Roteador e cliente VPN para Internet públicas em um exemplo de configuração da vara

Índice

Introdução

Este documento descreve como estabelecer um roteador de site central para executar o tráfego de IPSec em uma vara. Esta instalação aplica-se a um caso específico onde o roteador, sem permitir o Split Tunneling, e os usuários móveis (Cisco VPN Client) possam alcançar o Internet através do roteador de site central. A fim conseguir isto, configurar o mapa de política no roteador para apontar todo o tráfego VPN (Cisco VPN Client) a uma interface de loopback. Isto permite que o tráfego do Internet seja endereço de porta traduzido (PATed) ao mundo exterior.

Refira PIX/ASA 7.x e cliente VPN para os Internet públicas VPN em um exemplo de configuração da vara a fim terminar uma configuração similar em um PIX Firewall da instalação central.

Nota: A fim evitar a sobreposição dos endereços IP de Um ou Mais Servidores Cisco ICM NT na rede, atribua o pool totalmente diferente dos endereços IP de Um ou Mais Servidores Cisco ICM NT ao cliente VPN (por exemplo, 10.x.x.x, 172.16.x.x, 192.168.x.x). Este esquema de endereçamento de IP ajuda-o a pesquisar defeitos sua rede.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Roteador Cisco 3640 com Software Release 12.4 de Cisco IOS®
- Cisco VPN Client 4.8

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.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Configurações

Este documento utiliza as seguintes configurações:

- Router
- Cisco VPN Client

Router

```
 VPN#show run Building configuration... Current
configuration : 2170 bytes ! version 12.4 service
timestamps debug datetime msec service timestamps log
datetime msec no service password-encryption ! hostname
VPN ! boot-start-marker boot-end-marker ! ! !--- Enable
authentication, authorization and accounting (AAA) !---
for user authentication and group authorization. aaa
new-model ! !--- In order to enable Xauth for user
authentication, !--- enable the aaa authentication
commands. aaa authentication login userauthen local !---
```

```
In order to enable group authorization, enable !--- the aaa authorization commands. aaa authorization network groupauthor local ! aaa session-id common ! resource policy ! ! !--- For local authentication of the IPsec user, !--- create the user with a password. username user password 0 cisco ! ! !--- Create an Internet Security Association and !--- Key Management Protocol (ISAKMP) policy for Phase 1 negotiations. crypto isakmp policy 3 encr 3des authentication pre-share group 2 !--- Create a group that is used to specify the !--- WINS and DNS server addresses to the VPN Client, !--- along with the pre-shared key for authentication. crypto isakmp client configuration group vpnclient key cisco123 dns 10.10.10.10 wins 10.10.10.20 domain cisco.com pool ippool ! !--- Create the Phase 2 Policy for actual data encryption. crypto ipsec transform-set myset esp-3des esp-md5-hmac ! !--- Create a dynamic map and apply !--- the transform set that was created earlier. crypto dynamic-map dynmap 10 set transform-set myset reverse-route ! !--- Create the actual crypto map, !--- and apply the AAA lists that were created earlier. crypto map clientmap client authentication list userauthen crypto map clientmap isakmp authorization list groupauthor crypto map clientmap client configuration address respond crypto map clientmap 10 ipsec-isakmp dynamic dynmap ! ! ! ! !--- Create the loopback interface for the VPN user traffic . interface Loopback0 ip address 10.11.0.1 255.255.255.0 ip nat inside ip virtual-reassembly ! interface Ethernet0/0 ip address 10.10.10.1 255.255.255.0 half-duplex ip nat inside !--- Apply the crypto map on the interface. interface FastEthernet1/0 ip address 172.16.1.1 255.255.255.0 ip nat outside ip virtual-reassembly ip policy route-map VPN-Client duplex auto speed auto crypto map clientmap ! interface Serial2/0 no ip address ! interface Serial2/1 no ip address shutdown ! interface Serial2/2 no ip address shutdown ! interface Serial2/3 no ip address shutdown !--- Create a pool of addresses to be !--- assigned to the VPN Clients. ! ip local pool ippool 192.168.1.1 192.168.1.2 ip http server no ip http secure-server ! ip route 10.0.0.0 255.255.255.0 172.16.1.2 !--- Enables Network Address Translation (NAT) !--- of the inside source address that matches access list 101 !--- and gets PATed with the FastEthernet IP address. ip nat inside source list 101 interface FastEthernet1/0 overload ! !--- The access list is used to specify which traffic is to be translated for the !--- outside Internet. access-list 101 permit ip any any !--- Interesting traffic used for policy route. access-list 144 permit ip 192.168.1.0 0.0.0.255 any !--- Configures the route map to match the interesting traffic (access list 144) !--- and routes the traffic to next hop address 10.11.0.2. ! route-map VPN-Client permit 10 match ip address 144 set ip next-hop 10.11.0.2 ! ! control-plane ! line con 0 line aux 0 line vty 0 4 ! end
```

Configuração do cliente VPN 4.8

Termine estas etapas a fim configurar o cliente VPN 4.8.

1. Escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN**.

2. Clique **novo** a fim lançar a janela de entrada nova da conexão de VPN da criação.
3. Dê entrada com o nome da entrada de conexão junto com uma descrição, incorpore o endereço IP externo do roteador à caixa do host, e incorpore o nome do grupo VPN e a senha. Clique em Salvar.
4. Clique sobre a conexão que você gostaria de se usar e o clique **conecta da** janela principal do cliente VPN.
5. Quando alertado, incorpore a informação do nome de usuário e senha para o Xauth e clique a **APROVAÇÃO** a fim conectar à rede remota.
6. O cliente VPN obtém conectado com o roteador na instalação central.
7. Escolha o **estado > as estatísticas** a fim verificar as estatísticas do túnel do cliente VPN.

Verificar

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 isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.`VPN#show crypto ipsec sa interface: FastEthernet1/0 Crypto map tag: clientmap, local addr 172.16.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer 10.0.0.2 port 500 PERMIT, flags={} #pkts encaps: 270, #pkts encrypt: 270, #pkts digest: 270 #pkts decaps: 270, #pkts decrypt: 270, #pkts verify: 270 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.0.0.2 path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet1/0 current outbound spi: 0xEF7C20EA(4017889514) inbound esp sas: spi: 0x17E0CBEC(400608236) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: SW:1, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530341/3288) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xEF7C20EA(4017889514) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: SW:2, crypto map: clientmap sa timing: remaining key lifetime (k/sec): (4530354/3287) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:`
- **mostre IPsec cripto sa** — Mostra os ajustes usados por SA atuais.`VPN#show crypto isakmp sa dst src state conn-id slot status 172.16.1.1 10.0.0.2 QM_IDLE 15 0 ACTIVE`

Troubleshooting

Comandos para Troubleshooting

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.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **IPsec do debug crypto** — Indica as negociações de IPSEC de fase 2.
- debug crypto isakmp — Exibe as negociações ISAKMP da Fase 1.

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Cisco VPN Client - Sustentação do produto
- Roteador Cisco - Sustentação do produto
- Suporte Técnico e Documentação - Cisco Systems