PIX 6.x: Passagem de túnel IPsec através de um PIX Firewall com uso de lista de acesso e com exemplo de configuração de NAT

Contents

Introduction

Este documento fornece uma configuração de exemplo para um túnel de IPsec através de firewall que executa a tradução de endereço de rede (NAT). **Esta configuração não funciona com a PAT (Port Address Translation, tradução de endereço de porta) se você usar as versões do software Cisco IOS® anteriores e não incluindo a versão 12.2(13)T.** Esse tipo de configuração pode ser usado para fazer o túnel do tráfego IP. Isto não pode ser usado para criptografar o tráfego que não passa por um firewall, como IPX ou atualizações de roteamento. O tunelamento de Generic Routing Encapsulation (GRE) é apropriado para este tipo de configuração. No exemplo neste documento, os Cisco 2621 e 3660 Routers são os pontos de extremidade de túnel de IPSec que se unem a duas redes privadas, com conduítes ou listas de controle de acesso (ACLs) entre o PIX para permitir um tráfego de IPSec.

Observação: o NAT é uma tradução de endereço um para um, não deve ser confundido com o PAT, que é uma tradução muitos (dentro do firewall) para um. Consulte Verificando a Operação de NAT e Troubleshooting Básico de NAT ou Como o NAT funciona para obter mais informações sobre a operação e a configuração do NAT.

Observação: o IPSec com PAT pode não funcionar corretamente porque o dispositivo de endpoint de túnel externo não pode lidar com vários túneis de um endereço IP. Você precisa entrar em contato com seu fornecedor para determinar se os dispositivos de endpoint de túnel funcionam com PAT. Além disso, nas versões 12.2(13)T e posterior, o recurso NAT Transparency também pode ser usado para PAT. Consulte IPSec NAT Transparency para obter mais informações.

Consulte Suporte para IPSec ESP Através de NAT para obter mais informações sobre esses recursos nas versões 12.2(13)T e posteriores. Além disso, antes de abrir um caso no TAC, consulte Perguntas frequentes sobre NAT, que tem muitas respostas para perguntas comuns.

Consulte Passagem de Túnel IPsec através de um Aparelho de Segurança com o uso de Lista de Acesso e MPF com Exemplo de Configuração de NAT para obter mais informações sobre como configurar um túnel IPSec através de um firewall com NAT no PIX/ASA versão 7.x.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Cisco IOS versão 12.0.7.T [até, mas não incluindo, 12.2(13)T]Consulte IPSec NAT Transparency para obter versões mais recentes.
- Roteador Cisco 2621 que executa o Software Cisco IOS versão 12.4
- Roteador Cisco 3660 que executa o Software Cisco IOS versão 12.4
- Cisco PIX Firewall com 6.x

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

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

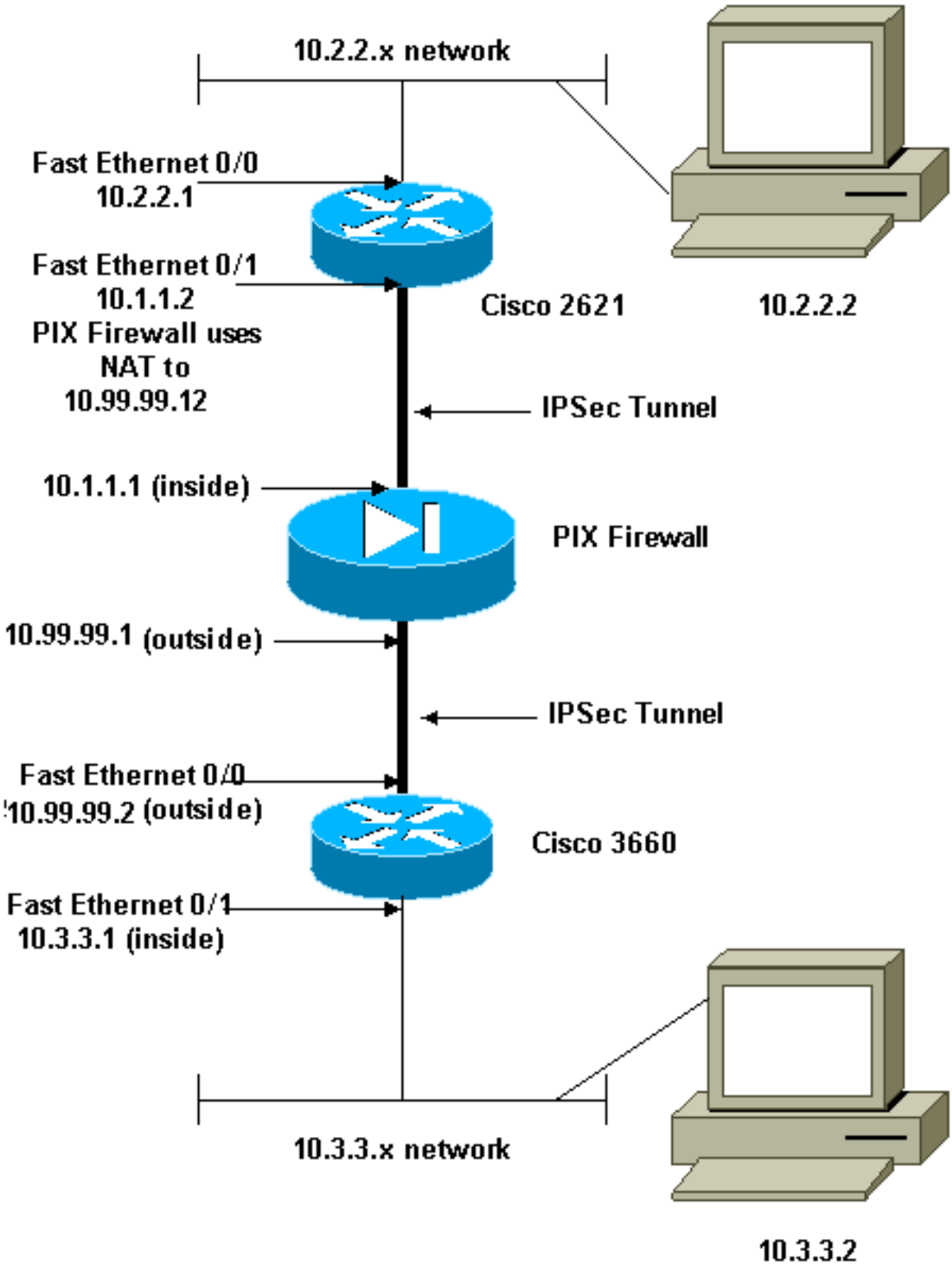
Configurar

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 neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. Esses são endereços RFC 1918 que foram usados em um ambiente de laboratório.

Configurações

Este documento utiliza as seguintes configurações:

- Configuração do Cisco 2621
- Configuração parcial do Cisco PIX Firewall

- Configuração do Cisco 3660

Configuração do Cisco 2621

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.2
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/1
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
```

```
 end
```

Configuração parcial do Cisco PIX Firewall

```
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
!--- The fixup protocol esp-ike command is disabled by
default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
 ip address inside 10.1.1.1 255.255.255.0
 !--- Range of registered IP addresses for use. global
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. nat (inside) 1 0.0.0.0 0.0.0.0 0 0
 static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0

 !--- or access-list acl-out permit esp host 10.99.99.2
host 10.99.99.12
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
!--- It is important to permit UDP port 4500 for NAT-T
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

Observação: o comando **fixup protocol esp-ike** é desabilitado por padrão. Se um comando **fixup protocol esp-ike** for emitido, o fixup será ativado e o PIX Firewall preservará a porta de origem do Internet Key Exchange (IKE). Também cria uma tradução PAT para o tráfego ESP. Além disso, se o fixup do tipo esp estiver ativado, o ISAKMP (Internet Security Association and Key Management Protocol) não poderá ser ativado em nenhuma interface.

Configuração do Cisco 3660

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
```

```
 !
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.12
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/0
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.12
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 interface FastEthernet0/0
  ip address 10.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
 !
 interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
 !
 interface Ethernet3/1
  no ip address
  no ip directed-broadcast
 interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
 !
 !--- Pool from which inside hosts translate to !--- the
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
 !--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
 ip classless
```

```
 ip route 0.0.0.0 0.0.0.0 10.99.99.1
 no ip http server
 !
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 !--- Except the private network from the NAT process.
access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
 access-list 110 permit ip 10.3.3.0 0.0.0.255 any
 route-map nonat permit 10
  match ip address 110
 !
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 end
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

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

- **show crypto ipsec sa** — Mostra as associações de segurança da fase 2.
- **show crypto isakmp sa** — Mostra as associações de segurança da fase 1.
- **show crypto engine connections ative** —Use para ver os pacotes criptografados e descriptografados.

Troubleshoot

Use esta seção para resolver problemas de configuração.

Comandos para Troubleshooting

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

- **debug crypto engine** —Mostra o tráfego que está criptografado.
- **debug crypto ipsec** —Use para ver as negociações de IPSec da fase 2.
- **debug crypto isakmp** — Use para ver as negociações ISAKMP da fase 1.

Limpando associações de segurança

- **clear crypto isakmp** — Limpa associações de segurança IKE.
- **clear crypto ipsec sa** — Limpa associações de segurança IPSec.

Informações Relacionadas

- Cisco PIX 500 Series Security Appliances
- Referências do comando Cisco Secure PIX Firewall
- Página de suporte de NAT
- Solicitação de comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems