

Exemplo de configuração de túnel IPsec entre PIX 7.x e VPN 3000 Concentrator

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configure o PIX](#)

[Configurar o VPN 3000 Concentrator](#)

[Verificar](#)

[Verificar o PIX](#)

[Verifique o VPN 3000 Concentrator](#)

[Troubleshoot](#)

[Solucionar problemas do PIX](#)

[Solucionar problemas do VPN 3000 Concentrator](#)

[PFS](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento fornece uma configuração de exemplo de como estabelecer um túnel de VPN IPsec LAN a LAN entre um PIX Firewall 7.x e um Cisco VPN 3000 Concentrator.

Consulte o [Exemplo de Configuração de PIX/ASA 7.x Enhanced Spoke-to-Client VPN com Autenticação TACACS+](#) para saber mais sobre o cenário em que o túnel de LAN para LAN entre os PIXes também permite que um VPN Client acesse o PIX do spoke através do PIX do hub.

Consulte o [PIX/ASA 7.x Security Appliance para um Exemplo de Configuração de Túnel IPsec LAN a LAN de um Roteador IOS](#) para saber mais sobre o cenário em que o túnel LAN a LAN entre o PIX/ASA e um Roteador IOS.

[Prerequisites](#)

[Requirements](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Este documento requer uma compreensão básica do protocolo de IPSec. Consulte [Uma Introdução à Criptografia IPsec](#) para saber mais sobre o IPsec.

Componentes Utilizados

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

- Cisco PIX 500 Series Security Appliance com versão de software 7.1(1)
- Cisco VPN 3060 Concentrator com versão de software 4.7.2(B)

Observação: o PIX 506/506E não suporta 7.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.

Para configurar o PIX 6.x, consulte o [Túnel IPSec LAN a LAN entre o Cisco VPN 3000 Concentrator e o PIX Firewall Configuration Example](#).

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Configurar

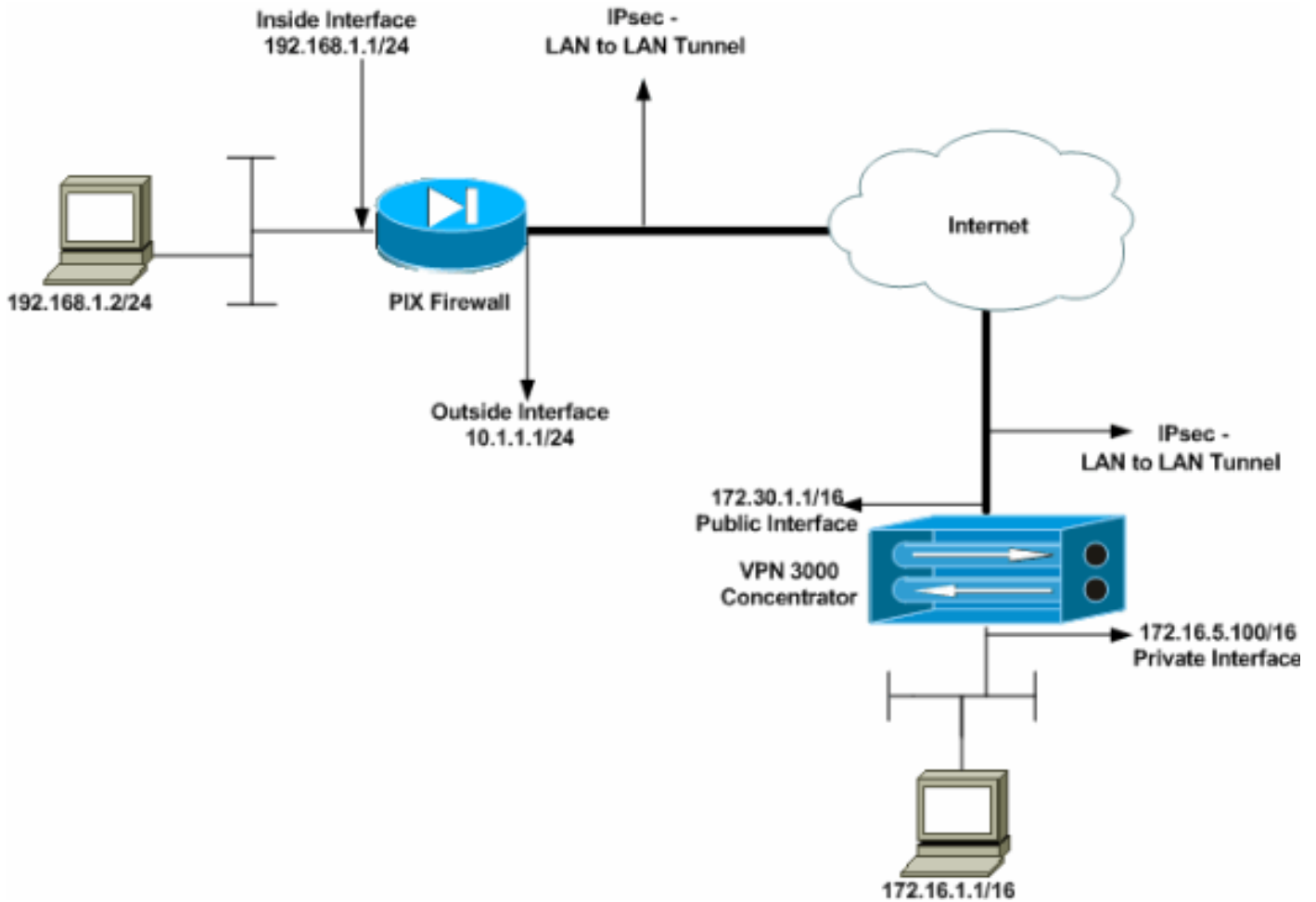
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

- [Configure o PIX](#)
- [Configurar o VPN 3000 Concentrator](#)

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:



Configure o PIX

PIX

```

PIX7#show running-config
: Saved
:
PIX Version 7.1(1)
!
hostname PIX7
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
!--- Configures the outside interface of the PIX. !---
By default, the security level for the outside interface
is 0. interface Ethernet0
  nameif outside
  security-level 0
  ip address 10.1.1.1 255.255.255.0
!
!--- Configures the inside interface of the PIX. !--- By
default, the security level for the inside interface is
100. interface Ethernet1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
!--- Defines the IP addresses that should not be NATed.
access-list nonat extended permit ip 192.168.1.0
255.255.255.0 172.16.0.0 255.255.0.0
access-list outside extended permit icmp any any

```

```

!--- Defines the IP addresses that can communicate via
the IPsec tunnel. access-list 101 extended permit ip
192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list OUT extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-504.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list nonat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
!--- Output is suppressed. !--- These are the IPsec
parameters that are negotiated with the client. crypto
ipsec transform-set my-set esp-aes-256 esp-sha-hmac
crypto map mymap 20 match address 101
crypto map mymap 20 set peer 172.30.1.1
crypto map mymap 20 set transform-set my-set
crypto map mymap interface outside
!--- These are the Phase I parameters negotiated by the
two peers. isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- A tunnel group consists of a set of records !---
that contain tunnel connection policies. The two
attributes !--- are General and IPsec. Use the remote
peer IP address as the !--- name of the Tunnel group. In
this example 172.30.1.1 is the peer IP address. !---
Refer to Tunnel Group for more information. tunnel-group
172.30.1.1 type ipsec-l2l
tunnel-group 172.30.1.1 ipsec-attributes
pre-shared-key *
!--- Output is suppressed. ! : end PIX7#

```

[Configurar o VPN 3000 Concentrator](#)

Os VPN Concentrators não são pré-programados com endereços IP em suas configurações de fábrica. Você precisa usar a porta de console para configurar as configurações iniciais que são uma interface de linha de comando (CLI) baseada em menu. Consulte [Configurando Concentradores VPN através do Console](#) para obter informações sobre como configurar através do console.

Depois de configurar o endereço IP na interface Ethernet 1 (privada), você pode configurar o restante com a CLI ou através da interface do navegador. A interface do navegador suporta HTTP e HTTP sobre SSL (Secure Socket Layer).

Esses parâmetros são configurados através do console:

- **Hora/Data** — A hora e a data corretas são muito importantes. Eles ajudam a garantir que os registros e registros contábilísticos sejam precisos e que o sistema possa criar um certificado de segurança válido.
- **Interface Ethernet 1 (privada)** — O endereço IP e a máscara (da topologia de rede 172.16.5.100/16).

O VPN Concentrator agora está acessível por meio de um navegador HTML da rede interna. Consulte [Utilização da Interface de Linha de Comando para Configuração Rápida](#) para obter informações sobre como configurar o VPN Concentrator no modo CLI.

Digite o endereço IP da interface privada no navegador da Web para ativar a interface GUI.

Clique no ícone **salvar as alterações necessárias** para salvar as alterações na memória. O nome de usuário e a senha padrão de fábrica são **admin**, que diferencia maiúsculas de minúsculas.

1. Inicie a GUI e selecione **Configuration > Interfaces** para configurar o endereço IP para a interface pública e o gateway padrão.


Configuration | Interfaces Sunday, 19 February 2006 16:54:00
Save Needed Refresh

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.5.100	255.255.0.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	172.30.1.1	255.255.0.0	00.03.A0.89.BF.D1	172.30.1.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- [Power Supplies](#)



2. Selecione **Configuration > Policy Management > Traffic Management > Network Lists > Add or Modify** para criar as listas de rede que definem o tráfego a ser criptografado. Adicione aqui as redes local e remota. Os endereços IP devem espelhar os da lista de acesso configurada no PIX remoto. Neste exemplo, as duas listas de rede são **remote_network** e **VPN Client Local LAN**.

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Name of the Network List you are adding. The name must be unique.

Network List

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

3. Selecione **Configuration > System > Tunneling Protocols > IPsec LAN-to-LAN > Add** para configurar o túnel IPsec LAN-to-LAN. Clique em **Apply** quando tiver concluído. Insira o endereço IP do peer, as listas de rede criadas na etapa 2, os parâmetros IPsec e ISAKMP e a chave pré-compartilhada. Neste exemplo, o endereço IP do peer é **10.1.1.1**, as listas de rede são **remote_network** e **VPN Client Local LAN**, e **cisco** é a chave pré-compartilhada.

Modify an IPSec LAN-to-LAN connection.

Enable <input checked="" type="checkbox"/>	Check to enable this LAN-to-LAN connection.
Name <input type="text" value="Test"/>	Enter the name for this LAN-to-LAN connection.
Interface <input type="text" value="Ethernet 2 (Public) (172.30.1.1)"/>	Select the interface for this LAN-to-LAN connection.
Connection Type <input type="text" value="Bi-directional"/>	Choose the type of LAN-to-LAN connection. An <i>Originate-Only</i> connection may have multiple peers specified below.
Peers <input type="text" value="10.1.1.1"/>	Enter the remote peer IP addresses for this LAN-to-LAN connection. <i>Originate-Only</i> connection may specify up to ten peer IP addresses. Enter one IP address per line.
Digital Certificate <input type="text" value="None (Use Preshared Keys)"/>	Select the digital certificate to use.
Certificate Transmission <input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key <input type="text" value="cisco"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication <input type="text" value="ESP/SHA/HMAC-160"/>	Specify the packet authentication mechanism to use.
Encryption <input type="text" value="AES-256"/>	Specify the encryption mechanism to use.
IKE Proposal <input type="text" value="IKE-AES256-SHA"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Filter <input type="text" value="-None-"/>	Choose the filter to apply to the traffic that is tunneled through this LAN-to-LAN connection.
IPSec NAT-T <input type="checkbox"/>	Check to let NAT-T compatible IPSec peers establish this LAN-to-LAN connection through a NAT device. You must also enable IPSec over NAT-T under NAT Transparency.
Bandwidth Policy <input type="text" value="-None-"/>	Choose the bandwidth policy to apply to this LAN-to-LAN connection.
Routing <input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Local Network: If a LAN-to-LAN NAT rule is used, this is the Translated Network address.

Network List <input type="text" value="VPN Client Local LAN (Default)"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	

Remote Network: If a LAN-to-LAN NAT rule is used, this is the Remote Network address.

Network List <input type="text" value="remote_network"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address <input type="text"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask <input type="text"/>	

4. Selecione **Configuration > User Management > Groups > Modify 10.1.1.1** para exibir as informações do grupo geradas automaticamente. **Observação:** não modifique essas configurações de grupo.

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters		
Attribute	Value	Description
Group Name	10.1.1.1	Enter a unique name for the group.
Password	XXXXXXXXXX	Enter the password for the group.
Verify	XXXXXXXXXX	Verify the group's password.
Type	Internal	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Apply Cancel

Verificar

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

- [Verificar o PIX](#)
- [Verifique o VPN 3000 Concentrator](#)

Verificar o PIX

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 isakmp sa](#) — Exibe todas as associações de segurança (SAs) IKE atuais em um peer. O estado MM_ACTIVE indica que o modo principal é usado para configurar o túnel VPN IPsec. Neste exemplo, o PIX Firewall inicia a conexão IPsec. O endereço IP do peer é 172.30.1.1 e usa o modo principal para estabelecer a conexão.

```
PIX7#show isakmp sa
```

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 172.30.1.1
  Type    : L2L                Role    : initiator
  Rekey   : no                 State   : MM_ACTIVE
```

- [show ipsec sa](#) — Exibe as configurações usadas pelas SAs atuais. Verifique os endereços IP dos pares, as redes acessíveis nas extremidades local e remota e o conjunto de transformações usado. Há duas SAs ESP, uma em cada direção.

```
PIX7#show ipsec sa
```

```
interface: outside
Crypto map tag: mymap, seq num: 20, local addr: 10.1.1.1

access-list 101 permit ip 192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
```


current_peer: 172.30.1.1

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0
```

local crypto endpt.: 10.1.1.1, remote crypto endpt.: 172.30.1.1

```
path mtu 1500, ipsec overhead 76, media mtu 1500
current outbound spi: 136580F6
```

inbound esp sas:

```
spi: 0xF24F4675 (4065281653)
transform: esp-aes-256 esp-sha-hmac
in use settings = {L2L, Tunnel,}
slot: 0, conn_id: 1, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (3824999/28747)
IV size: 16 bytes
replay detection support: Y
```

outbound esp sas:

```
spi: 0x136580F6 (325419254)
transform: esp-aes-256 esp-sha-hmac
in use settings = {L2L, Tunnel,}
slot: 0, conn_id: 1, crypto-map: mymap
sa timing: remaining key lifetime (kB/sec): (3824999/28745)
IV size: 16 bytes
replay detection support: Y
```

Use os comandos [clear ipsec sa](#) e [clear isakmp sa](#) para redefinir o túnel.

[Verifique o VPN 3000 Concentrator](#)

Selecione **Monitoring > Statistics > IPsec** para verificar se o túnel foi ativado no VPN 3000 Concentrator. Contém as estatísticas para os parâmetros IKE e IPsec.

IKE (Phase 1) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	5720
Sent Bytes	5576
Received Packets	57
Sent Packets	56
Received Packets Dropped	0
Sent Packets Dropped	0
Received Notifies	52
Sent Notifies	104
Received Phase-2 Exchanges	1
Sent Phase-2 Exchanges	0
Invalid Phase-2 Exchanges Received	0
Invalid Phase-2 Exchanges Sent	0
Rejected Received Phase-2 Exchanges	0
Rejected Sent Phase-2 Exchanges	0
Phase-2 SA Delete Requests Received	0
Phase-2 SA Delete Requests Sent	0
Initiated Tunnels	0
Failed Initiated Tunnels	0
Failed Remote Tunnels	0
Authentication Failures	0
Decryption Failures	0
Hash Validation Failures	0
System Capability Failures	0
No-SA Failures	0

IPSec (Phase 2) Statistics

Active Tunnels	1
Total Tunnels	1
Received Bytes	448
Sent Bytes	448
Received Packets	4
Sent Packets	4
Received Packets Dropped	0
Received Packets Dropped (Anti-Replay)	0
Sent Packets Dropped	0
Inbound Authentications	4
Failed Inbound Authentications	0
Outbound Authentications	4
Failed Outbound Authentications	0
Decryptions	4
Failed Decryptions	0
Encryptions	4
Failed Encryptions	0
System Capability Failures	0
No-SA Failures	0
Protocol Use Failures	0

Você pode monitorar ativamente a sessão em **Monitoramento > Sessões**. Você pode redefinir o túnel IPsec aqui.

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name.

Group

Session Summary

Active LAN-to-LAN Sessions since Stats Reset	Active Remote Access Sessions since Stats Reset	Active Management Sessions since Stats Reset	Total Active Sessions since Stats Reset	Peak Concurrent Sessions since Stats Reset	Weighted Active Load since Stats Reset	Percent Session Load since Stats Reset	Concurrent Sessions Limit	Total Cumulative Sessions since Stats Reset
1	0	0	1	0	1	1.00%	100	2

NAC Session Summary

Accepted since Stats Reset		Rejected since Stats Reset		Exempted since Stats Reset		Non-responsive since Stats Reset		Hold-off since Stats Reset		N/A since Stats Reset	
Active	Total	Active	Total	Active	Total	Active	Total	Active	Total	Active	Total
0	0	0	0	0	0	0	0	0	0	0	0

LAN-to-LAN Sessions

[[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Test	10.1.1.1	IPSec/LAN-to-LAN	AES-256	Feb 19 17:02:01	0:06:02	448	448

Remote Access Sessions

[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token
No Remote Access Sessions							

Management Sessions

[[LAN-to-LAN Sessions](#) | [Remote Access Sessions](#)]

Administrator	IP Address	Protocol	Encryption	Login Time	Duration
admin	172.16.1.1	HTTP	3DES-168 SSLv3	Jan 01 05:45:00	0:11:30

Troubleshoot

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

- [Solucionar problemas do PIX](#)
- [Solucionar problemas do VPN 3000 Concentrator](#)
- [PFS](#)

Solucionar problemas do PIX

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`.

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

Os comandos **debug** no PIX para túneis VPN são:

- [debug crypto isakmp](#) —Depura as negociações SA ISAKMP.
- [debug crypto ipsec](#) —Depura as negociações de SA IPsec.

Solucionar problemas do VPN 3000 Concentrator

Semelhante aos comandos debug nos roteadores Cisco, você pode configurar Classes de Evento para visualizar todos os alarmes. Selecione **Configuration > System > Events > Classes > Add** para ativar o registro de classes de eventos.

Selecione **Monitoring > Filterable Event Log** para monitorar os eventos habilitados.

Select Filter Options

Event Class	<input type="text" value="All Classes"/> AUTH AUTHDBG AUTHDECODE	Severities	<input type="text" value="ALL"/> 1 2 3
Client IP Address	<input type="text" value="0.0.0.0"/>	Events/Page	<input type="text" value="100"/>
Group	<input type="text" value="-All-"/>	Direction	<input type="text" value="Oldest to Newest"/>

```
1 02/19/2006 17:17:00.080 SEV-5 IKEDBG/64 RPT-33 10.1.1.1
IKE Peer included IKE fragmentation capability flags:
Main Mode:      True
Aggressive Mode: True

3 02/19/2006 17:17:00.750 SEV-4 IKE/119 RPT-23 10.1.1.1
Group [10.1.1.1]
PHASE 1 COMPLETED

4 02/19/2006 17:17:00.750 SEV-4 AUTH/22 RPT-23 10.1.1.1
User [10.1.1.1] Group [10.1.1.1] connected, Session Type: IPSec/LAN-to-LAN

5 02/19/2006 17:17:00.750 SEV-4 AUTH/84 RPT-23
LAN-to-LAN tunnel to headend device 10.1.1.1 connected

6 02/19/2006 17:17:01.020 SEV-5 IKE/35 RPT-23 10.1.1.1
Group [10.1.1.1]
Received remote IP Proxy Subnet data in ID Payload:
  Address 192.168.1.0, Mask 255.255.255.0, Protocol 0, Port 0

9 02/19/2006 17:17:01.020 SEV-5 IKE/34 RPT-23 10.1.1.1
Group [10.1.1.1]
Received local IP Proxy Subnet data in ID Payload:
  Address 172.16.0.0, Mask 255.255.0.0, Protocol 0, Port 0

12 02/19/2006 17:17:01.020 SEV-5 IKE/66 RPT-13 10.1.1.1
Group [10.1.1.1]
IKE Remote Peer configured for SA: L2L: Test

13 02/19/2006 17:17:01.350 SEV-4 IKE/49 RPT-3 10.1.1.1
Group [10.1.1.1]
Security negotiation complete for LAN-to-LAN Group (10.1.1.1)
Responder, Inbound SPI = 0x136580f6, Outbound SPI = 0xf24f4675

16 02/19/2006 17:17:01.350 SEV-4 IKE/120 RPT-3 10.1.1.1
Group [10.1.1.1]
PHASE 2 COMPLETED (msgid=6b2795cd)
```

[PFS](#)

Nas negociações de IPsec, o Perfect Forward Secrecy (PFS) garante que cada nova chave

criptográfica não tenha relação com nenhuma chave anterior. Habilite ou desabilite o PFS em ambos os peers do túnel; caso contrário, o túnel IPsec de LAN para LAN (L2L) não será estabelecido no PIX/ASA.

O PFS é desabilitado por padrão. Para habilitar o PFS, use o comando **pfs** com a palavra-chave *enable* no modo de configuração de política de grupo. Para desabilitar o PFS, insira a palavra-chave *disable*.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Para remover o atributo de PFS da configuração em execução, insira a forma no deste comando. Uma política de grupo pode herdar um valor para o PFS de outra política de grupo. Insira a forma no deste comando para impedir que um valor seja herdado.

```
hostname(config-group-policy)#no pfs
```

[Informações Relacionadas](#)

- [Cisco PIX 500 Series Security Appliances - Página de suporte](#)
- [Cisco VPN 3000 Series Concentrator - Página de suporte](#)
- [Referência de comando do Cisco PIX 500 Series Security Appliance](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)