o concentrador VPN e o cliente identificam e se autenticam para estabelecer sessões de túnel. Esta negociação inicial é referida porque fase 1. os parâmetros da fase 1 são globais ao dispositivo e não são associados com uma interface particular. As palavras-chaves reconhecidas nesta seção são descritas abaixo. Os parâmetros de negociação da fase 1 para túneis de LAN para LAN podem ser ajustados na seção do [Tunnel Partner <Section ID>]. Controles da negociação de IKE da fase 2 como o concentrador VPN e o cliente VPN tratam sessões de túnel individual. Os parâmetros da negociação de IKE da fase 2 para o concentrador VPN e o cliente VPN são ajustados no dispositivo do [VPN Group <Name>].

A sintaxe para a política de IKE é como segue.

```
* 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#
```

As palavras-chave de proteção especificam uma suite de proteção para a negociação ISAKMP/IKE entre o concentrador VPN e o cliente VPN. Esta palavra-chave pode aparecer épocas múltiplas dentro desta seção, neste caso o concentrador VPN propõe todos os conjuntos de proteção especificados. O cliente VPN aceita uma das opções para a negociação. A primeira parte de cada opção, MD5 (message digest 5), é o algoritmo de autenticação usado para a negociação. O SHA representa o algoritmo de mistura segura, que é considerado ser mais seguro do que o MD5. A segunda parte de cada opção é o algoritmo de criptografia. O DES (criptografia padrão de dados) usa uma chave 56-bit à precipitação os dados. A terceira parte de cada opção é o grupo Diffie-Hellman, usado para trocas de chave. Porque os números maiores são usados pelo algoritmo do grupo2 (G2), é mais seguro do que o grupo1 (G1).

Para começar a configuração, inscreva o **comando configure IKE policy**, respondendo às alertas com sua informação de sistema. Um exemplo é mostrado abaixo.

```
* 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#
```

Agora que você configurou os princípios, é hora de definir o túnel e os parâmetros de comunicação IP.

Configuração de site a site do modo principal

Para configurar o concentrador VPN para apoiar conexões de LAN para LAN, você precisa de definir a configuração de túnel, assim como os parâmetros de comunicação IP a ser usados no túnel. Você fará este em duas seções, na seção do [Tunnel Partner VPN x], e na seção do [IP VPN x]. Para toda a configuração de site para site dada, o *x* definido nestas duas seções deve combinar, de modo que a configuração de túnel seja associada corretamente com a configuração de protocolo.

Deixe-nos olhar em detalhe cada um destas seções.

Configurando a seção de sócio de túnel

Na seção do sócio de túnel, você deve definir pelo menos os seguintes oito parâmetros.

- Transforme
- Sócio
- Gerente principal

- Chave compartilhada
- Modo
- LocalAccess
- Par
- BindTo

Transforme

A palavra-chave da transformação especifica os tipos de proteção e os algoritmos usados para sessões de cliente IKE. Cada opção associada com este parâmetro é uma parte da proteção que especifique a autenticação e os parâmetros de criptografia. O parâmetro da transformação pode aparecer épocas múltiplas dentro desta seção, neste caso o concentrador VPN propõe as peças de proteção especificadas na ordem que estão analisados gramaticalmente, até que uma esteja aceitado pelo cliente para o uso durante a sessão. Na maioria dos casos, somente um transforma a palavra-chave é precisado.

As opções para a palavra-chave da transformação são como segue.

```
* 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#
```

O ESP representa o Encapsulating Security Payload e o AH representa o cabeçalho de autenticação. Ambos estes encabeçamentos são usados para cifrar e autenticar pacotes. O DES (criptografia padrão de dados) usa uma chave 56-bit à precipitação os dados. O 3DES usa três chaves diferentes e três aplicativos do algoritmo de DES à precipitação os dados. O MD5 é o algoritmo de hash do sumário de mensagem 5. O SHA é o algoritmo de mistura segura, que é considerado ser um tanto mais seguro do que o MD5.

ESP(MD5,DES) são a configuração padrão, e são recomendados para a maioria de instalações. Uso ESP de ESP(MD5) e ESP(SHA) autenticar pacotes (sem a criptografia). Uso AH de AH(MD5) e AH(SHA) autenticar pacotes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), e AH(SHA)+ESP(3DES) uso AH autenticar pacotes e ESP para cifrar pacotes.

Sócio

As palavras-chave de parceiro definem o endereço IP de Um ou Mais Servidores Cisco ICM NT do outro exterminador de túnel na parceria do túnel. Este número deve ser um público, o endereço IP roteável com que o concentrador VPN local pode criar uma conexão IPSec.

Gerente principal

As palavras-chave de gerenciamento principal definem como os dois concentradores VPN em uma parceria do túnel determinam que dispositivo inicia o túnel e que tipo de procedimento de

estabelecimento de túnel a seguir. As opções são automático, iniciar, responder e manual. Você pode usar as primeiras três opções para configurar túneis IKE, e o palavra-chave manual para configurar túneis de criptografia fixa. Este documento não cobre como configurar túneis de criptografia fixa. O automóvel especifica que o sócio de túnel pode iniciar e responder aos pedidos da configuração do túnel. O novato especifica que o sócio de túnel envia somente pedidos da configuração do túnel, ele não lhes responde. Responda especifica que o sócio de túnel responde às solicitações de ajuste de túnel, mas nunca inicia-as.

Chave compartilhada

As palavras-chave de chave compartilhadas são usadas como o segredo compartilhado de IKE. Você deve ajustar o mesmo valor de chave compartilhada em ambos os sócios de túnel.

Modo

As palavras-chave de modo definem o protocolo da negociação de IKE. A configuração padrão é agressiva, assim que para ajustar o concentrador VPN para o modo de interoperabilidade, você deve ajustar as palavras-chave de modo ao cano principal.

LocalAccess

O LocalAccess define os números IP que podem ser alcançados através do túnel, de uma máscara do host a uma rota padrão. O palavra-chave LocalProto define que os números do protocolo IP podem ser alcançados através do túnel, tal como ICMP(1), TCP(6), UDP(17), e assim por diante. Se você quer passar todos os números IP, a seguir você deve ajustar LocalProto=0. LocalPort determina que números de porta podem ser alcançados através do túnel. LocalProto e LocalPort optam 0, ou todo-acesso.

Par

A palavra-chave do par especifica que sub-redes são encontradas através de um túnel. PeerProto especifica que protocolos são permitidos através do ponto final de túnel remoto, e PeerPort ajusta-se que números de porta podem ser alcançados no outro extremo do túnel.

BindTo

Especifica BindTo que porta Ethernet termina conexões de site para site. Você deve sempre ajustar este parâmetro a Ethernet1, exceto quando o concentrador VPN está sendo executado no modo de porta único.

Configurando os parâmetros

Para configurar estes parâmetros, inscreva o **comando configure Tunnel Partner VPN 1**, respondendo às alertas com sua informação de sistema.

A sequência das alertas deve olhar como o exemplo abaixo.

```
*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.
```

Agora é hora de configurar a seção IP.

Configuração da seção de IP

Você pode usar conexões numeradas ou não numerada (como na configuração IP em conexões de WAN) na seção de configuração IP de cada parceria do túnel. Aqui, nós usamos unnumbered.

A configuração mínima para uma conexão de site-a-site não numerada exige duas indicações: numbered=false e mode=routed. Comece inscrevendo os **comandos configure ip vpn 1**, e responda às alertas do sistema como segue.

```
*[ 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
```

Agora é hora de estabelecer uma rota padrão.

Configurando a rota padrão (tabela de rota TCP/IP)

Você precisa de configurar uma rota padrão que o concentrador VPN possa usar para enviar todo o tráfego TCP/IP destinado para redes diferentes das redes a que se conecta diretamente, ou para quais tem rotas dinâmica. Os pontos da rota padrão de volta a todas as redes encontradas na porta interna. Você já configurou Intraport para enviar o tráfego de IPSec a e do Internet usando o parâmetro de Gateway IPSec. Para começar a configuração da rota padrão, inscreva o comando edit config ip static, respondendo às alertas com sua informação de sistema. A sequência das alertas deve olhar como o exemplo abaixo.

```
*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#
```

Finalizando

A última etapa é salvar a configuração. Quando perguntado se você é certo que você quer transferir a configuração e reiniciar o dispositivo, o tipo **y** e pressiona **entra**. Não desligue o concentrador VPN durante o processo de boot. Depois que o concentrador recarregou, os usuários podem conectar usando o software do cliente VPN do concentrador.

Para salvar a configuração, inscreva o **comando save**, como segue.

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

Se você é conectado ao concentrador VPN usando o telnet, a saída acima é tudo que você verá. Se você é conectado através de um console, você verá a saída similar ao seguinte, somente muito mais por muito tempo. Na extremidade desta saída, o concentrador VPN retorna o “console de hello…” e pede uma senha. Isto é como você sabe que você está terminado.

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

Informações Relacionadas

- Anúncio End-of-Life de concentradores do Cisco VPN 5000 Series
- Página de suporte do Cisco VPN 5000 Concentrator
- Página de suporte ao cliente do Cisco VPN 5000
- Página de suporte IPSec
- Suporte Técnico e Documentação - Cisco Systems