Configuring the Cisco VPN 3000 Concentrator to a Cisco Router

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Configurar
Diagrama de Rede
Configurações
Configuração do VPN Concentrator
Verificar
No roteador
No VPN Concentrator
Troubleshooting
No roteador
Problema - Incapaz de iniciar o túnel
PFS
Informações Relacionadas

Introdução

Esta configuração de exemplo mostra como conectar uma rede privada atrás de um roteador que execute o software do ® do Cisco IOS a uma rede privada atrás do Cisco VPN 3000 Concentrator. Os dispositivos nas redes se reconhecem por seus endereços privados.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2611 Router com Cisco IOS Software Release 12.3.(1)a**Note**: Certifique-se de que os Cisco 2600 Series Router estão instalados com uma imagem IOS cripto do IPSec VPN que

apoie a característica VPN.
- Cisco VPN 3000 Concentrator com 4.0.1 B

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Note: Use a ferramenta Command Lookup Tool (apenas para clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede.

Configurações

Este documento usa esta configuração.

Configuração do roteador

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
```

```
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
```

```
!
line con 0
line aux 0
line vty 0 4
!
end
```

Configuração do VPN Concentrator

Nesta configuração de laboratório, o concentrador VPN é alcançado primeiramente através da porta de Console e uma configuração mínima é adicionada de modo que a configuração mais adicional possa ser feita através da interface gráfica de usuário (GUI).

Escolha o **Administração > Reinicialização de Sistema > Programar Reinicialização > Reinicialização com Configuração de Fábrica/Padrão** assegurar-se de que não haja nenhuma configuração existente no concentrador VPN.

O concentrador VPN aparece na configuração rápida, e estes artigos são configurados após a repartição:

- Hora/Data
- Interfaces/Máscaras em Configuration > Interfaces (pública=200.1.1.2/24, privada=192.168.10.1/24)
- Gateway padrão em Configuration > System > IP routing > Default_Gateway (200.1.1.1)

Neste momento, o concentrador VPN é acessível com o HTML da rede interna.

Note: Porque o concentrador VPN é controlado de fora, você igualmente tem que selecionar:

- **Configuração > interfaces > 2-public > filtro IP seleto > 1. privado (padrão)**.
- **Administração > Direitos de Acesso > Lista de Controle de Acesso** > Add Manager Workstation para adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do *gerenciador externo*.

Isto não é necessário a menos que você controlar o concentrador VPN da *parte externa*.

1. Escolha o **configuração > interfaces** verificar novamente as relações depois que você traz acima o GUI.
2. Escolha o > IP Routing > os **gateways padrão do Configuration > System** para configurar o **gateway do padrão** (Internet) e o **gateway do padrão do túnel** (para dentro) para que o IPsec alcance as outras sub-redes na rede privada.
3. Escolha o **Configuration > Policy Management** > Network Lists criar os listes de redes que definem o tráfego a ser cifrado.Estas são as redes local:Estas são as redes remotas:
4. Quando concluídas, estas são as duas listas de rede:**Note**: Se o túnel de IPsec não vem acima, verifique para ver se o tráfego interessante combina em ambos os lados. O tráfego interessante é definido pela lista de acessos no roteador e em caixas PIX. São definidos por listes de redes nos concentradores VPN.
5. Escolha o **Configuration > System** > Tunneling Protocols > **LAN para LAN do IPsec** e defina o túnel de LAN para LAN.
6. Depois que você clique **se aplica**, este indicador está indicado com a outra configuração que é criada automaticamente em consequência da configuração de túnel de Rede-para-Rede.Previamente os parâmetros IPSec LAN-a-LAN criados podem ser vistos ou alterado

no **Configuration > System** > Tunneling Protocols > **LAN para LAN do IPsec**.
7. Escolha o **configuração > sistema > protocolos de tunelamento > IPSEC > propostas de IKE** confirmar a proposta do IKE ativo.
8. Escolha o **Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Associações de Segurança** ver a lista de associações de segurança.
9. Clique o nome de associação de segurança, e clique-o então **alteram** para verificar as associações de segurança.

Verificar

Esta seção alista os **comandos show** usados nesta configuração.

No roteador

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- show crypto ipsec sa – Mostra as configurações usadas pelas associações segurança atuais.
- **mostre isakmp cripto sa** — Mostra todas as associações atuais da segurança do intercâmbio chave de Internet em um par.
- **show crypto engine connection ative** — Mostra as conexões de sessão de criptografia ativas atuais para todas as crypto-engines.

Você pode usar a ferramenta de pesquisa do comando IOS (clientes registrados somente) para ver mais informação sobre comandos específicos.

No VPN Concentrator

Escolha o **Configuração > Sistema > Eventos > Classes > Modificar** girar sobre o registro. Estas opções estão disponíveis:

- IKE
- IKEDBG
- IKEDECODE
- IPSEC
- IPSECDBG
- IPSECDECODE

Gravidade para registro = 1-13

Severidade para console = 1-3

Selecione a **monitoração** > o **log de eventos** para recuperar o log de eventos.

Troubleshooting

No roteador

Refira a informação importante em comandos Debug antes que você tente todos os comandos debug.

- debug crypto engine — Exibe o tráfego que está criptografado.
- **IPsec do debug crypto** — Indica as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Indica as negociações de ISAKMP de fase 1.

Problema - Incapaz de iniciar o túnel

Mensagem de erro

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask 255.255.255.0
ip nat inside source route-map nonat pool mypool overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255 192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

Solução

Termine esta ação a fim configurar o número desejado de inícios de uma sessão simultâneos ou ajustar os inícios de uma sessão simultâneos a 5 para este SA:

Vá ao **configuration > user management > aos grupos > Modify 10.19.187.229 > general > inícios de uma sessão de Simultaneouts** e mude o número de inícios de uma sessão ao 5.

PFS

Nas negociações de IPsec, o Perfect Forward Secrecy (PFS) garante que cada nova chave criptográfica não tenha relação com nenhuma chave anterior. Permita ou desabilite o PFS em ambos os tunnel peer. Se não, o túnel de IPsec do LAN para LAN (L2L) não é estabelecido no Roteadores.

A fim especificar que o IPsec deve pedir o PFS quando as associações de segurança novas são pedidas para esta entrada do crypto map, ou que o IPsec exige o PFS quando receber pedidos para associações de segurança novas, usa o **comando set pfs no** modo de configuração do crypto map. A fim especificar que o IPsec não deve pedir o PFS, não use **nenhum** formulário deste comando.

```
set pfs [group1 | group2]
no set pfs
```

Para o comando set pfs:

- *grupo1* — Especifica que o IPsec deve usar o grupo do módulo da prima de Diffie-Hellman do 768-bit quando o intercâmbio Diffie-Hellman novo for executado.

- *grupo2* — Especifica que o IPsec deve usar o grupo do módulo da prima 1024-bit Diffie-Hellman quando o intercâmbio Diffie-Hellman novo for executado.

Por padrão, o PFS não é solicitado. Se nenhum grupo for especificado com este comando, group1 será usado como o padrão.

Exemplo:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

Refira a referência de comandos do Cisco IOS Security para obter mais informações sobre do **comando set pfs**.

Informações Relacionadas

- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Cisco VPN 3000 Series Concentrators
- Cisco VPN 3002 Hardware Clients
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems