Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenções](#)
[Configuração de conectividade básica](#)
[Porta Ethernet 1](#)
[Rota padrão](#)
[Gateway de IPSec](#)
[Política IKE](#)
[Configuração de grupo de VPN](#)
[Configuração do VPN User](#)
[Finalizando](#)
[Informações Relacionadas](#)

Introdução

Este guia explica a configuração inicial do concentrador do Cisco VPN 5000, especificamente como configurar-lo para conectar à rede usando o IP, e oferece a Conectividade do cliente remoto.

Você pode instalar o concentrador em qualquer uma de duas configurações, segundo onde você o conecta à rede com relação a um Firewall. O concentrador 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 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 a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

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 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 para terminar a configuração. Você pode igualmente gerar um arquivo de configuração em um editor de texto apropriado, e envia-o ao concentrador 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 esta:

```
*[ 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.

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. Evite usar um endereço na mesma rede TCP/IP que o ethernet0, porque isto desabilitará o TCP/IP no concentrador VPN.

Inscreva os **comandos configure ip ethernet 1**, respondendo às alertas com sua informação de sistema. A sequência das alertas deve olhar como esta:

```
*[ 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 a rota padrão.

Rota padrão

Você precisa de configurar uma rota padrão que o concentrador 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. Mais tarde, você configurará 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 esta:

```
*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 de configurar o gateway IPSec.

Gateway de IPSec

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

```
* 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, configurar a política de IKE.

Política IKE

Ajuste os parâmetros do protocolo internet security association key management/intercâmbio de chave de Internet (ISAKMP/IKE) para o concentrador. Estes ajustes controlam como o concentrador e o cliente identificam e se autenticam a fim 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 as sessões de túnel individual de identificador de cliente. Os parâmetros da negociação de IKE da fase 2 para o concentrador VPN e o cliente 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. Esta palavra-chave pode aparecer épocas múltiplas dentro desta seção, neste caso 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 (sumário de mensagem 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.

```
* 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 princípios são configurados, incorpore parâmetros do grupo.

Configuração de grupo de VPN

Ao incorporar parâmetros do grupo, recorde que o nome do grupo VPN não deve conter espaços, mesmo que o parser dos dados da linha de comando permita que você incorpore espaços ao nome do grupo VPN. O nome do grupo VPN pode conter letras, números, traços, e relevos.

Há quatro parâmetros básicos que são exigidos em cada grupo de VPN para a operação IP:

- Maxconnections
- StartIPaddress ou LocalIPNet
- Transforme
- IPNet

O Parâmetro máximo de conexões é o número máximo de sessões cliente simultâneas permitidas nesta configuração de grupo de VPN particular. Mantenha este número na mente, como trabalha conjuntamente com o Endereço IP inicial ou o parâmetro LocalIPNet.

O concentrador VPN atribui endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes remotos por dois esquemas, Endereços IP iniciais e LocalIPNet diferentes. O Endereço IP inicial atribui números IP da sub-rede conectada ao ethernet0 e aos proxys ARP para os clientes conectados. O LocalIPNet atribui números IP aos clientes remotos de uma sub-rede original aos clientes VPN, e exige que o resto da rede está feito ciente da existência da sub-rede VPN com o roteamento estático ou dinâmico. O Endereço IP inicial oferece uma configuração mais fácil, mas pode limitar o tamanho do espaço de endereços. O LocalIPNet oferece a maior flexibilidade do endereçamento para usuários remotos, mas exige levemente mais trabalho configurar o roteamento necessário.

Para o Endereço IP inicial, use o primeiro endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído a uma sessão de túnel do cliente de entrada. Em uma instalação da configuração básica, este deve ser um endereço IP de Um ou Mais Servidores Cisco ICM NT na rede interna TCP/IP (a mesma rede que a porta do ethernet0). Em nosso exemplo abaixo, a primeira sessão cliente é atribuída o endereço de 192.168.233.50, a sessão cliente simultânea seguinte é atribuída 192.168.233.51, e assim por diante. Nós atribuímos um valor de Maxconnections de 30, que significasse que nós precisamos de ter um bloco de 30 endereços IP de Um ou Mais Servidores Cisco ICM NT não utilizados (que incluem servidores DHCP se você tem alguns) que começam com 192.168.233.50 e que terminam com 192.168.233.79. Avoid que sobrepõe os

endereços IP de Um ou Mais Servidores Cisco ICM NT usados em configurações de grupo de VPN diferentes.

O LocalIPNet atribui endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes remotos de uma sub-rede que deva ser não utilizada em outra parte no LAN. Por exemplo, se você especifica o parâmetro "LocalIPNet=182.168.1.0/24" na configuração de grupo de VPN, o concentrador atribui endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes que começam com 192.168.1.1. Consequentemente, você precisa de atribuir "Maxconnections=254", porque o concentrador não observará limites de sub-rede ao atribuir o IP numera usando o LocalIPNet.

A palavra-chave da transformação especifica os tipos de proteção e os algoritmos que o concentrador usa para sessões de cliente IKE. As opções 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#
```

Cada opção é uma parte da proteção que especifique a autenticação e os parâmetros de criptografia. Esta palavra-chave pode aparecer épocas múltiplas dentro desta seção, neste caso o concentrador 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.

O ESP (SHA, DES), ESP(SHA,3DES), ESP(MD5,DES), e ESP(MD5,3DES) denotam o encabeçamento do Encapsulating Security Payload (ESP) 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, e 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 de ESP(MD5) e ESP(SHA) o cabeçalho de ESP autenticar pacotes sem a criptografia. Uso de AH(MD5) e AH(SHA) o Authentication Header (AH) autenticar pacotes. AH(MD5)+ESP(DES), AH(MD5)+ESP(3DES), AH(SHA)+ESP(DES), e AH(SHA)+ESP(3DES) uso o cabeçalho de autenticação autenticar pacotes e o cabeçalho de ESP para cifrar pacotes.

Nota: O software do cliente do Mac OS não apoia a opção AH. Você deve especificar pelo menos uma opção de ESP se você usa o software do cliente do Mac OS.

O campo de IPNet é importante, desde que controla onde os clientes concentrador podem ir. Os valores que você incorpora a este campo determinam que tráfego TCP/IP é escavado um túnel, ou mais comumente, onde um cliente que pertença a este grupo de VPN pode ir em sua rede.

Cisco recomenda configurar a rede interna (neste exemplo 192.168.233.0/24), assim que todo o tráfego de um cliente que vai à rede interna é enviado através do túnel, e autenticado consequentemente e cifrado (se você Enable Encryption). Nesta encenação, nenhum outro tráfego é escavado um túnel; em lugar de, distribuiu normalmente. Você pode ter entradas múltiplas, incluir único ou endereços de host. O formato é o endereço (em nosso exemplo, no endereço de rede 192.168.233.0) e então a máscara associada com esse endereço nos bit (/24, que é uma máscara do C da classe).

Comece isto parte da configuração inscrevendo o **comando configure VPN group basic-user**, e

responda então às alertas com sua informação de sistema. Está aqui um exemplo da sequência da configuração 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#
```

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

Configuração do VPN User

Nesta seção da configuração, você define o banco de dados de usuários do VPN. Cada linha define um usuário VPN junto com a configuração de grupo de VPN e a senha desse usuário. a Multi-linha entradas deve ter a linha rupturas que terminam com um corte traseiro. Contudo, linha rupturas fechadas em uma cotação dobro - as marcas são preservadas.

Quando um cliente VPN começa uma sessão de túnel, o username do cliente está transmitido ao dispositivo. Se o dispositivo encontra o usuário nesta seção, usa a informação na entrada para estabelecer o túnel. (Você pode igualmente usar um servidor Radius para a autenticação de usuários do VPN). Se o dispositivo não encontra o username, e você não configurou um servidor Radius para executar a autenticação, a sessão de túnel não está aberta e um erro é retornado ao cliente.

Comece a configuração inscrevendo o **comando edit config VPN users**. Deixe-nos olhar um exemplo que adicione um usuário nomeado "User1" ao grupo de VPN “básico-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 Chave compartilhada deste usuário “é queimada”. Todos estes valores da configuração são diferenciando maiúsculas e minúsculas; se você configura "User1", o usuário deve incorporar "User1" ao software do cliente. Incorporar "user1" conduz a um Mensagem de Erro inválido ou do usuário não autorizado. Você pode continuar a inscrever usuários em vez de retirar o editor, mas para recordar, você deve incorporar um período para retirar o editor. A falha fazer assim pode causar entradas inválidas na configuração.

Finalizando

Sua última etapa salvar a configuração. Quando perguntado se você é certo que você quer transferir a configuração e reiniciar o dispositivo, o tipo y e pressionar a tecla ENTER. Não desligue o concentrador 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 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 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