

# Exemplo de configuração de VPN entre produtos da Sonicwall e Cisco Security Appliance

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Conventions](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração Sonicwall](#)

[Configuração do modo principal do IPsec](#)

[Configuração do modo agressivo IPsec](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## [Introduction](#)

Este documento demonstra como configurar um túnel de IPsec com chaves pré-compartilhada para comunicar-se entre duas redes privadas utilizando os modos principal e agressivo. Neste exemplo, as redes de comunicação são a rede privada 192.168.1.x dentro do Cisco Security Appliance (PIX/ASA) e a rede privada 172.22.1.x dentro do Firewall do Sonicwall™ TZ170.

## [Prerequisites](#)

## [Requirements](#)

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

- O tráfego de dentro do Cisco Security Appliance e de dentro do Sonicwall TZ170 deve fluir para a Internet (representada aqui pelas redes 10.x.x.x) antes de iniciar esta configuração.
- Os usuários devem estar familiarizados com a negociação de IPsec. Esse processo pode ser dividido em cinco etapas que incluem duas fases de Internet Key Exchange (IKE). Um túnel de IPsec é iniciado por um tráfego interessante. O tráfego é considerado interessante quando ele é transmitido entre os peers IPsec. Na Fase 1 IKE, os correspondentes IPsec negociam a política de Associação de segurança (SA) IKE estabelecida. Quando os peers são autenticados, um túnel seguro é criado com o uso do Internet Security Association and Key

Management Protocol (ISAKMP). Em IKE Phase 2, os correspondentes de IPSec utilizam o túnel autenticado e seguro para negociar transformações de IPSec AS. A negociação da política compartilhada determina como o túnel de IPSec é estabelecido. O túnel de IPSec é criado e os dados são transferidos entre peers de IPSec com base nos parâmetros de IPSec configurados em grupos de transformação do IPSec. O túnel de IPSec finaliza quando os IPSec SAs são excluídos ou quando sua vida útil expira.

## Componentes Utilizados

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

- Cisco PIX 515E versão 6.3(5)
- Cisco PIX 515 versão 7.0(2)
- Sonicwall TZ170, SonicOS Standard 2.2.0.1

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.

## Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- A configuração do PIX 6.3(5) pode ser usada com todos os outros produtos de firewall Cisco PIX que executam essa versão do software (PIX 501, 506 e assim por diante)
- A configuração do PIX/ASA 7.0(2) só pode ser usada em dispositivos que executam a linha de software PIX 7.0 (exclui os 501, 506 e possivelmente alguns 515s mais antigos) assim como o Cisco 5500 Series ASA.

## Conventions

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

## Configurar

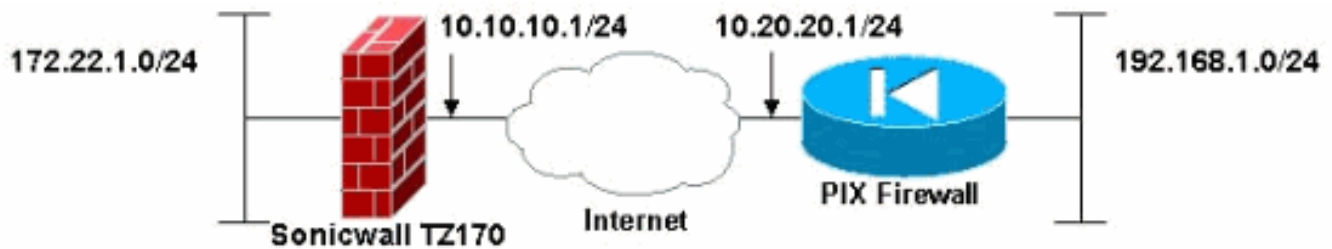
Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

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

**Observação:** no modo Agressivo IPsec, é necessário que o Sonicwall inicie o túnel IPsec para o PIX. Você pode ver isso ao analisar as depurações para essa configuração. Isso é inerente à maneira como o Modo Agressivo IPsec opera.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



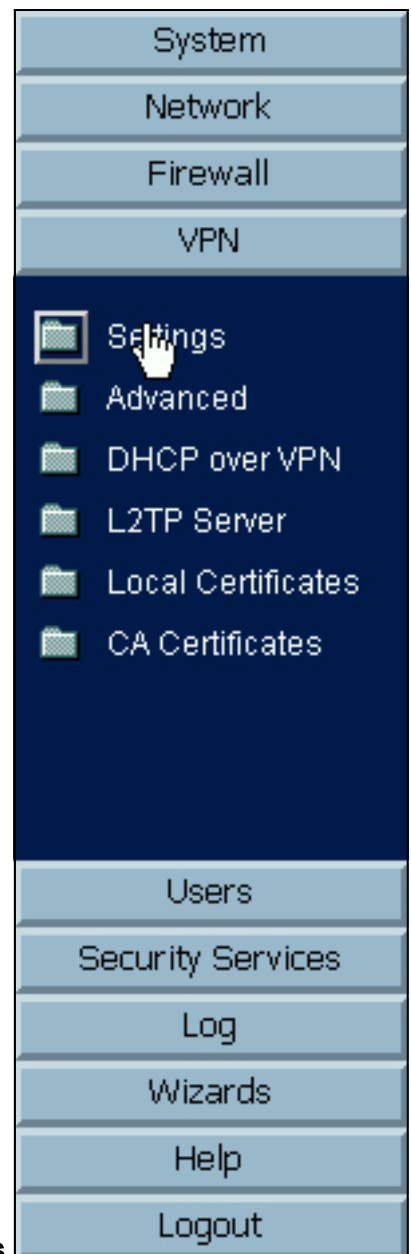
## Configuração Sonicwall

A configuração do Sonicwall TZ170 é realizada através de uma interface baseada na Web.

Conclua estes passos:

1. Conecte-se ao endereço IP do roteador em uma das interfaces internas usando um navegador da Web padrão. Isso ativa a janela de login.

The screenshot shows the Sonicwall login page. At the top, there is a blue header with the Sonicwall logo and the text "COMPREHENSIVE INTERNET SECURITY™". Below the header, the main content area is light blue. In the bottom right corner, there is a dark blue login box. Inside this box, there are two input fields: "Name:" with the value "admin" and "Password:" with a masked password "XXXXXXXXXX". Below the password field is a "Login" button with a mouse cursor pointing to it.



2. Faça login no dispositivo Sonicwall e selecione **VPN > Settings**.
3. Insira o endereço IP do peer VPN e o segredo pré-compartilhado que será usado. Clique em **Adicionar** em Redes de

General Proposals **Advanced**

### Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: To Cisco PIX

IPSec Primary Gateway Name or Address: 10.20.20.1

IPSec Secondary Gateway Name or Address: 0.0.0.0

Shared Secret: cisco123

### Destination Networks

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Specify destination networks below

Network	Subnet Mask
---------	-------------

Add... Edit... Delete

Ready

OK Cancel Help

destino.

Network: 192.168.1.0

Subnet Mask: 255.255.255.0

OK Cancel

4. Digite a rede de destino.

A janela de Settings é

General Proposals **Advanced**

### Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: To Cisco PIX

IPSec Primary Gateway Name or Address: 10.20.20.1

IPSec Secondary Gateway Name or Address: 0.0.0.0

Shared Secret: cisco123

### Destination Networks

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Specify destination networks below

Network	Subnet Mask
192.168.1.0	255.255.255.0

Add... Edit... Delete

Ready

OK Cancel Help

exibida.

5. Clique na guia Propostas na parte superior da janela Configurações.
6. Selecione a troca que você planeja usar para essa configuração (Modo principal ou Modo agressivo) junto com o resto das configurações da Fase 1 e Fase 2. Este exemplo de configuração usa criptografia AES-256 para ambas as fases com o algoritmo hash SHA1 para autenticação e a política Diffie-Hellman 2 de 1024 bits para

General Proposals **Advanced**

### IKE (Phase 1) Proposal

Exchange: Main Mode  
DH Group: Group 2  
Encryption: AES-256  
Authentication: SHA1  
Life Time (seconds): 28800

### Ipssec (Phase 2) Proposal

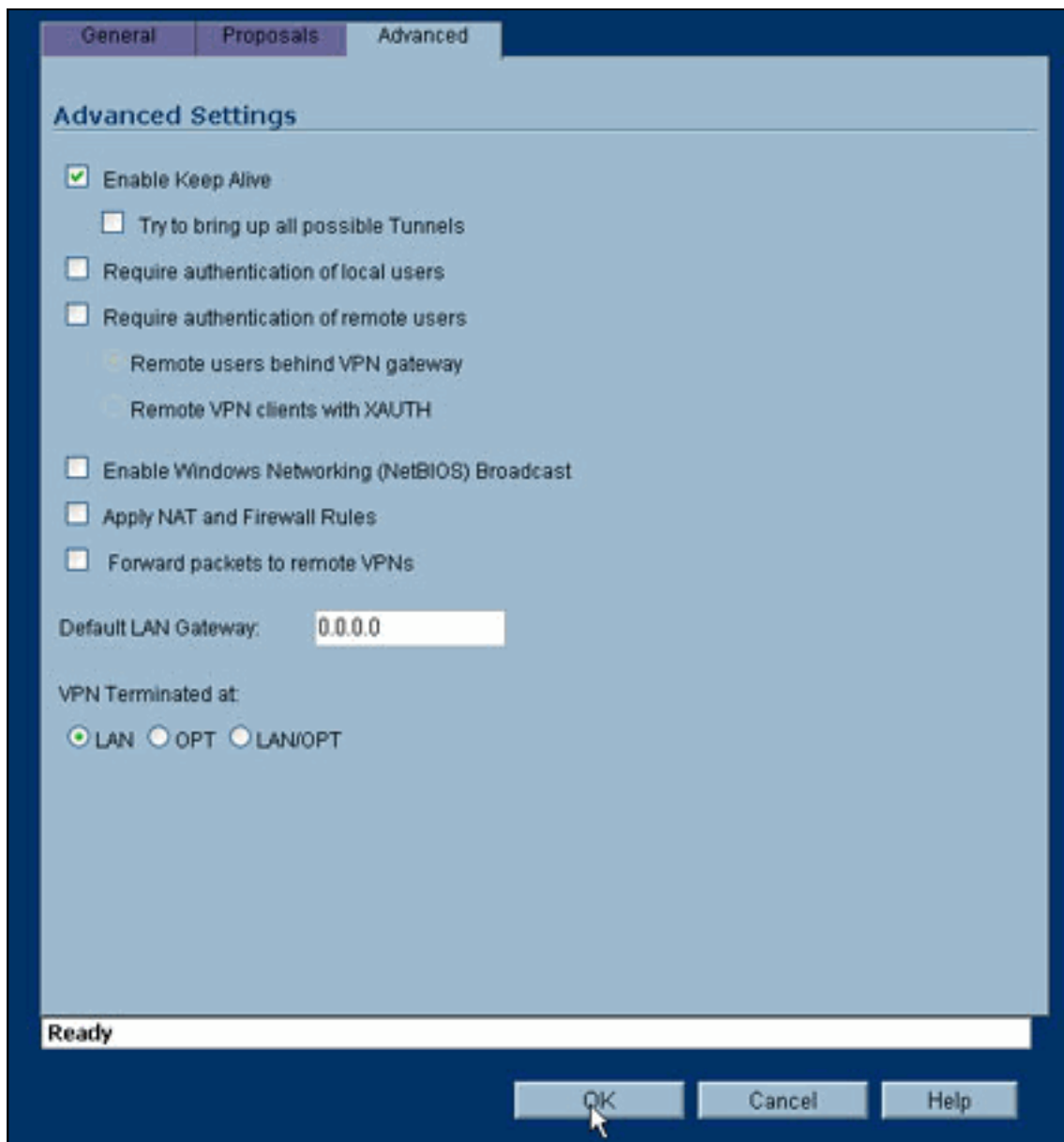
Protocol: ESP  
Encryption: AES-256  
Authentication: SHA1  
 Enable Perfect Forward Secrecy  
DH Group: Group 2  
Life Time (seconds): 28800

Ready

OK Cancel Help

IKE.

7. Clique na guia Advanced. Há opções adicionais que você pode desejar configurar nesta guia. Estas são as configurações usadas para esta configuração de



exemplo.

8. Click **OK**. Depois de concluir essa configuração e a configuração no PIX remoto, a janela Configurações deve ser semelhante a esta janela Configurações de exemplo.








VPN > Settings VPN Policy Wizard... Apply Cancel ?

VPN Global Settings

Enable VPN  
 Unique Firewall Identifier: 0094011-048C79


VPN Policies

Name	Gateway	Destinations	Crypto Suite	Enable	Configure
GroupVPN			ESP AES-256 HMAC SHA1 (IKE)	<input type="checkbox"/>	  
To Cisco PIX	10.20.20.1	192.168.1.1 - 192.168.1.254	ESP AES-256 HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	 

Add... Delete All

2 Policies Defined, 1 Policies Enabled, 3 Maximum Policies Allowed

Currently Active VPN Tunnels

Name	Local	Remote	Gateway	
To Cisco PIX	172.22.1.1 - 172.22.1.255	192.168.1.1 - 192.168.1.254	10.20.20.1	Renegotiate 

## Configuração do modo principal do IPsec

Esta seção utiliza as seguintes configurações:

- [Cisco PIX 515e versão 6.3\(5\)](#)
- [Cisco PIX 515 versão 7.0\(2\)](#)

### Cisco PIX 515e versão 6.3(5)

```

pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 names !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and

```

```

subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server
TACACS+ deadtime 10 aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3 aaa-server
RADIUS deadtime 10 aaa-server LOCAL protocol local no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION: !--- Defines the transform set
for Phase 2 encryption and authentication. !---
Austinlab is the name of the transform set that uses
aes-256 encryption !--- as well as the SHA1 hash
algorithm for authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies IKE is used to establish the IPsec SAs
for the map "maptosw". crypto map maptosw 67 ipsec-
isakmp !--- Specifies the ACL "pixtosw" to use with this
map . crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map. crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Specifies the interface
to use for the IPsec tunnel.

isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used with the preshared key cisco123. isakmp key
***** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#

```

## Cisco PIX 515 versão 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS@. !--- This output configures the IP
address, interface name, !--- and security level for
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pxtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pxtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies the ACL pxtosw to use with this map.
crypto map maptosw 67 match address pxtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map . crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Defines how the PIX
```

```
identifies itself in !--- IKE negotiations (IP address in this case).
```

```
isakmp identity address
```

```
!--- Specifies the interface to use for the IPsec tunnel. isakmp enable outside !--- These five commands specify the Phase 1 configuration !--- settings specific to this sample configuration. isakmp policy 13 authentication pre-share isakmp policy 13 encryption aes-256 isakmp policy 13 hash sha isakmp policy 13 group 2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh timeout 5 console timeout 0 !--- These three lines set the IPsec attributes for the tunnel to the !--- remote peer. This is where the preshared key is defined for Phase 1 and the !--- IPsec tunnel type is set to site-to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-group 10.10.10.1 ipsec-attributes pre-shared-key * Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end pix515-702#
```

## Configuração do modo agressivo IPsec

Esta seção utiliza as seguintes configurações:

- [Cisco PIX 515e versão 6.3\(5\)](#)
- [Cisco PIX 515 versão 7.0\(2\)](#)

### **Cisco PIX 515e versão 6.3(5)**

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !--- Specifies the inside and outside interfaces. nameif ethernet0 outside security0 nameif ethernet1 inside security100 enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635 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 names !--- Specifies the traffic that can pass through the IPsec tunnel. access-list pixtosw permit ip 192.168.1.0 255.255.255.0 172.22.1.0 255.255.255.0 pager lines 24 mtu outside 1500 mtu inside 1500 !--- Sets the inside and outside IP addresses and subnet masks. ip address outside 10.20.20.1 255.255.255.0 ip address inside 192.168.1.1 255.255.255.0 ip audit info action alarm ip audit attack action alarm history enable arp timeout 14400 !--- Instructs PIX to perform PAT on the IP address on the outside interface. global (outside) 1 interface !--- Specifies addresses to be exempt from NAT (traffic to be tunneled). nat (inside) 0 access-list pixtosw !--- Specifies which addresses should use NAT (all except
```

```

those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server
TACACS+ deadtime 10 aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3 aaa-server
RADIUS deadtime 10 aaa-server LOCAL protocol local no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Implicit permit for all packets that come
from IPsec tunnels.
sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION !--- Defines the transform set for
Phase 2 encryption and authentication. !--- Austinlab is
the name of the transform set that uses aes-256
encryption !--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map ciscopix for the transform
set.
crypto dynamic-map ciscopix 1 set transform-set
austinlab !--- Specifies the IKE that should be used to
establish SAs !--- for the dynamic map.
crypto map
dynamptosw 66 ipsec-isakmp dynamic ciscopix !--- Applies
the settings above to the outside interface.
crypto map
dynamptosw interface outside !--- PHASE 1 CONFIGURATION
!--- Specifies the interface to use for the IPsec tunnel
.
isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used as the preshared key "cisco123".
isakmp key
***** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case).
isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration.
isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256
isakmp policy 13 hash sha
isakmp policy 13 group 2
isakmp policy 13 lifetime 28800
telnet timeout 5
ssh timeout 5
console
timeout 0
terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#

```

## Cisco PIX 515 versão 7.0(2)

```

pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

```

*!--- PIX 7 uses an interface configuration mode similar to Cisco IOS. !--- This output configures the IP*

```

address, interface name, and security level for !---
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map "ciscopix" for the defined
transform set. crypto dynamic-map ciscopix 1 set
transform-set austinlab !--- Specifies that IKE should
be used to establish SAs !--- for the defined dynamic
map. crypto map dynmptosw 66 ipsec-isakmp dynamic
ciscopix !--- Applies the settings to the outside
interface. crypto map dynmptosw interface outside !---
PHASE 1 CONFIGURATION !--- Defines how the PIX
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration settings !--- specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh

```

```
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

## 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 isakmp sa** — Exibe todas as SAs IKE atuais em um peer.
- **show crypto ipsec sa** — Exibe as configurações usadas pelas SAs atuais.

Essas tabelas mostram as saídas de algumas depurações para o modo Principal e Agressivo no PIX 6.3(5) e no PIX 7.0(2) depois que o túnel estiver totalmente estabelecido.

**Observação:** essas informações devem ser suficientes para estabelecer um túnel IPsec entre esses dois tipos de hardware. Se você tiver algum comentário, use o formulário de comentários no lado esquerdo deste documento.

- [Cisco PIX 515e versão 6.3\(5\) - Modo principal](#)
- [Cisco PIX 515 versão 7.0\(2\) - Modo principal](#)
- [Cisco PIX 515e versão 6.3\(5\) - Modo agressivo](#)
- [Cisco PIX 515 versão 7.0\(2\) - Modo agressivo](#)

### Cisco PIX 515e versão 6.3(5) - Modo principal

```
pix515e-635#show crypto isakmp sa
Total      : 1
Embryonic  : 0
dst        src        state    pending
created
   10.10.10.1    10.20.20.1    QM_IDLE    0
1
pix515e-635#

pix515e-635#show crypto ipsec sa

interface: outside
Crypto map tag: maptosw, local addr.
10.20.20.1

local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
current_peer: 10.10.10.1:500
PERMIT, flags={origin_is_acl,}
```

```
#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: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
path mtu 1500, ipsec overhead 72, media mtu
1500
current outbound spi: ed0afa33

inbound esp sas:
spi: 0xac624692(2892121746)
transform: esp-aes-256 esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: maptosw
sa timing: remaining key lifetime (k/sec):
(4607999/28718)
IV size: 16 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0xed0afa33(3976919603)
transform: esp-aes-256 esp-sha-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: maptosw
sa timing: remaining key lifetime (k/sec):
(4607999/28718)
IV size: 16 bytes
replay detection support: Y

outbound ah sas:

outbound pcp sas:

pix515e-635#
```

## Cisco PIX 515 versão 7.0(2) - Modo principal

```
pix515-702#show crypto 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: 10.10.10.1
Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
pix515-702#
```



```

pix515-702#show crypto ipsec sa
interface: outside
  Crypto map tag: maptosw, local addr: 10.20.20.1

  local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
    current_peer: 10.10.10.1

  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
    #send errors: 0, #recv errors: 0

  local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

  path mtu 1500, ipsec overhead 76, media mtu 1500
    current outbound spi: 2D006547

  inbound esp sas:
    spi: 0x309F7A33 (815757875)
    transform: esp-aes-256 esp-sha-hmac
    in use settings = {L2L, Tunnel, }
    slot: 0, conn_id: 1, crypto-map: maptosw
    sa timing: remaining key lifetime (kB/sec):
(4274999/28739)
    IV size: 16 bytes
    replay detection support: Y
  outbound esp sas:
    spi: 0x2D006547 (755000647)
    transform: esp-aes-256 esp-sha-hmac
    in use settings = {L2L, Tunnel, }
    slot: 0, conn_id: 1, crypto-map: maptosw
    sa timing: remaining key lifetime (kB/sec):
(4274999/28737)
    IV size: 16 bytes
    replay detection support: Y

pix515-702#

```

### Cisco PIX 515e versão 6.3(5) - Modo agressivo

```

pix515e-635#show crypto isakmp sa
Total      : 1
Embryonic  : 0

   dst          src          state      pending
created
   10.20.20.1   10.10.10.1   QM_IDLE   0
1

pix515e-635#show crypto ipsec sa

interface: outside
  Crypto map tag: dynmaptosw, local addr.
10.20.20.1

```

```
local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
    current_peer: 10.10.10.1:500
    PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts
digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts
verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
    path mtu 1500, ipsec overhead 72, media mtu
1500
    current outbound spi: efb1149d

inbound esp sas:
    spi: 0x2ad2c13c(718455100)
    transform: esp-aes-256 esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2, crypto map: dynmptosw
    sa timing: remaining key lifetime (k/sec):
(4608000/28736)
    IV size: 16 bytes
    replay detection support: Y

inbound ah sas:

inbound pcg sas:

outbound esp sas:
    spi: 0xefb1149d(4021359773)
    transform: esp-aes-256 esp-sha-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 1, crypto map: dynmptosw
    sa timing: remaining key lifetime (k/sec):
(4608000/28727)
    IV size: 16 bytes
    replay detection support: Y

outbound ah sas:

outbound pcg sas:

pix515e-635#
```

## Cisco PIX 515 versão 7.0(2) - Modo agressivo

```
pix515-702#show crypto 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: 10.10.10.1
  Type : L2L Role : responder
  Rekey : no State : AM_ACTIVE
  pix515-702#

pix515-702#show crypto ipsec sa
  interface: outside
  Crypto map tag: ciscopix, local addr:
10.20.20.1

  local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
  current_peer: 10.10.10.1

  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

  path mtu 1500, ipsec overhead 76, media mtu 1500
  current outbound spi: D7E2F5FD

inbound esp sas:
  spi: 0xDCBF6AD3 (3703532243)
  transform: esp-aes-256 esp-sha-hmac
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 1, crypto-map: ciscopix
  sa timing: remaining key lifetime (sec):
28703

  IV size: 16 bytes
  replay detection support: Y
outbound esp sas:
  spi: 0xD7E2F5FD (3621975549)
  transform: esp-aes-256 esp-sha-hmac
  in use settings = {L2L, Tunnel, }
  slot: 0, conn_id: 1, crypto-map: ciscopix
  sa timing: remaining key lifetime (sec):
28701

  IV size: 16 bytes
  replay detection support: Y

pix515-702#

```

## [Troubleshoot](#)

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

## [Informações Relacionadas](#)

- [Cisco PIX Firewall Software](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Avisos de campo de produto de segurança \(incluindo PIX\)](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)