PIX 6.x: Passagem do túnel de IPsec com um PIX Firewall com uso da lista de acessos e com exemplo da configuração de NAT

Índice

Introdução

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 trabalha com tradução de endereço de porta (PAT) se você usa software release de Cisco IOS® antes de e não incluindo 12.2(13)T.** Este tipo de configuração pode ser usado para escavar um túnel o 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.

Nota: O NAT é uma tradução de endereço de um para um, para não ser confundido com a PANCADINHA, que é umas muitas (dentro do Firewall) - -um à tradução. Refira a verificação da operação de NAT e do Troubleshooting de NAT básico ou como o NAT trabalha para obter mais informações sobre da operação de NAT e da configuração.

Nota: O IPsec com PANCADINHA não pôde trabalhar corretamente porque o dispositivo de ponto final de túnel exterior não pode segurar túneis múltiplos de um endereço IP de Um ou Mais Servidores Cisco ICM NT. Você precisa de contactar seu vendedor para determinar se os dispositivos de ponto final de túnel funcionam com PANCADINHA. Adicionalmente, nas versões 12.2(13)T e mais recente, a característica da transparência de NAT pode igualmente ser usada

para a PANCADINHA. Refira a transparência de NAT de IPSec para mais informação. Refira o apoio para o IPsec ESP com o NAT para obter mais informações sobre destas características nas versões 12.2(13)T e mais recente. Igualmente, antes que você abra um caso com TAC, refira perguntas mais frequentes de NAT, que tem muitas respostas às perguntas comum.

Refira a passagem do túnel de IPsec com uma ferramenta de segurança com uso da lista de acessos e o MPF com exemplo da configuração de NAT para obter mais informações sobre de como configurar um túnel de IPsec com um Firewall com o NAT na versão 7.x PIX/ASA.

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 IOS Software Release12.0.7.T [até mas não incluindo 12.2(13)T]Refira a transparência de NAT de IPSec para mais versões recentes.
- Cisco 2621 Router que executa o Cisco IOS Software Release 12.4
- Cisco 3660 Router que executa o Cisco IOS Software Release 12.4
- Cisco PIX Firewall que executa 6.x

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.

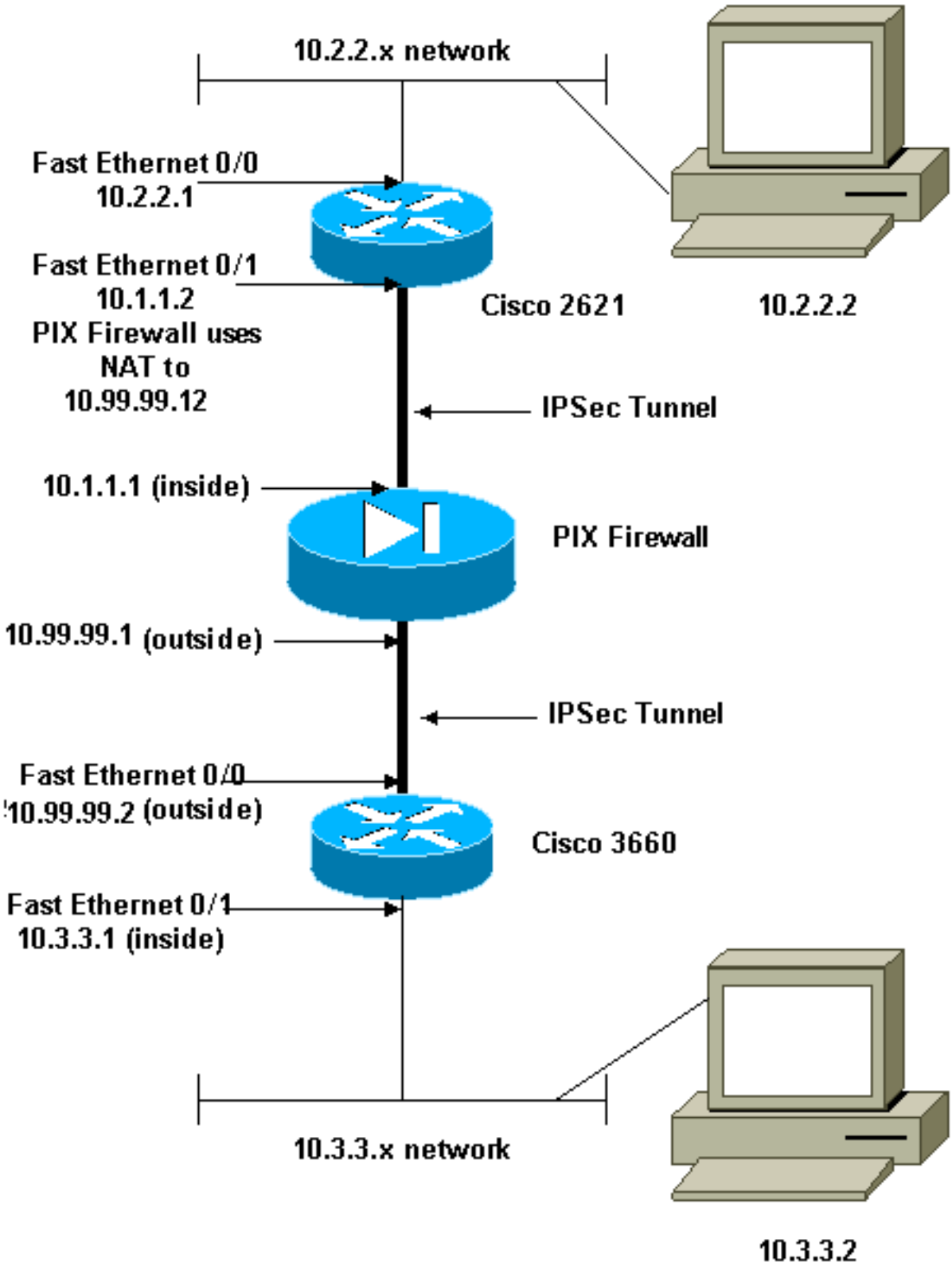
Configurar

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

Nota: Use a 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:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. Estes são os endereços do 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
```

Nota: O comando do **fixup protocol ESP-IKE** é desabilitado à revelia. Se um comando do **fixup protocol ESP-IKE** é emitido, o reparar está girado sobre, e o PIX Firewall preserva a porta de origem do Internet Key Exchange (IKE). Igualmente cria uma tradução da PANCADINHA para o tráfego ESP. Adicionalmente, se o reparar ESP-IKE está ligada, o Internet Security Association and Key Management Protocol (ISAKMP) não pode ser permitido em nenhuma relação.

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 (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 associações de segurança da fase 2.
- show crypto isakmp sa - Mostra as associações de segurança da fase 1.
- **active do show crypto engine connections** — Use para ver os pacotes criptografado e decriptografado.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Comandos para Troubleshooting

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

- **motor do debug crypto** — Mostra o tráfego que é cifrado.
- **IPsec do debug crypto** — Use para ver as negociações de IPSEC de fase 2.
- **isakmp do debug crypto** — Use para ver as negociações de ISAKMP de fase 1.

Limpando associações de segurança

- **cancele o isakmp cripto** — Associações de segurança dos espaços livres IKE.
- clear crypto ipsec sa - Limpa as associações de segurança do IPSec

Informações Relacionadas

- Cisco PIX 500 Series Security Appliances

- Referências do comando Cisco Secure PIX Firewall
- Página de suporte de NAT
- Request For Comments (RFC)
- Suporte Técnico e Documentação - Cisco Systems