

Túnel do IPSec VPN PIX/ASA (versão 7.x e mais recente) com exemplo de configuração da tradução de endereço de rede

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Produtos Relacionados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Ferramenta de segurança e configuração de lista de acesso PIX](#)

[Ferramenta de segurança PIX e configuração MPF \(estrutura de política modular\)](#)

[Verificar](#)

[Troubleshooting](#)

[Comandos de Troubleshooting para o IPSec de roteador](#)

[Limpendo associações de segurança](#)

[Comandos de Troubleshooting para o PIX](#)

[Informações Relacionadas](#)

Introdução

Esta configuração de exemplo demonstra um túnel do IPSec VPN por um 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® mais cedo do que e não incluindo 12.2(13)T.** O este tipo de configuração pode ser usado para escavar um túnel o tráfego IP. Esta configuração não pode ser usada para cifrar o tráfego que não atravessa um Firewall, tal como o IPX ou as atualizações de roteamento. A escavação de um túnel do Generic Routing Encapsulation (GRE) é uma escolha mais apropriada. Neste exemplo, os Cisco 2621 e 3660 Router são os pontos finais de túnel de IPSec que se juntam a duas redes privadas, com conduítes ou Access Control Lists (ACLs) no PIX in-between a fim permitir o 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. Para obter mais informações sobre da operação de NAT e da configuração, refira a [verificação da operação de NAT e do Troubleshooting de NAT básico](#) ou [como o NAT trabalha](#).

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. Contacte seu vendedor a fim determinar se os dispositivos de ponto final de túnel funcionam com PANCADINHA. Adicionalmente, no Cisco IOS Software Release 12.2(13)T e Mais Recente, a característica da transparência de NAT pode ser usada para a PANCADINHA. Para mais detalhes, refira a [transparência de NAT de IPsec](#). Refira o [apoio para o IPsec ESP com o NAT](#) a fim aprender mais sobre estas características no Cisco IOS Software Release 12.2(13)T e Mais Recente.

Nota: Antes que você abra um caso com Suporte técnico de Cisco, refira [perguntas mais frequentes de NAT](#), que tem muitas respostas às perguntas comum.

Refira [configurar um túnel de IPsec com um Firewall com o NAT](#) para obter mais informações sobre de como configurar o túnel de IPsec com o Firewall com o NAT na versão de PIX 6.x e mais cedo.

[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 Release 12.0.7.T (até mas não incluindo o Cisco IOS Software Release 12.2(13)T)Para mais versões recentes, refira a [transparência de NAT de IPsec](#).
- Cisco 2621 Router
- Cisco 3660 Router
- Ferramenta de segurança da série do Cisco PIX 500 que executa 7.x e acima.

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.

[Produtos Relacionados](#)

Este documento pode igualmente ser usado com a ferramenta de segurança adaptável do Cisco 5500 Series (ASA) com versão de software 7.x e mais tarde.

[Configurar](#)

Esta seção apresenta-o com a informação que você pode se usar para configurar as

características este documento descreve.

Nota: A fim encontrar a informação adicional nos comandos que este documento usa, usa a [ferramenta de consulta de comandos \(clientes registrados somente\)](#).

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:

[Configurações](#)

Este documento utiliza as seguintes configurações:

- [Configuração do Cisco 2621](#)
- [Configuração do Cisco 3660](#)
- [Ferramenta de segurança e configuração de lista de acesso PIXConfiguração do gerenciador de dispositivo GUI da segurança avançada \(ASDM\)Configuração do comando line interface\(cli\)](#)
- [Ferramenta de segurança PIX e configuração MPF \(estrutura de política modular\)](#)

Cisco 2621

```
Current configuration:
!
version 12.0
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
!
!--- The IKE policy. crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco123
address 99.99.99.2 ! 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 99.99.99.2 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 the 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
```

Cisco 3660

```
version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
 !

!--- The IKE policy. crypto isakmp policy 10 hash md5
authentication pre-share crypto isakmp key cisco123
address 99.99.99.12 ! crypto ipsec transform-set myset
esp-des esp-md5-hmac ! crypto map mymap local-address
FastEthernet0/0 !--- The IPsec policy. crypto map mymap
10 ipsec-isakmp set peer 99.99.99.12 set transform-set
myset !--- Include the private-network-to-private-
network traffic !--- in the encryption process. match
address 101 ! interface FastEthernet0/0 ip address
99.99.99.2 255.255.255.0 no ip directed-broadcast ip nat
outside duplex auto speed auto !--- Apply to the
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 ! !--- The pool from which inside hosts translate to
!--- the globally unique 99.99.99.0/24 network. ip nat
pool OUTSIDE 99.99.99.70 99.99.99.80 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 99.99.99.1
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
```

[Ferramenta de segurança e configuração de lista de acesso PIX](#)

[Configuração ASDM 5.0](#)

Termine estas etapas a fim configurar a versão 7.0 do PIX Firewall usando o ASDM.

1. Console no PIX. De uma configuração esclarecida, use as alertas interativas para permitir o gerenciador de dispositivo GUI da segurança avançada (ASDM) para o Gerenciamento do PIX da estação de trabalho 10.1.1.3.

2. Da estação de trabalho 10.1.1.3, abra um navegador da Web e use o ASDM (neste exemplo, <https://10.1.1.1>).
3. Escolha **sim nas** alertas e no início de uma sessão do certificado com a senha da possibilidade como configurado na [configuração construída a mão ASDM do PIX Firewall](#).
4. Se isto é a primeira vez o ASDM está executado no PC, alerta-o se usar a launcher ASDM, ou usar o ASDM como um App das Javas. Neste exemplo, a launcher ASDM é selecionada e instala estas alertas.
5. Continue à janela ASDM Home e selecione o guia de configuração.
6. Destaque a **relação do ethernet0** e o clique **edita** a fim configurar a interface externa.
7. **APROVAÇÃO** do clique na alerta da relação da edição.
8. Incorpore os detalhes da relação e clique a **APROVAÇÃO** quando você é feito.
9. Clique a **APROVAÇÃO em** mudar uma alerta da relação.
10. O clique **aplica-se** a fim aceitar a configuração da interface. A configuração igualmente obtém empurrada no PIX. Este exemplo usa rotas estáticas.
11. Clique o **roteamento** sob as características aba, destaque a **rota estática**, e o clique **adiciona**.
12. Configurar o gateway padrão e clique a **APROVAÇÃO**.
13. O clique **adiciona** e adiciona as rotas às redes internas.
14. Confirme que as rotas corretas estão configuradas e o clique **se aplica**.
15. Neste exemplo, o NAT é usado. Remova a verificação na caixa para o **tráfego Enable com o Firewall sem a tradução de endereços** e o clique **adiciona** a fim configurar a regra NAT.
16. Configurar a rede da fonte (este exemplo usa). Clique então **controlam associações** a fim definir a PANCADINHA.
17. Selecione a **interface externa** e o clique **adiciona**. Este exemplo usa uma PANCADINHA usando o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação.
18. **APROVAÇÃO** do clique quando a PANCADINHA for configurada.
19. O clique **adiciona** a fim configurar a tradução estática.
20. Selecione o **interior na** gota-para baixo da relação, a seguir incorpore o endereço IP 10.1.1.2, máscara de sub-rede **255.255.255.255**, escolha a **estática** e no endereço exterior **99.99.99.12** do tipo de campo do endereço IP de Um ou Mais Servidores Cisco ICM NT. Clique a **APROVAÇÃO** quando você é feito.
21. O clique **aplica-se** para aceitar a configuração da interface. A configuração igualmente obtém empurrada no PIX.
22. Selecione a **política de segurança** sob a aba das características a fim configurar a regra da política de segurança.
23. O clique **adiciona** para permitir que esp a **APROVAÇÃO do** tráfego e do clique a fim continuar.
24. O clique **adiciona** a fim permitir que o tráfego ISAKMP e a **APROVAÇÃO do** clique a fim continuar.
25. O clique **adiciona** a fim permitir que o tráfego da porta 4500 UDP para o NAT-T e a **APROVAÇÃO do** clique a fim continuar.
26. O clique **aplica-se** a fim aceitar a configuração da interface. A configuração igualmente obtém empurrada no PIX.
27. A configuração está agora completa. Escolha **configuração running do arquivo > da mostra na nova janela** a fim ver a configuração de CLI.

Firewall de PIX

```
pixfirewall# show run : Saved : PIX Version 7.0(0)102
names ! interface Ethernet0 nameif outside security-
level 0 ip address 99.99.99.1 255.255.255.0 ! interface
Ethernet1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ! enable password
2KFQnbNIdI.2KYOU encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pixfirewall domain-name cisco.com ftp
mode passive access-list outside_access_in remark Access
Rule to Allow ESP traffic access-list outside_access_in
extended permit esp host 99.99.99.2 host 99.99.99.12
access-list outside_access_in remark Access Rule to
allow ISAKMP to host 99.99.99.12 access-list
outside_access_in extended permit udp host 99.99.99.2 eq
isakmp host 99.99.99.12 access-list outside_access_in
remark Access Rule to allow port 4500 (NAT-T) to host
99.99.99.12 access-list outside_access_in extended
permit udp host 99.99.99.2 eq 4500 host 99.99.99.12
pager lines 24 mtu inside 1500 mtu outside 1500 no
failover monitor-interface inside monitor-interface
outside asdm image flash:/asdmfile.50073 no asdm history
enable arp timeout 14400 nat-control global (outside) 1
interface nat (inside) 0 0.0.0.0 0.0.0.0 static
(inside,outside) 99.99.99.12 10.1.1.2 netmask
255.255.255.255 access-group outside_access_in in
interface outside route inside 10.2.2.0 255.255.255.0
10.1.1.2 1 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00 h323
0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
http server enable http 10.1.1.3 255.255.255.255 inside
no snmp-server location no snmp-server contact snmp-
server enable traps snmp telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic !! policy-map
asa_global_fw_policy class inspection_default inspect
dns maximum-length 512 inspect ftp inspect h323 h225
inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy asa_global_fw_policy global
Cryptochecksum:0a12956036ce4e7a97f351cde61fba7e : end
```

[Ferramenta de segurança PIX e configuração MPF \(estrutura de política modular\)](#)

Em vez da lista de acessos, use o comando **inspect IPsec-passagem-através em MPF** (estrutura de política modular) a fim passar o tráfego de IPsec através das ferramentas de segurança PIX/ASA.

Esta inspeção é configurada para abrir furo de pino para o tráfego ESP. Todos os fluxos de dados ESP estão permitidos quando um fluxo dianteiro existe, e não há nenhum limite no número máximo de conexão que pode ser permitido. O AH não é permitido. O default idle timeout para fluxos de dados ESP à revelia é ajustado aos minutos 10. Esta inspeção pode ser aplicada em todos os lugar que outras inspeções podem ser aplicadas, que inclui modos da classe e de comando match. A passagem do IPsec com a inspeção de aplicativo fornece o traversal conveniente do tráfego ESP (50 pés do protocolo IP) associado com uma conexão da porta 500 IKE UDP. Evita a configuração de lista de acesso longa para permitir o tráfego ESP e igualmente fornece a Segurança o intervalo e as conexões máximas. Use o **mapa de classe**, o **mapa de**

política, e os comandos **service-policy** a fim definir uma classe de tráfego, aplicar o comando **inspect** à classe, e aplicar a política a umas ou várias relações. Quando permitida, a **inspeção IPsec-passagem-através** do comando permite tráfego ilimitado ESP com um intervalo dos minutos 10, que não seja configurável. O tráfego NAT e NON-NAT é permitido.

```
hostname(config)#access-list test-udp-acl extended permit udp any any eq 500
hostname(config)#class-map test-udp-class hostname(config-cmap)#match access-list test-udp-acl
hostname(config)#policy-map test-udp-policy hostname(config-pmap)#class test-udp-class
hostname(config-pmap-c)#inspect ipsec-pass-thru hostname(config)#service-policy test-udp-policy
interface outside
```

Verificar

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

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite 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** — Mostra os pacotes criptografado e decriptografado.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos de Troubleshooting para o IPsec de roteador

Nota: Consulte [Informações Importantes sobre Comandos de Debugação](#) antes de usar 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 do Internet Security Association and Key Management Protocol (ISAKMP) da fase 1.

Limpendo associações de segurança

- **clear crypto isakmp** - Limpa as associações de segurança do IKE (Intercâmbio de chave de Internet).
- **clear crypto ipsec sa** — Associações de segurança IPsec dos espaços livres.

Comandos de Troubleshooting para o PIX

A [Output Interpreter Tool \(somente clientes registrados\)](#) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- logging buffer debugging - Mostra as conexões estabelecidas e negadas aos hosts que passam pelo PIX. A informação é armazenada no buffer de registro PIX e a saída pode ser considerada usar o **comando show log**.
 - O ASDM pode ser usado para permitir o registro e para ver igualmente os logs segundo as indicações destas etapas.
1. Escolha a **configuração > as propriedades > instalação de registro > de registro > permitem o registro** e clicam-no então **aplicam-se**.
 2. Escolha a **monitoração > registrando > buffer de registro > no nível de registro > no logging buffer**, a seguir clique a **vista**. Este é um exemplo do buffer de registro.

Informações Relacionadas

- [Página de Suporte de Negociação IPSec/Protocolos IKE](#)
- [Página de suporte do PIX](#)
- [Referências de comando PIX](#)
- [Página de suporte de NAT](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)