Configurando o Concentrador Cisco VPN 5000 Inicialmente e para Acesso ao Cliente Remoto

Contents

Introduction

Este guia explica a configuração inicial do Cisco VPN 5000 Concentrator, especificamente como configurá-lo para se conectar à rede usando IP e oferecer conectividade de cliente remoto.

Você pode instalar o concentrador em uma das duas configurações, dependendo de onde você o conecta à rede em relação a um firewall. O concentrador 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 concentrador 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.

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.

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 do console no concentrador 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 concentrador para concluir a configuração. Você também pode gerar um arquivo de configuração em um editor de texto apropriado e enviá-lo ao concentrador 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 assim:

```
*[ 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.

Porta Ethernet 1

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

Insira os comandos **configure ip ethernet 1**, respondendo aos prompts com as informações do sistema. A sequência de prompts deve ser assim:

```
*[ 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 a rota padrão.

Rota padrão

Você precisa configurar uma rota padrão que o concentrador pode 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. Posteriormente, você configurará 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 assim:

```
*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#
```

Agora você precisa configurar o Gateway IPSec.

Gateway de IPSec

O Gateway IPSec controla onde o concentrador envia todo o tráfego IPSec ou em túnel. Isso é independente da rota padrão que você acabou de configurar. Comece inserindo o comando **configure general**, respondendo aos prompts com as informações do sistema. A sequência de prompts deve ser assim:

```
* 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#
```

Em seguida, configure a política IKE.

Política IKE

Defina os parâmetros do Internet Security Association Key Management Protocol/Internet Key Exchange (ISAKMP/IKE) para o concentrador. Essas configurações controlam como o concentrador e o cliente se identificam e se 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 negociação IKE da Fase 2 controla como o VPN Concentrator e o cliente lidam com sessões de túnel individuais. Os parâmetros de negociação IKE da fase 2 para o VPN Concentrator e o cliente 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 cliente. Essa palavra-chave pode aparecer várias vezes nesta seção, caso em que o concentrador propõe todos os conjuntos de proteção especificados. O cliente aceita uma das opções para a negociação. A primeira parte de cada opção, MD-5 (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.

```
* 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 os conceitos básicos estão configurados, insira os parâmetros do grupo.

Configuração de grupo de VPN

Ao inserir parâmetros de grupo, lembre-se de que o nome do grupo VPN não deve conter espaços, mesmo que o analisador de linha de comando permita inserir espaços no nome do grupo VPN. O nome do grupo VPN pode conter letras, números, traços e sublinhados.

Há quatro parâmetros básicos necessários em cada grupo VPN para a operação IP:

- Máxconexões
- StartIPaddress ou LocalIPNet
- Transformação
- IPNet

O parâmetro Maxconnections é o número máximo de sessões simultâneas de cliente permitidas nesta configuração específica do grupo VPN. Lembre-se desse número, pois ele funciona em conjunto com o parâmetro StartIPAaddress ou LocalIPNet.

O VPN Concentrator atribui endereços IP a clientes remotos por dois esquemas diferentes, StartIPAaddress e LocalIPNet. StartIPAaddress atribui números IP da sub-rede conectada à Ethernet 0 e proxy-arps para os clientes conectados. LocalIPNet atribui números IP a clientes remotos de uma sub-rede exclusiva para os clientes VPN e exige que o resto da rede seja informado sobre a existência da sub-rede VPN através de roteamento estático ou dinâmico. StartIPAaddress oferece configuração mais fácil, mas pode limitar o tamanho do espaço de endereço. O LocalIPNet oferece maior flexibilidade de endereçamento para usuários remotos, mas requer um pouco mais de trabalho para configurar o roteamento necessário.

Para StartIPAaddress, use o primeiro endereço IP atribuído a uma sessão de túnel de cliente de entrada. Em uma configuração básica, esse deve ser um endereço IP na rede TCP/IP interna (a mesma rede da porta Ethernet 0). Em nosso exemplo abaixo, a primeira sessão de cliente recebe o endereço 192.168.233.50, a próxima sessão de cliente simultânea recebe 192.168.233.51 e assim por diante. Atribuímos um valor Maxconnections de 30, o que significa que precisamos ter um bloco de 30 endereços IP não utilizados (incluindo servidores DHCP, se houver) começando com 192.168.233.50 e terminando com 192.168.233.79. Evite sobrepor os endereços IP usados em diferentes configurações de grupo VPN.

LocalIPNet atribui endereços IP a clientes remotos a partir de uma sub-rede que deve ser não utilizada em outro lugar na LAN. Por exemplo, se você especificar o parâmetro "LocalIPNet=182.168.1.0/24" na configuração do grupo VPN, o concentrador atribuirá endereços IP a clientes que começam com 192.168.1.1. Portanto, você precisa atribuir "Maxconnections=254", já que o concentrador não atenderá aos limites de sub-rede ao atribuir números IP usando LocalIPNet.

A palavra-chave Transform especifica os tipos de proteção e os algoritmos que o concentrador usa para sessões de cliente IKE. As opções são as seguintes:

```
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 opção é uma peça de proteção que especifica parâmetros de autenticação e criptografia. Essa palavra-chave pode aparecer várias vezes nesta seção, caso em que o concentrador 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.

ESP(SHA,DES), ESP(SHA,3DES), ESP(MD5,DES) e ESP(MD5,3DES) indicam o cabeçalho de carga de segurança de encapsulamento (ESP) 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 de hash message-digest 5, e 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 instalações. ESP(MD5) e ESP(SHA) usam o cabeçalho ESP para autenticar pacotes sem criptografia. AH(MD5) e AH(SHA) usam o cabeçalho de autenticação (AH) para autenticar pacotes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES) e AH(SHA)+ESP(3DES) usam o Cabeçalho de autenticação para autenticar pacotes e o cabeçalho ESP para criptografar pacotes.

Observação: o software do cliente Mac OS não oferece suporte à opção AH. Você deve especificar pelo menos uma opção ESP se usar o software cliente Mac OS.

O campo IPNet é importante, pois controla para onde os clientes do concentrador podem ir. Os valores inseridos neste campo determinam qual tráfego TCP/IP é encapsulado, ou mais comumente, para onde um cliente que pertence a esse grupo de VPN pode ir na sua rede.

A Cisco recomenda a configuração da rede interna (neste exemplo 192.168.233.0/24), de modo que todo o tráfego de um cliente que vai para a rede interna é enviado através do túnel e, portanto, autenticado e criptografado (se você habilitar a criptografia). Neste cenário, nenhum outro tráfego é encapsulado; em vez disso, é roteado normalmente. Você pode ter várias entradas, incluindo endereços de host ou únicos. O formato é o endereço (em nosso exemplo, o endereço de rede 192.168.233.0) e a máscara associada a esse endereço em bits (/24, que é uma máscara de classe C).

Inicie essa parte da configuração inserindo o comando **configure group basic-user** e responda aos prompts com as informações do sistema. Aqui está um exemplo de toda a sequência de configuração:

```
*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#
```

A próxima etapa é definir o banco de dados do usuário.

Configuração do VPN User

Nesta seção da configuração, você define o banco de dados de usuários da VPN. Cada linha define um usuário VPN junto com a configuração e a senha do grupo VPN desse usuário. As entradas de várias linhas devem ter quebras de linha terminando com uma barra invertida. No entanto, as quebras de linha entre aspas duplas são preservadas.

Quando um cliente VPN inicia uma sessão de túnel, o nome de usuário do cliente é transmitido ao dispositivo. Se o dispositivo encontrar o usuário nesta seção, ele usará as informações na entrada para configurar o túnel. (Você também pode usar um servidor RADIUS para autenticação de

usuários de VPN). Se o dispositivo não encontrar o nome de usuário e você não tiver configurado um servidor RADIUS para executar a autenticação, a sessão de túnel não será aberta e um erro será retornado ao cliente.

Inicie a configuração inserindo o comando **edit config VPN users**. Vamos ver um exemplo que adiciona um usuário chamado "User1" ao 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#
```

A SharedKey deste usuário é "queimada". Todos esses valores de configuração diferenciam maiúsculas e minúsculas; se você configurar "User1", o usuário deverá digitar "User1" no software cliente. Digitar "user1" resulta em uma mensagem de erro de usuário inválida ou não autorizada. Você pode continuar a digitar usuários em vez de sair do editor, mas lembre-se de inserir um período para sair do editor. Se isso não for feito, poderão ocorrer entradas inválidas na configuração.

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 a tecla Enter. Não desligue o concentrador durante o processo de inicialização. Após a reinicialização do concentrador, os usuários podem se conectar usando o software do VPN Client do concentrador.

Para salvar a configuração, insira o comando **save**, da seguinte maneira:

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

Se você estiver conectado ao concentrador 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 desta saída, o concentrador 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