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

Contents

Introduction

Este documento explica a configuração inicial do Cisco VPN 5000 Concentrator e demonstra como se conectar à rede usando IP e como oferecer conectividade VPN LAN-to-LAN de modo principal IPSec.

Você pode instalar o VPN Concentrator em uma das duas configurações, dependendo de onde você o conecta à rede em relação a um firewall. O VPN Concentrator tem duas portas Ethernet, uma das quais (Ethernet 1) passa apenas tráfego IPSec. A outra porta (Ethernet 0) roteia todo o tráfego IP. Se você planeja instalar o VPN Concentrator em paralelo com o firewall, você deve usar ambas as portas para que a Ethernet 0 encare a LAN protegida, e a Ethernet 1 enfrenta a Internet através do roteador de gateway de Internet da rede. Você também pode instalar o VPN Concentrator atrás do firewall na LAN protegida e conectá-lo através da porta Ethernet 0, de modo que o tráfego IPSec que passa entre a Internet e o concentrador passe pelo firewall.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco VPN 5000 Concentrator.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

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

Configuração de conectividade básica

A maneira mais fácil de estabelecer a conectividade básica da rede é conectar um cabo serial à porta de console no VPN Concentrator e usar o software de terminal para configurar o endereço IP na porta Ethernet 0. Depois de configurar o endereço IP na porta Ethernet 0, você pode usar o Telnet para se conectar ao VPN Concentrator para concluir a configuração. Você também pode gerar um arquivo de configuração em um editor de texto apropriado e enviá-lo ao VPN Concentrator usando TFTP.

Usando o software terminal através da porta de console, você é inicialmente solicitado a fornecer uma senha. Use a senha "letmein". Depois de responder com a senha, emita o comando **configure ip ethernet 0**, respondendo aos prompts com as informações do sistema. A sequência de prompts deve ser semelhante ao exemplo a seguir.

```
*[ 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 Ethernet 1.

Configurando a porta Ethernet 1

As informações de endereçamento TCP/IP na porta Ethernet 1 são o endereço TCP/IP externo roteável pela Internet atribuído ao VPN Concentrator. Evite usar um endereço na mesma rede TCP/IP da Ethernet 0, pois isso desabilitará o TCP/IP no concentrador.

Insira os comandos **configure ip ethernet 1**, respondendo aos prompts com as informações do sistema. A sequência de prompts deve ser semelhante ao exemplo a seguir.

```
*[ 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 configurar o gateway IPSec.

Configurando o gateway IPSec

O gateway IPSec controla onde o VPN Concentrator envia todo o tráfego IPSec ou em túnel. Isso é independente da rota padrão configurada posteriormente. Comece inserindo o comando **configure general**, respondendo aos prompts com as informações do sistema. A sequência de prompts deve ser semelhante ao 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#
```

Observação: nas versões 6.x e posterior, o comando **ipsecgateway** foi alterado para o comando **vpngateway**.

Agora, vamos configurar a política do Internet Key Exchange (IKE).

Configurando a política de IKE

Os parâmetros ISAKMP (Internet Security Association Key Management Protocol)/IKE controlam como o VPN Concentrator e o cliente se identificam e autenticam para estabelecer sessões de túnel. Essa negociação inicial é conhecida como Fase 1. Os parâmetros da fase 1 são globais para o dispositivo e não estão associados a uma interface específica. As palavras-chave reconhecidas nesta seção estão descritas abaixo. Os parâmetros de negociação da fase 1 para túneis LAN a LAN podem ser definidos na seção [Tunnel Partner <Section ID>]. A fase 2 da negociação de IKE controla como o VPN Concentrator e o VPN Client tratam sessões individuais de túnel. Os parâmetros de negociação IKE da Fase 2 para o VPN Concentrator e o VPN Client estão definidos no dispositivo [VPN Group <Name>].

A sintaxe da política IKE é a seguinte.

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

A palavra-chave protection especifica um conjunto de proteção para a negociação ISAKMP/IKE entre o VPN Concentrator e o VPN Client. Essa palavra-chave pode aparecer várias vezes nesta seção, caso em que o VPN Concentrator propõe todos os conjuntos de proteção especificados. O VPN Client 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. SHA significa Algoritmo de hash seguro, que é considerado mais seguro que MD5. A segunda parte de cada opção é o algoritmo de criptografia. O DES (Data Encryption Standard) usa uma chave de 56 bits

para embaralhar os dados. A terceira parte de cada opção é o grupo Diffie-Hellman, usado para troca de chaves. Como números maiores são usados pelo algoritmo Grupo 2 (G2), ele é mais seguro do que Grupo 1 (G1).

Para iniciar a configuração, insira o comando **configure IKE policy**, respondendo aos prompts com as informações do 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 conceitos básicos, é hora de definir os parâmetros de túnel e de comunicação IP.

Configuração de site a site do modo principal

Para configurar o VPN Concentrator para suportar conexões LAN a LAN, você precisa definir a configuração do túnel, bem como os parâmetros de comunicação IP a serem usados no túnel. Você fará isso em duas seções, a seção [Tunnel Partner VPN x] e a seção [IP VPN x]. Para qualquer configuração de site a site específica, o *x* definido nessas duas seções deve corresponder, de modo que a configuração do túnel esteja corretamente associada à configuração do protocolo.

Vamos ver cada uma dessas seções em detalhes.

Configurando a seção de sócio de túnel

Na seção tunnel partner, você deve definir pelo menos os oito parâmetros a seguir.

- Transformação
- Parceiro
- KeyManage
- SharedKey
- Modo
- LocalAccess
- Correspondente
- VincularA

Transformação

A palavra-chave Transform especifica os tipos de proteção e os algoritmos usados para sessões de cliente IKE. Cada opção associada a esse parâmetro é uma peça de proteção que especifica parâmetros de autenticação e criptografia. O parâmetro Transform pode aparecer várias vezes nesta seção, caso em que o VPN Concentrator propõe os pedaços de proteção especificados na ordem em que são analisados, até que um seja aceito pelo cliente para uso durante a sessão. Na

maioria dos casos, apenas uma palavra-chave Transform é necessária.

As opções para a palavra-chave Transform são as seguintes.

```
[ 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 e AH significa Authentication Header. Ambos os cabeçalhos são usados para criptografar e autenticar pacotes. O DES (Data Encryption Standard) usa uma chave de 56 bits para embaralhar os dados. 3DES usa três chaves diferentes e três aplicativos do algoritmo DES para embaralhar os dados. MD5 é o algoritmo hash message-digest 5. SHA é o algoritmo de hash seguro, que é considerado um pouco mais seguro do que MD5.

ESP(MD5,DES) é a configuração padrão e é recomendado para a maioria das configurações. ESP(MD5) e ESP(SHA) usam ESP para autenticar pacotes (sem criptografia). AH(MD5) e AH(SHA) usam AH para autenticar pacotes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) e AH(SHA)+ESP(3DES) usam AH para autenticar pacotes e ESP para criptografar pacotes.

Parceiro

A palavra-chave Partner define o endereço IP do outro terminador de túnel na parceria de túnel. Esse número deve ser um endereço IP público roteável com o qual o VPN Concentrator local pode criar uma conexão IPSec.

KeyManage

A palavra-chave KeyManage define como os dois VPN Concentrators em uma parceria de túnel determinam qual dispositivo inicia o túnel e que tipo de procedimento de estabelecimento de túnel seguir. As opções são Automático, Iniciar, Responder e Manual. Você pode usar as três primeiras opções para configurar túneis IKE e a palavra-chave Manual para configurar túneis de criptografia fixa. Este documento não aborda como configurar túneis de criptografia fixa. Auto especifica que o parceiro de túnel pode iniciar e responder às solicitações de configuração de túnel. Initiate especifica que o parceiro de túnel envia somente solicitações de configuração de túnel, ele não responde a elas. Respond especifica que o parceiro de túnel responde às solicitações de configuração de túnel, mas nunca as inicia.

SharedKey

A palavra-chave SharedKey é usada como o segredo compartilhado IKE. Você deve definir o mesmo valor SharedKey em ambos os parceiros de túnel.

Modo

A palavra-chave Mode define o protocolo de negociação IKE. A configuração padrão é Aggressive, portanto, para definir o VPN Concentrator para o modo de interoperabilidade, você deve definir a palavra-chave Mode como Main.

LocalAccess

LocalAccess define os números IP que podem ser acessados pelo túnel, de uma máscara de host para uma rota padrão. A palavra-chave LocalProto define quais números de protocolo IP podem ser acessados pelo túnel, como ICMP(1), TCP(6), UDP(17) e assim por diante. Se quiser passar todos os números IP, defina LocalProto=0. LocalPort determina quais números de porta podem ser acessados pelo túnel. LocalProto e LocalPort padrão são 0 ou all-access.

Correspondente

A palavra-chave Peer especifica quais sub-redes são encontradas através de um túnel. PeerProto especifica quais protocolos são permitidos através do ponto final do túnel remoto e PeerPort define quais números de porta podem ser acessados na outra extremidade do túnel.

VincularA

BindTo especifica qual porta Ethernet encerra conexões site a site. Você deve sempre definir esse parâmetro como Ethernet 1, exceto quando o VPN Concentrator está sendo executado no modo de porta única.

Configuração dos parâmetros

Para configurar esses parâmetros, insira o comando **configure Tunnel Partner VPN 1**, respondendo aos prompts com as informações do sistema.

A sequência de prompts deve ser semelhante ao 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 numeradas (como na configuração IP em conexões WAN) na seção de configuração IP de cada parceria de túnel. Aqui, usamos não numerados.

A configuração mínima para uma conexão site a site não numerada requer duas afirmações: numbered=false e mode=routed. Comece inserindo os comandos **configure ip vpn 1** e responda aos prompts do sistema da seguinte maneira.

```
*[ 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 configurar uma rota padrão.

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

Você precisa configurar uma rota padrão que o VPN Concentrator possa usar para enviar todo o tráfego TCP/IP destinado a redes diferentes da(s) rede(s) à(s) qual(is) ele está diretamente conectado(s) ou para a qual ele tem rotas dinâmicas. A rota padrão aponta de volta para todas as redes encontradas na porta interna. Você já configurou a Intraport para enviar tráfego IPSec de e para a Internet usando o parâmetro IPSec Gateway. Para iniciar a configuração da rota padrão, insira o comando edit config ip static, respondendo aos prompts com as informações do sistema. A sequência de prompts deve ser semelhante ao 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 tem certeza de que deseja baixar a configuração e reiniciar o dispositivo, digite **y** e pressione **Enter**. Não desligue o VPN Concentrator durante o processo de inicialização. Após a reinicialização do concentrador, os usuários podem se conectar usando o software VPN Client do concentrador.

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

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

Se você estiver conectado ao VPN Concentrator usando Telnet, a saída acima é tudo o que você verá. Se estiver conectado por um console, você verá uma saída semelhante à seguinte, apenas por muito tempo. No final dessa saída, o VPN Concentrator retorna "Hello Console..." e solicita

uma senha. É assim que você sabe que terminou.

```
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....
```

Informações Relacionadas

- Anúncio do fim do ciclo de comercialização dos concentradores Cisco VPN 5000 Series
- Página de suporte do Cisco VPN 5000 Concentrator
- Página de suporte do Cisco VPN 5000 Client
- Página de suporte do IPSec
- Suporte Técnico e Documentação - Cisco Systems