

PIX/ASA 7.x e acima: Exemplo da configuração de túnel PIX-à-PIX VPN

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Diagrama de Rede](#)

[Convenções](#)

[Informações de Apoio](#)

[Configuração](#)

[Configuração ASDM](#)

[Configuração de CLI PIX](#)

[Túnel de site para site alternativo](#)

[Cancele as associações de segurança \(os SA\)](#)

[Verificar](#)

[Troubleshooting](#)

[PFS](#)

[Acesso de gerenciamento](#)

[Comandos debug](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve o procedimento para configurar túneis VPN entre dois PIX Firewalls usando o Cisco Adaptive Security Device Manager (ASDM). O ASDM é uma ferramenta de configuração com base em aplicativo projetada para ajudá-lo a instalar, configurar e monitorar seu PIX Firewall com a GUI. Os PIX Firewalls são colocados em dois locais diferentes.

Um túnel é formado usando o IPsec. O IPsec é uma combinação de padrões abertos que fornecem a confidencialidade de dados, a integridade de dados, e a autenticação de origem de dados entre ipsec peer.

Nota: Em PIX 7.1 e mais atrasado, o comando `sysopt connection permit-ipsec` é mudado à **conexão licença-VPN do sysopt**. Este comando permite que o tráfego que entra na ferramenta de segurança através de um túnel VPN e é decifrado então, contorneie Listas de acesso da relação. A política do grupo e por usuário Listas de acesso da autorização ainda aplica-se ao tráfego. A fim desabilitar esta característica, não use **nenhum** formulário deste comando. Este comando não é visível na configuração de CLI.

Refira [PIX 6.x: Exemplo de configuração do túnel PIX a PIX VPN simples](#) a fim aprender a

encenação mais mais ou menos idêntica onde a ferramenta de segurança de Cisco PIX executa a versão de software 6.x.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento especifica que este par inicia a primeira troca proprietária a fim determinar o par apropriado a que para conectar.

- Ferramenta de segurança da série do Cisco PIX 500 com versão 7.x e mais recente
- Versão 5.x.and ASDM mais atrasada

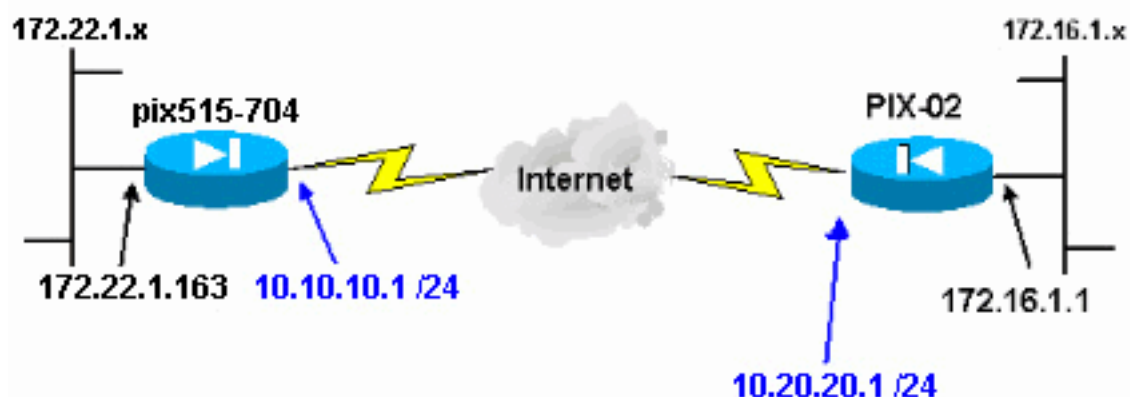
Nota: Consulte [Habilitação de Acesso HTTPS para o ASDM](#) para permitir que o ASA seja configurado pelo ASDM.

Nota: A versão 7.x/8.x do 5500 Series ASA executa o mesmo software considerado na versão de PIX 7.x/8.x. As configurações neste documento são aplicáveis a ambas as linhas de produto.

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Convenções

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

Informações de Apoio

A negociação de IPsec pode ser dividida em cinco etapas, e inclui duas fases de intercâmbio de chave de Internet (IKE).

1. Um túnel de IPsec é iniciado pelo tráfego interessante. O tráfego está considerado interessante quando viaja entre os ipsec peer.
2. Na fase 1 IKE, os ipsec peer negociam a política estabelecida da associação de segurança IKE (SA). Quando os correspondentes forem autenticados, um túnel seguro é criado, com uso da associação de segurança da Internet e protocolo de gerenciamento chave (ISAKMP).
3. Na fase 2 IKE, os ipsec peer usam o túnel seguro e autenticado para negociar IPsec SA transformam. A negociação da política compartilhada determina como o túnel de IPsec é estabelecido.
4. O túnel de IPsec é criado e os dados são transferidos entre os ipsec peer baseados nos parâmetros IPsec configurados no IPsec transformam grupos.
5. O túnel de IPsec termina quando o sas de IPsec é suprimido ou quando sua vida expira.**Nota:** A negociação de IPsec entre as duas PIXes falha se os SA em ambas as fases IKE não combinam nos pares.

Configuração

- [Configuração ASDM](#)
- [Configurações de CLI PIX](#)

Configuração ASDM

Conclua estes passos:

1. Abra seu navegador e datilografe o **<Inside_IP_Address_of_PIX> de https://** para alcançar o ASDM no PIX. Seja certo autorizar todos os avisos que seu navegador o der relativo à autenticidade de certificado de SSL. O nome de usuário padrão e a senha são ambos placa. O PIX apresenta este indicador para permitir a transferência do aplicativo ASDM. Este exemplo carrega o aplicativo no computador local e não o é executado em um Java applet.



Cisco ASDM 5.0



Cisco ASDM 5.0 provides an intuitive graphical user interface that makes it easy to set up, configure and manage your Cisco Security Appliances.

Cisco ASDM runs as either a local application or a Java Applet.

Running Cisco ASDM as a local Application

When you run Cisco ASDM as a local application, it connects to your Security Appliance from your desktop via SSL. Running Cisco ASDM as an application has these advantages:

- Upgrades of the local application are performed automatically.
- You can invoke ASDM from desktop shortcuts. No browser is required.
- One desktop shortcut allows you to connect to *multiple* Security Appliances.

[Download ASDM Launcher and Start ASDM](#)

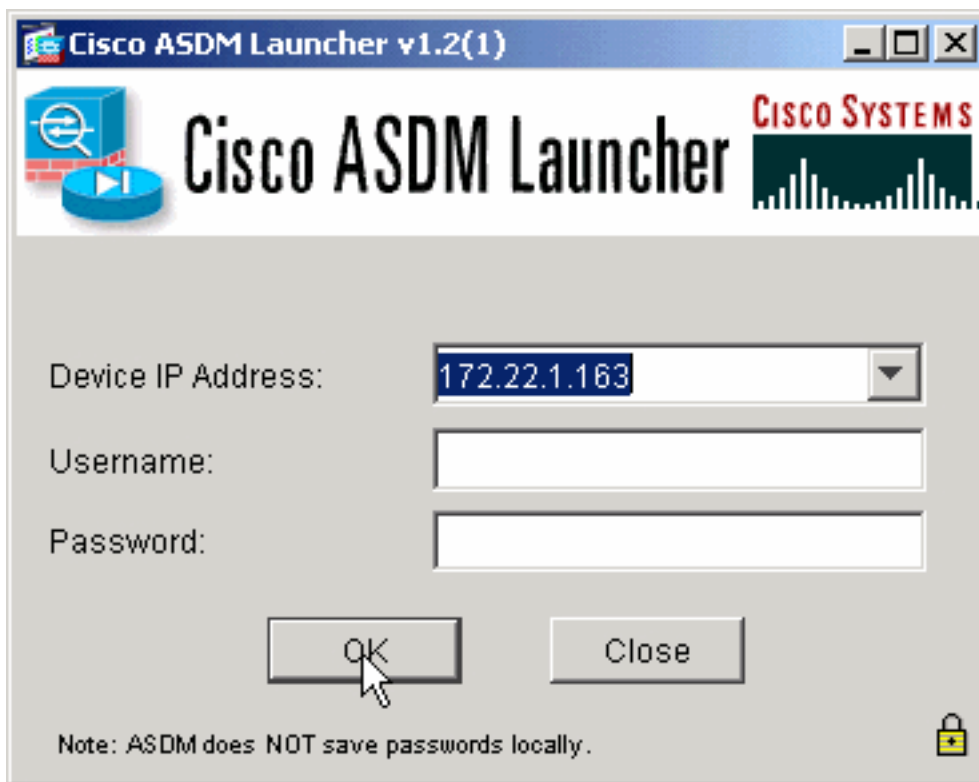
Running Cisco ASDM as a Java Applet

You can run Cisco ASDM as a Java applet that is dynamically downloaded from the device to which you connect.

[Run ASDM as a Java Applet](#)

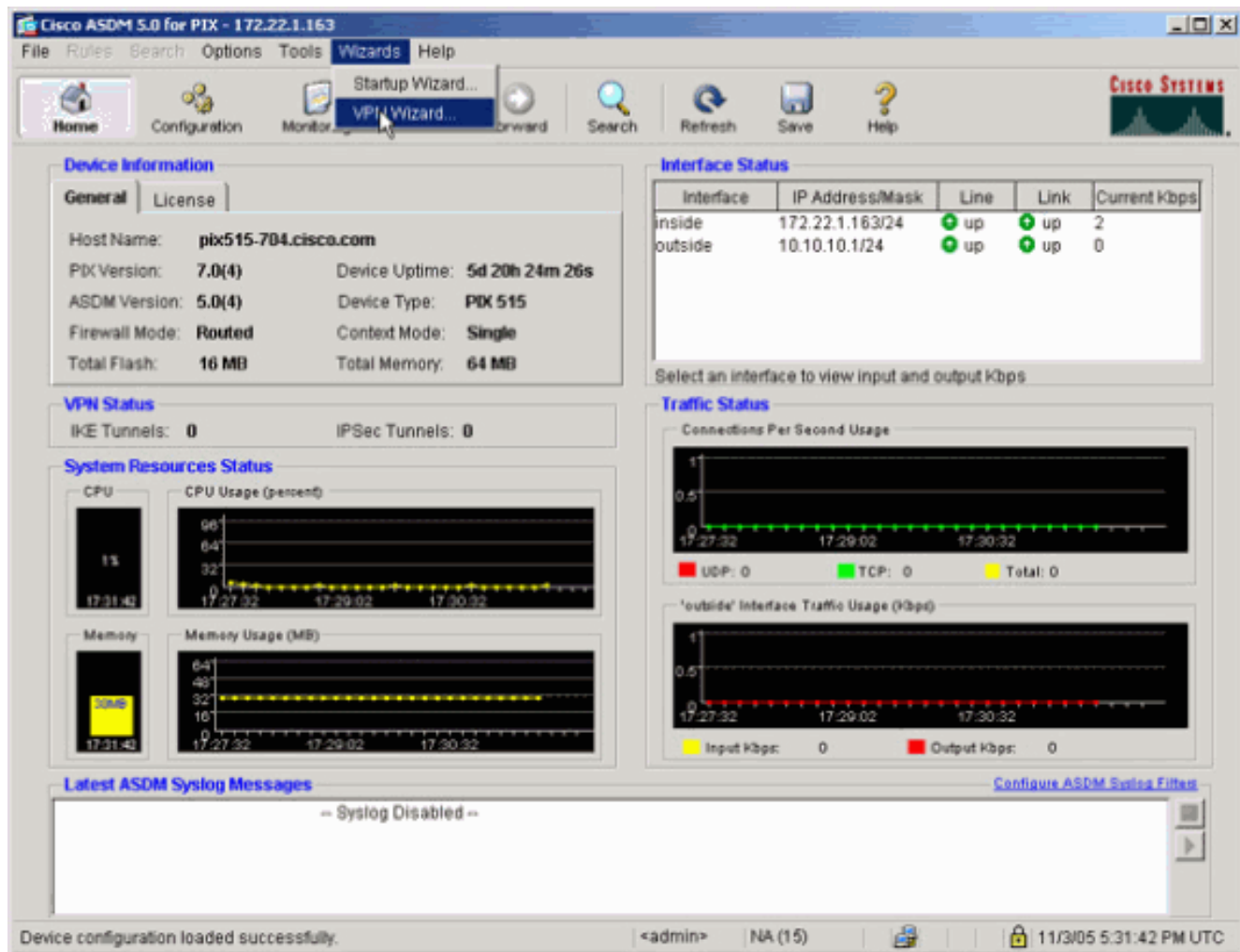
Copyright © 2005 Cisco Systems, Inc. All rights reserved.

2. Clique a **launcher ASDM da transferência e comece o ASDM** transferir o instalador para o aplicativo ASDM.
3. Uma vez que a launcher ASDM transfere, siga as alertas a fim instalar o software e executar o lançador ASDM Cisco.
4. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT para a relação que você configurou com o **HTTP** - comande e um nome de usuário e senha se você especificou um. Este exemplo usa o nome de usuário e senha da placa do

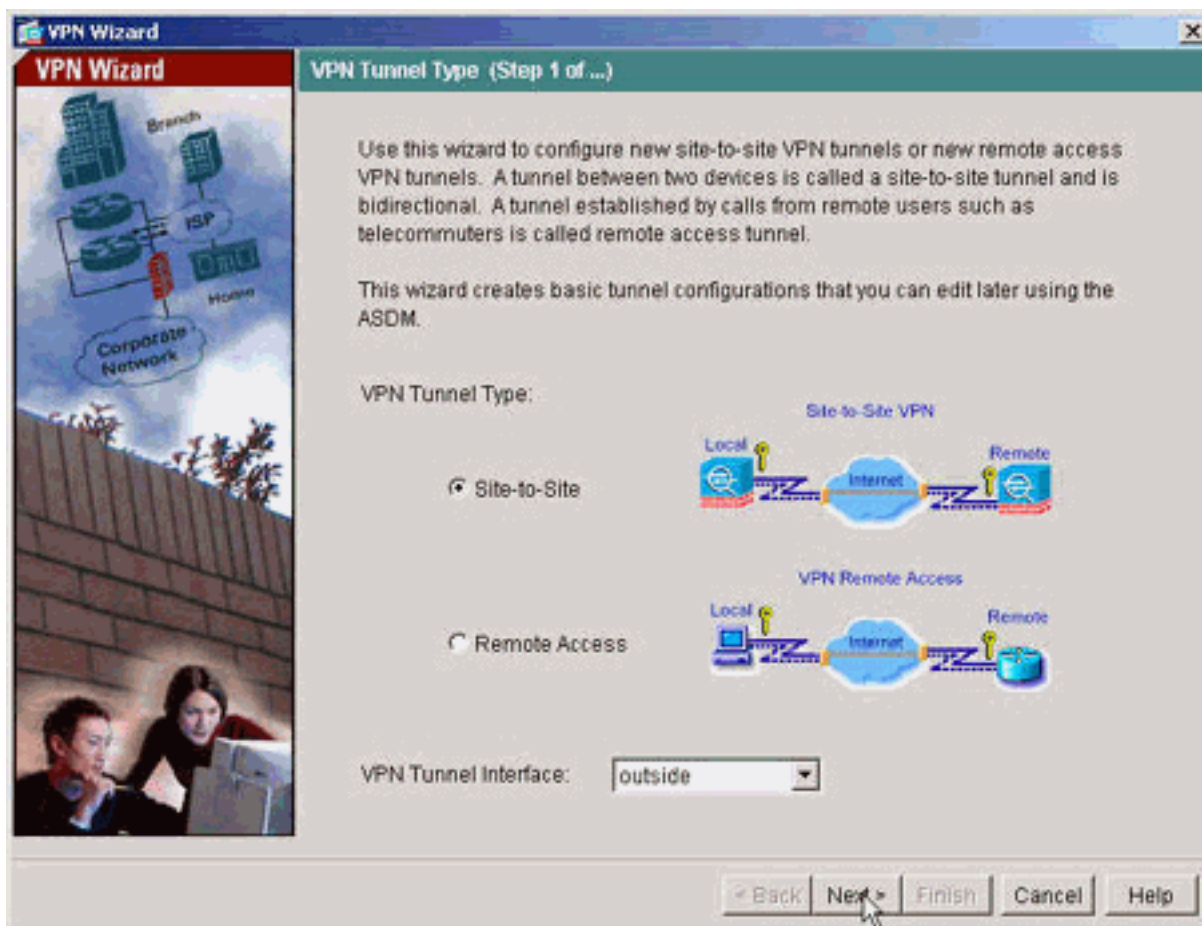


padrão.

5. Execute o wizard VPN uma vez que o aplicativo ASDM conecta ao PIX.

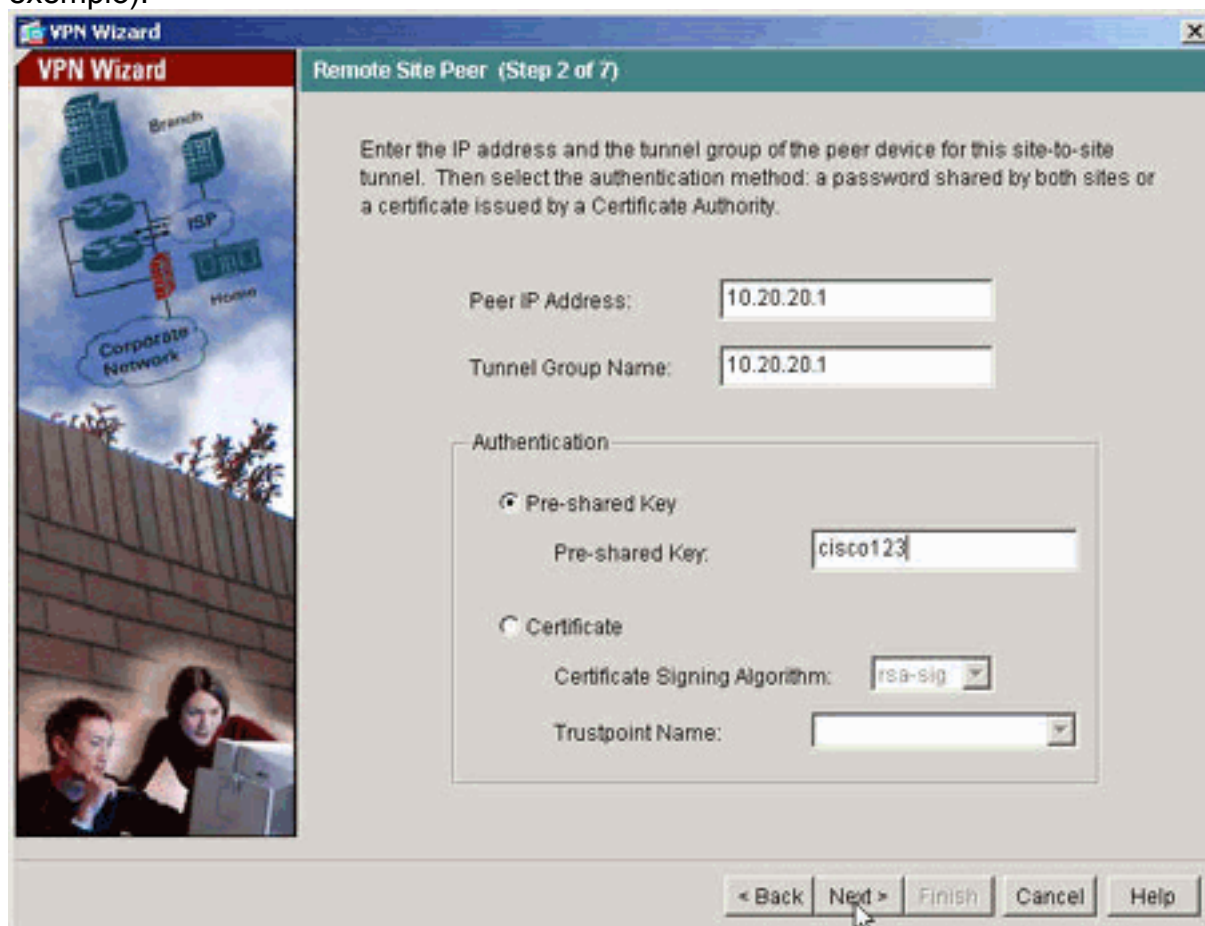


6. Escolha o tipo de túnel do VPN de Site-para-



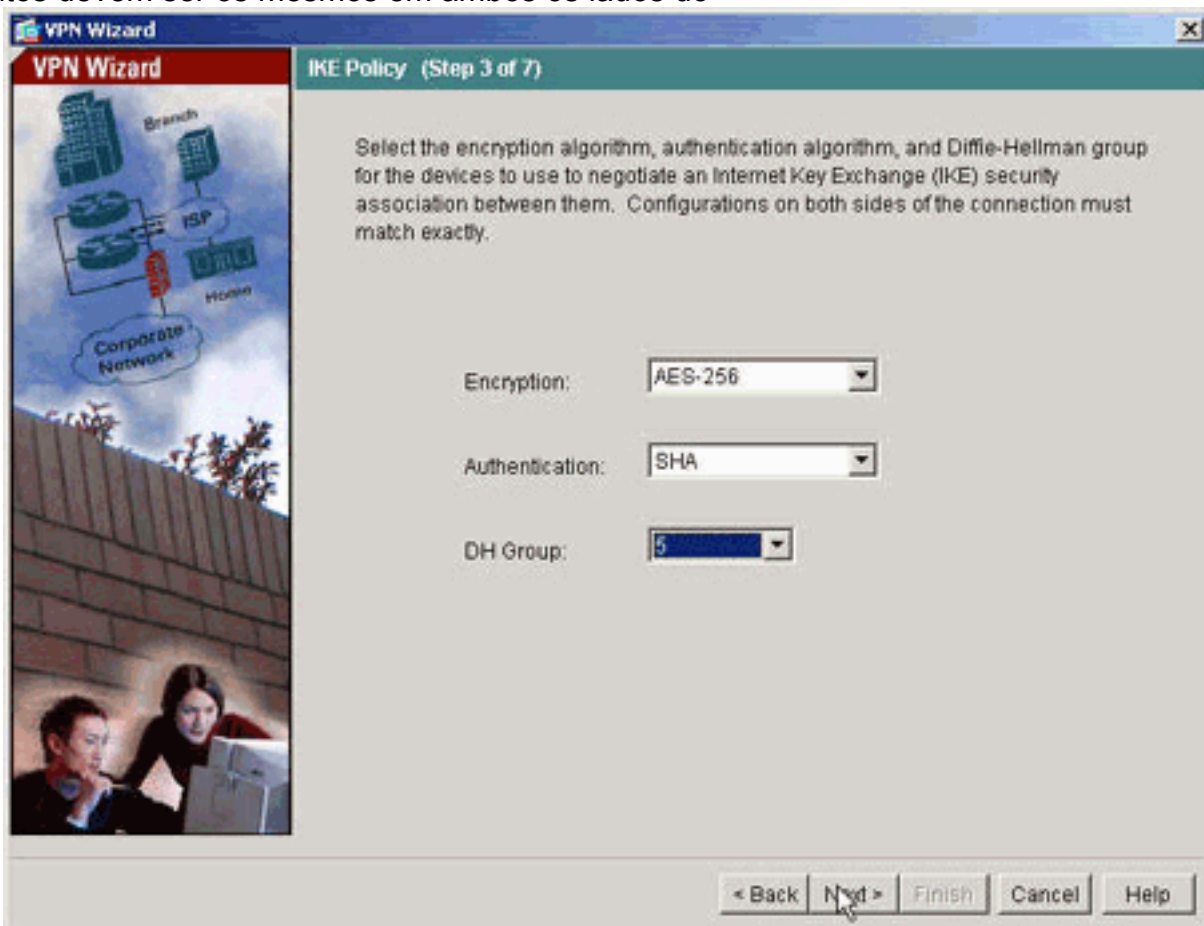
Site.

7. Especifique o endereço IP externo do peer remoto. Incorpore a informação da autenticação para usar-se (chave pré-compartilhada neste exemplo).



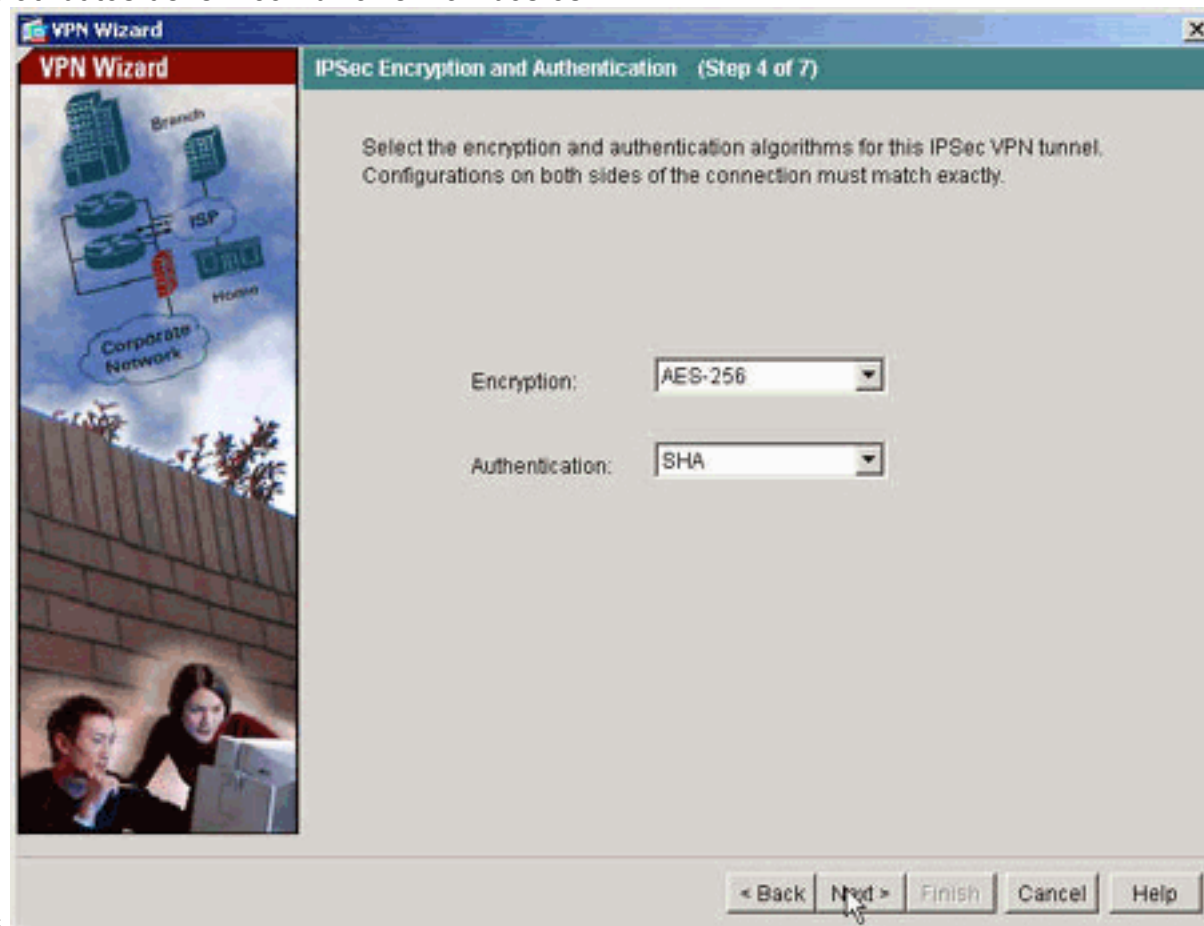
8. Especifique os atributos para usar-se para o IKE, igualmente sabido como a "fase 1". Estes

atributos devem ser os mesmos em ambos os lados do



túnel.

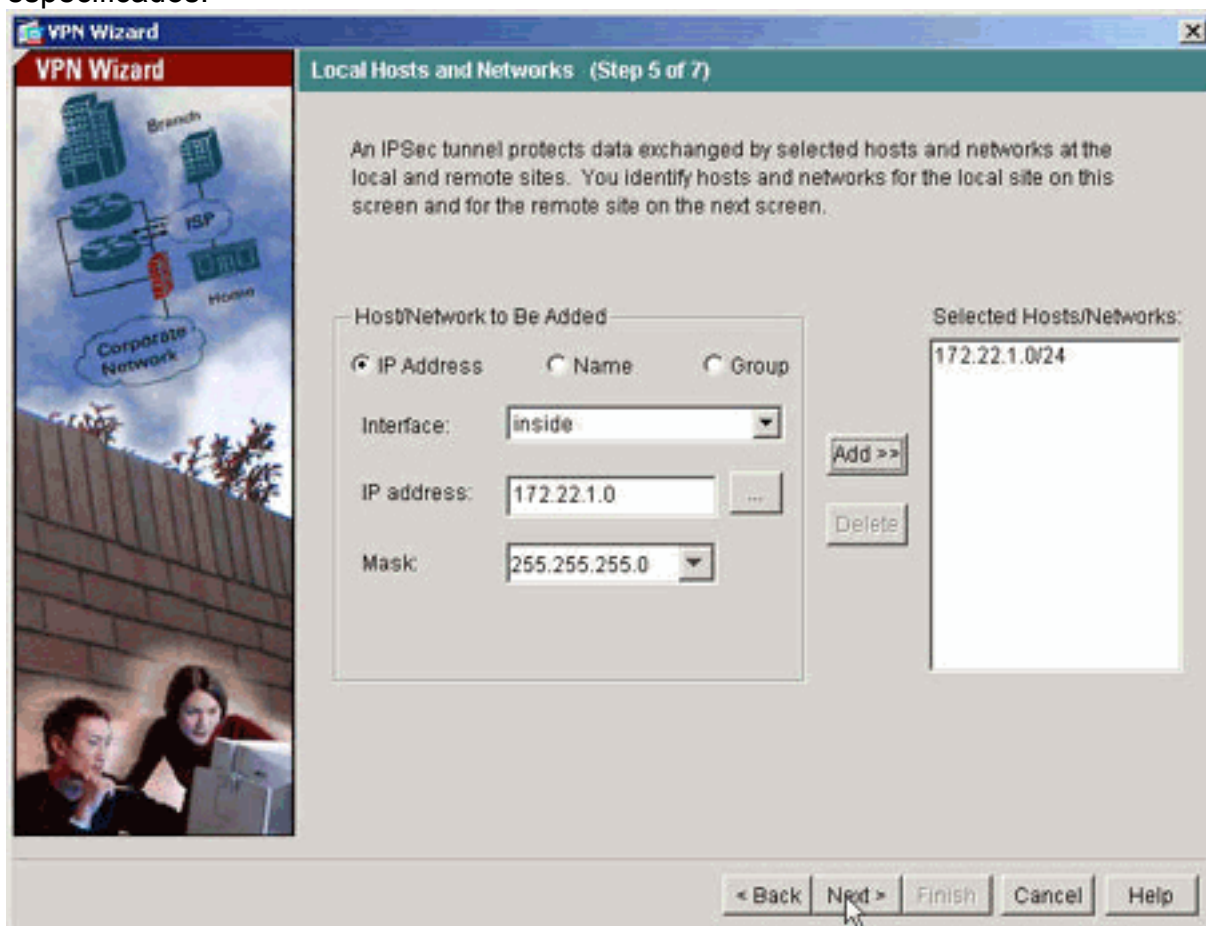
- 9. Especifique os atributos para usar-se para o IPsec, igualmente sabido como a "fase 2". Estes atributos devem combinar em ambos os



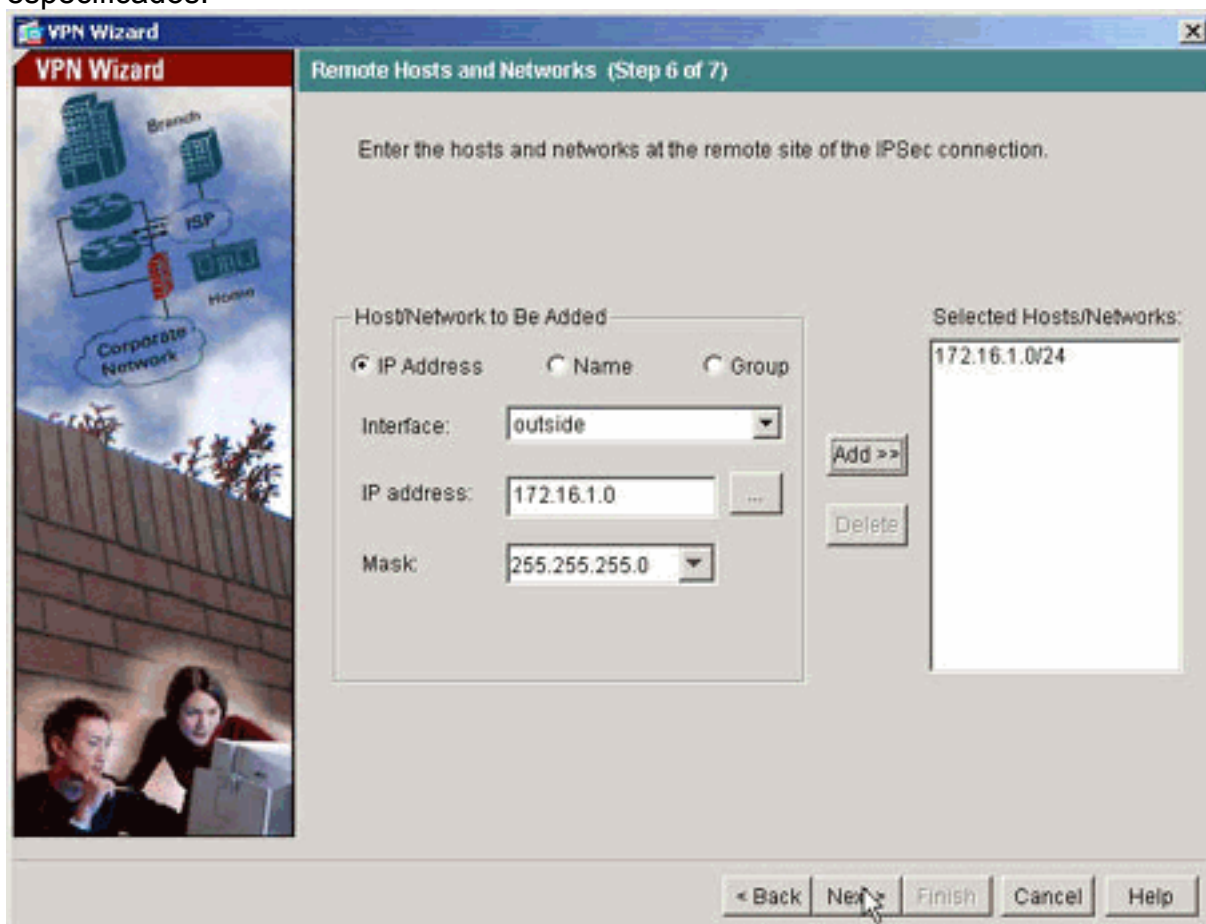
lados.

- 10. Especifique os anfitriões cujo o tráfego deve ser permitido passar através do túnel VPN.

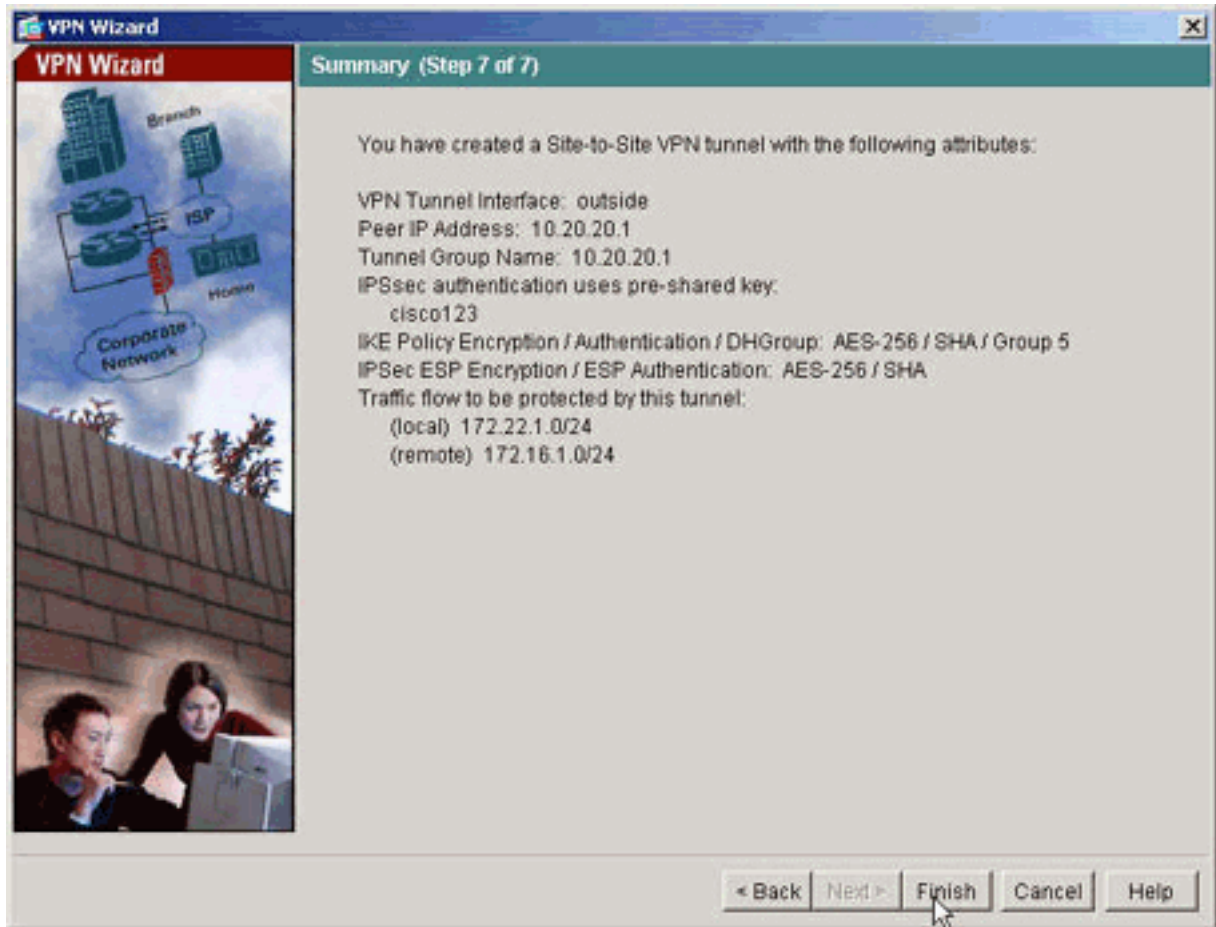
Nesta etapa, os anfitriões locais a pix515-704 são especificados.



11. Os anfitriões e as redes no lado remoto do túnel são especificados.



12. Os atributos definidos pelo wizard VPN são indicados neste sumário. Verifique novamente a configuração e clique o **revestimento** quando você é satisfeito os ajustes está correto.



Configuração de CLI PIX

pix515-704

```
pixfirewall#show run : Saved PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 ip
address 10.10.10.1 255.255.255.0 !--- Configure the
outside interface. ! interface Ethernet1 nameif inside
security-level 100 ip address 172.22.1.163 255.255.255.0
!--- Configure the inside interface. ! !-- Output
suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list inside_nat0_outbound
extended permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used with the nat zero
command. !--- This prevents traffic which matches the
access list from undergoing !--- network address
translation (NAT). The traffic specified by this ACL is
!--- traffic that is to be encrypted and !--- sent
across the VPN tunnel. This ACL is intentionally !---
the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration. access-list outside_cryptomap_20 extended
permit ip 172.22.1.0 255.255.255.0 172 .16.1.0
255.255.255.0 !--- This access list
(outside_cryptomap_20) is used with the crypto map !---
```

```

outside_map to determine which traffic should be
encrypted and sent !--- across the tunnel. !--- This ACL
is intentionally the same as (inside_nat0_outbound). !--
- Two separate access lists should always be used in
this configuration. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image flash:/asdm-511.bin
!--- Enter this command to specify the location of the
ASDM image. asdm history enable arp timeout 14400 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound. route outside 0.0.0.0 0.0.0.0
10.10.10.2 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 http server enable !---
Enter this command in order to enable the HTTPS server
for ASDM. http 172.22.1.1 255.255.255.255 inside !---
Identify the IP addresses from which the security
appliance !--- accepts HTTPS connections. no snmp-server
location no snmp-server contact !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. crypto ipsec transform-set ESP-AES-
256-SHA esp-aes-256 esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 20
match address outside_cryptomap_20 !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
peer crypto map outside_map 20 set transform-set ESP-
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
256-SHA" !--- to be used with the crypto map entry
"outside_map". crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- Policy 65535 is included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256 isakmp policy 10
hash sha isakmp policy 10 group 5 isakmp policy 10
lifetime 86400 isakmp policy 65535 authentication pre-
share isakmp policy 65535 encryption 3des isakmp policy
65535 hash sha isakmp policy 65535 group 2 isakmp policy
65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-
l2l !--- In order to create and manage the database of
connection-specific records !--- for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the tunnel-group !--- command
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer. tunnel-group 10.20.20.1 ipsec-
attributes pre-shared-key * !--- Enter the pre-shared-
key in order to configure the authentication method.
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic !! policy-map global_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
esmtplib inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end

```

```

PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
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 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on pix515-704. access-list
outside_cryptomap_20 extended permit ip 172.16.1.0
255.255.255.0 172 .22.1.0 255.255.255.0 !--- Note that
this ACL is a mirror of the outside_cryptomap_20 !---
ACL on pix515-704. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image flash:/asdm-511.bin
no asdm history enable arp timeout 14400 nat (inside) 0
access-list inside_nat0_outbound 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
http server enable http 0.0.0.0 0.0.0.0 inside no snmp-
server location no snmp-server contact crypto ipsec
transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20 crypto map outside_map 20 set peer
10.10.10.1 crypto map outside_map 20 set transform-set
ESP-AES-256-SHA crypto map outside_map interface outside
isakmp enable outside isakmp policy 10 authentication
pre-share isakmp policy 10 encryption aes-256 isakmp
policy 10 hash sha isakmp policy 10 group 5 isakmp
policy 10 lifetime 86400 tunnel-group 10.10.10.1 type
ipsec-l2l tunnel-group 10.10.10.1 ipsec-attributes pre-
shared-key * telnet timeout 5 ssh timeout 5 console
timeout 0 ! class-map inspection_default match default-
inspection-traffic !! policy-map global_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
esmtcp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:6774691244870705f858ad4e9b810874 : end
pixfirewall#

```

[Túnel de site para site alternativo](#)

A fim especificar o tipo de conexão para a característica de site para site alternativa para esta entrada do crypto map, use o comando **ajustado do tipo de conexão do crypto map** no modo de configuração global. Não use `nenhum` formulário deste comando a fim retornar à configuração padrão.

Sintaxe:

```
crypto map map-name seq-num set connection-type {answer-only | originate-only | bidirectional}
```

- **resposta-somente** — Isto especifica que este par responde somente às conexões de entrada IKE primeiramente durante a troca proprietária inicial a fim determinar o par apropriado a que para conectar.
- **bidirecional** — Isto especifica que este par pode aceitar e originar as conexões baseadas nesta entrada do crypto map. Este é o tipo de conexão padrão para todas as conexões de site para site.
- **origem-somente** — Isto especifica que este par inicia a primeira troca proprietária a fim determinar o par apropriado a que para conectar.

O comando **ajustado do tipo de conexão do crypto map** especifica os tipos de conexão para a característica alternativa do LAN para LAN. Permite que os pares do backup múltiplo sejam especificados em uma extremidade da conexão. Esta característica trabalha somente entre estas Plataformas:

- Duas ferramentas de segurança do 5500 Series de Cisco ASA
- Ferramenta de segurança do 5500 Series de Cisco ASA e um Cisco VPN 3000 Concentrator
- Ferramenta de segurança do 5500 Series de Cisco ASA e uma ferramenta de segurança que execute a versão de software 7.0 da ferramenta de segurança de Cisco PIX ou mais atrasado

A fim configurar uma conexão de LAN para LAN alternativa, Cisco recomenda que você configura uma extremidade da conexão como origem-somente com a palavra-chave da `origem-somente`, e a extremidade com os pares do backup múltiplo como a resposta-somente com a palavra-chave da `resposta-somente`. Na extremidade da origem-somente, use o **comando set peer do crypto map** a fim pedir a prioridade dos pares. A ferramenta de segurança da origem-somente tenta negociar com o primeiro par na lista. Se esse peer não responde, a ferramenta de segurança continua nos outros peers até que um peer responda ou até não houver mais peers na lista.

Quando configurado desta maneira, o par da origem-somente tenta inicialmente estabelecer um túnel proprietário e negociá-lo com um par. Depois disso, um ou outro par pode estabelecer uma conexão de LAN para LAN normal e os dados de uma ou outra extremidade podem iniciar a conexão de túnel.

Nota: Se você configurou o VPN com endereços IP de Um ou Mais Servidores Cisco ICM NT dos peer múltiplos para uma entrada cripto, o VPN obtém estabelecido com o IP do peer de backup uma vez que o peer principal vai para baixo. Contudo, uma vez que o peer principal volta, o VPN não cancela ao endereço IP primário. Você deve manualmente suprimir do SA existente a fim reinicie a negociação VPN para comutá-la sobre ao endereço IP primário. Enquanto a conclusão diz, o VPN cancela não está apoiado no túnel de site para site.

Tipos de conexão de LAN para LAN alternativos apoiados

Lado remoto	Lado central
Originate-Only	Answer-Only
Bi-Directional	Answer-Only

Bi-Directional	Bi-Directional
----------------	----------------

Exemplo

Este exemplo, incorporado ao modo de configuração global, configura o **mymap** do **crypto map** e ajusta o tipo de conexão *para originar-somente*.

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

[Cancele as associações de segurança \(os SA\)](#)

No modo do privilégio do PIX, use o seguinte os comandos:

- **clear [crypto] ipsec sa** — Suprime do IPSec ativo SA. As palavras-chave **crypto** são opcionais.
- **clear [crypto] isakmp sa** — Suprime do IKE ativo SA. As palavras-chave **crypto** são opcionais.

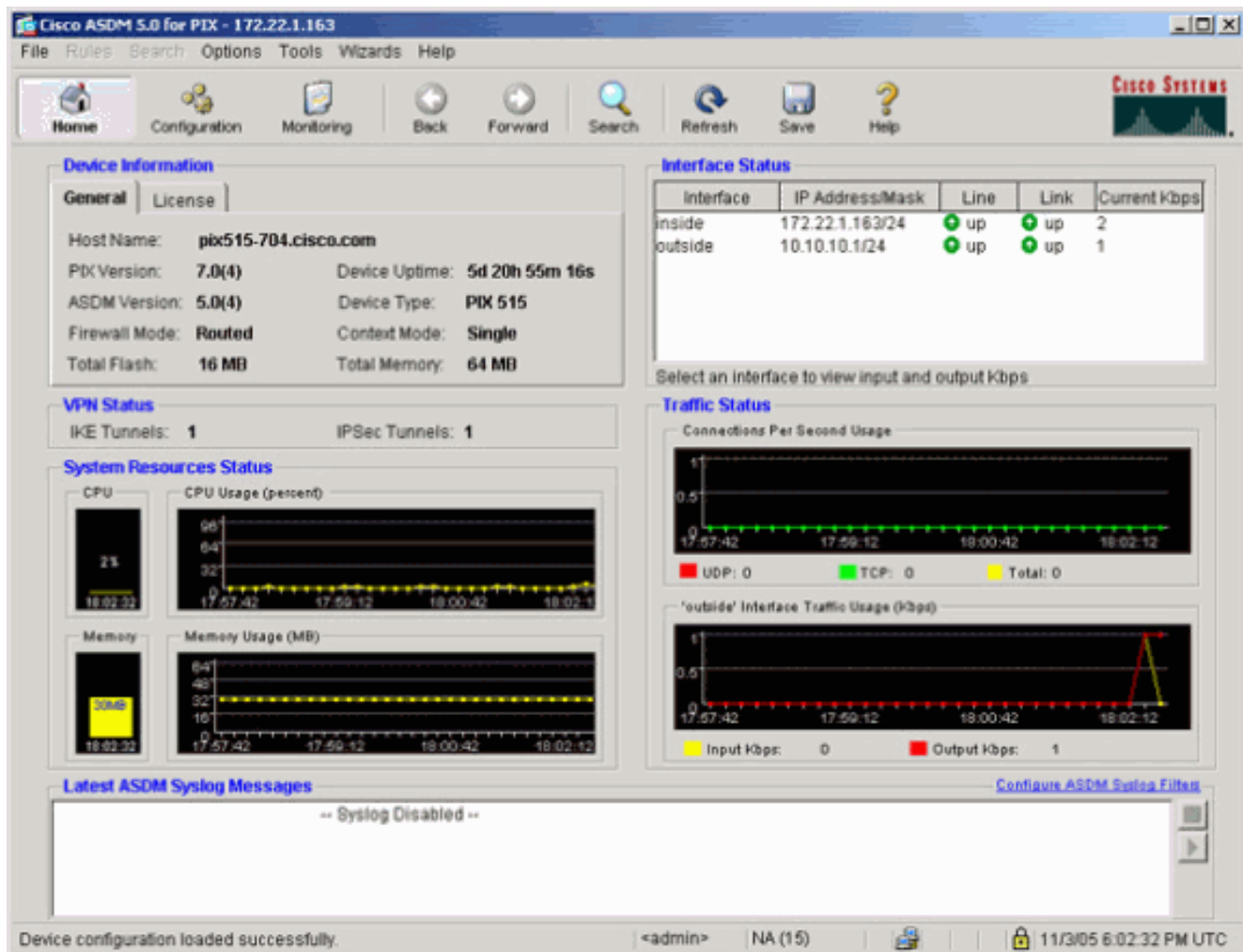
[Verificar](#)

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

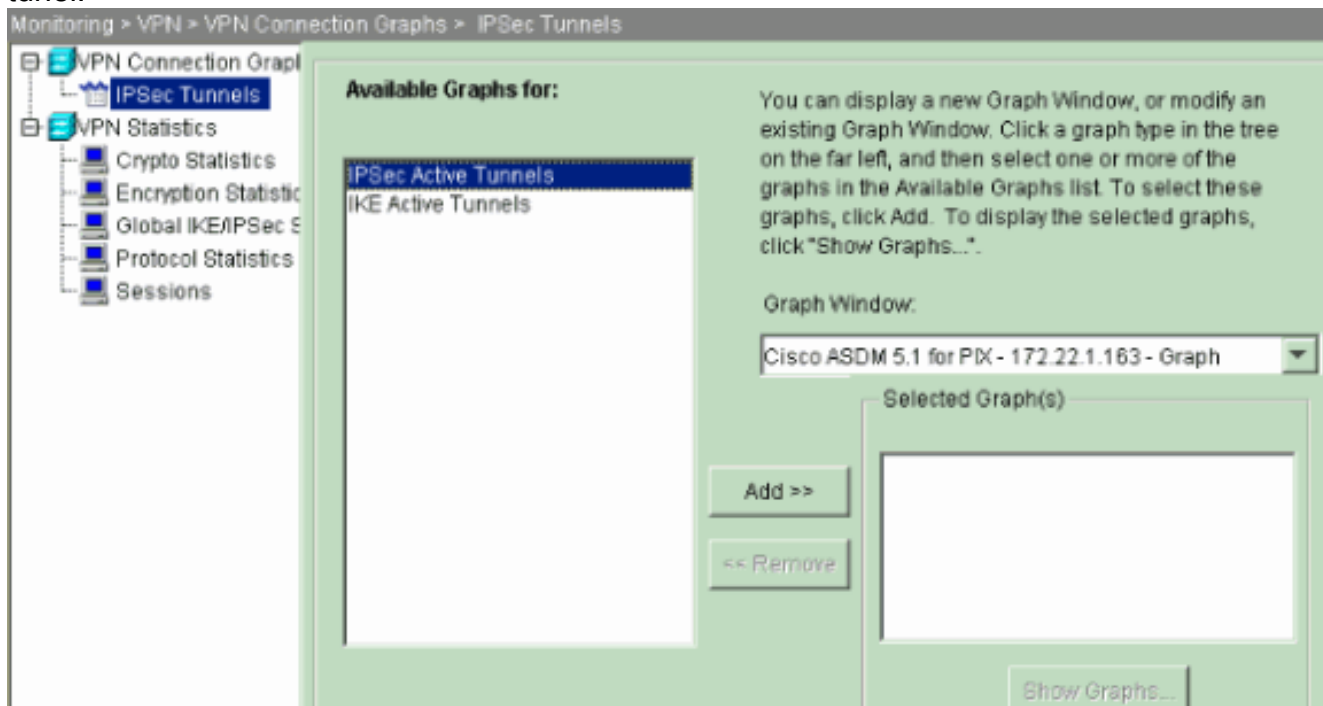
A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos **show**. Use a OIT para exibir uma análise da saída do comando **show**.

Se há um tráfego interessante ao par, o túnel está estabelecido entre **pix515-704** e **PIX-02**.

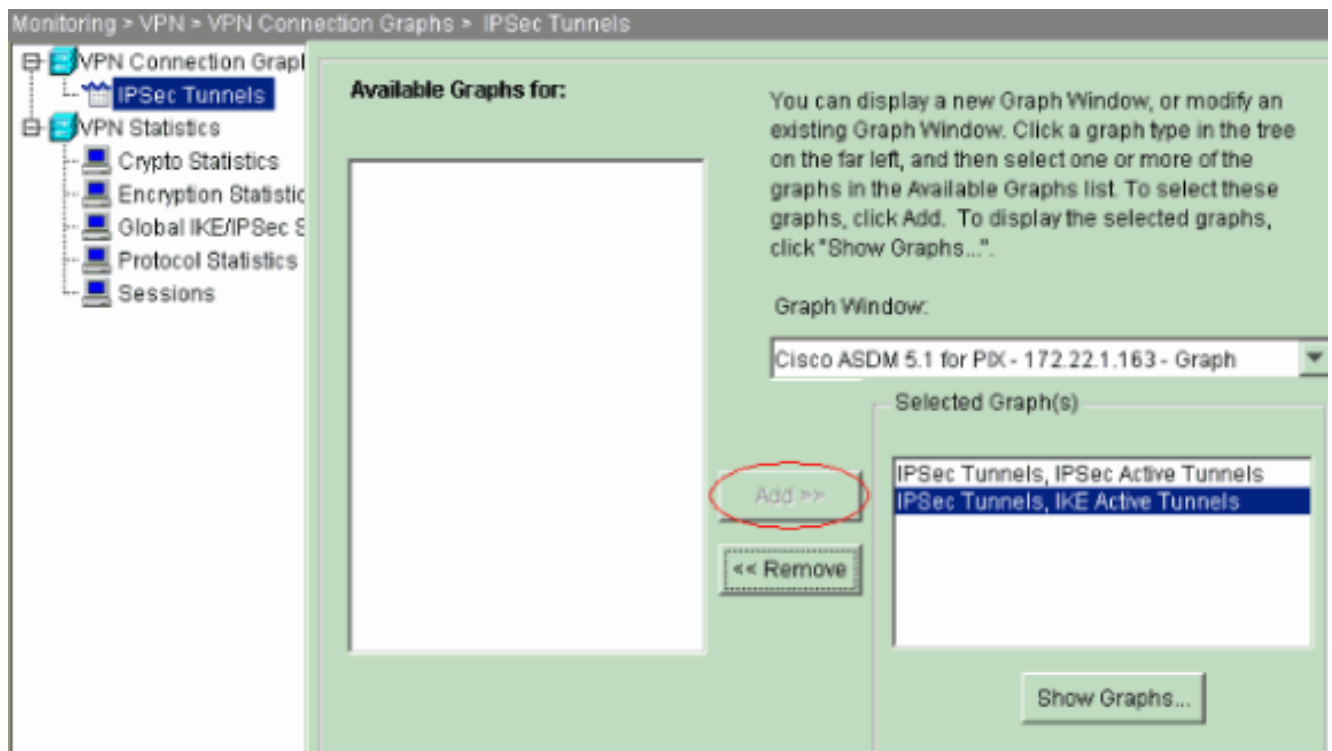
1. Veja o status VPN sob a **HOME** no ASDM a fim verificar a formação do túnel.



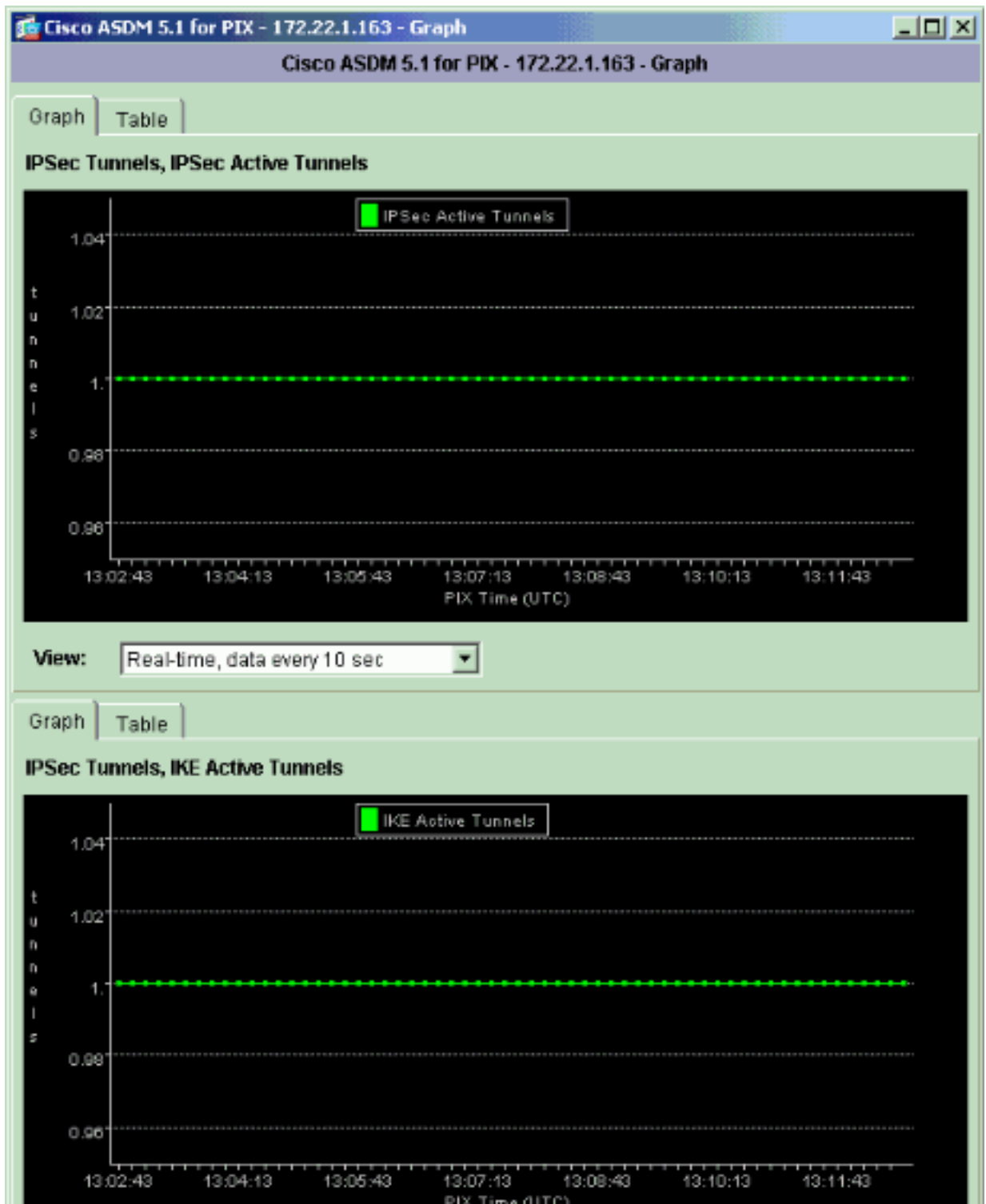
2. Escolha a **monitoração** > o **VPN** > a **conexão de VPN** representa graficamente > **túneis de IPsec** a fim verificar os detalhes sobre o estabelecimento de túnel.



3. O clique **adiciona** para selecionar os gráficos disponíveis a fim ver no indicador do gráfico.

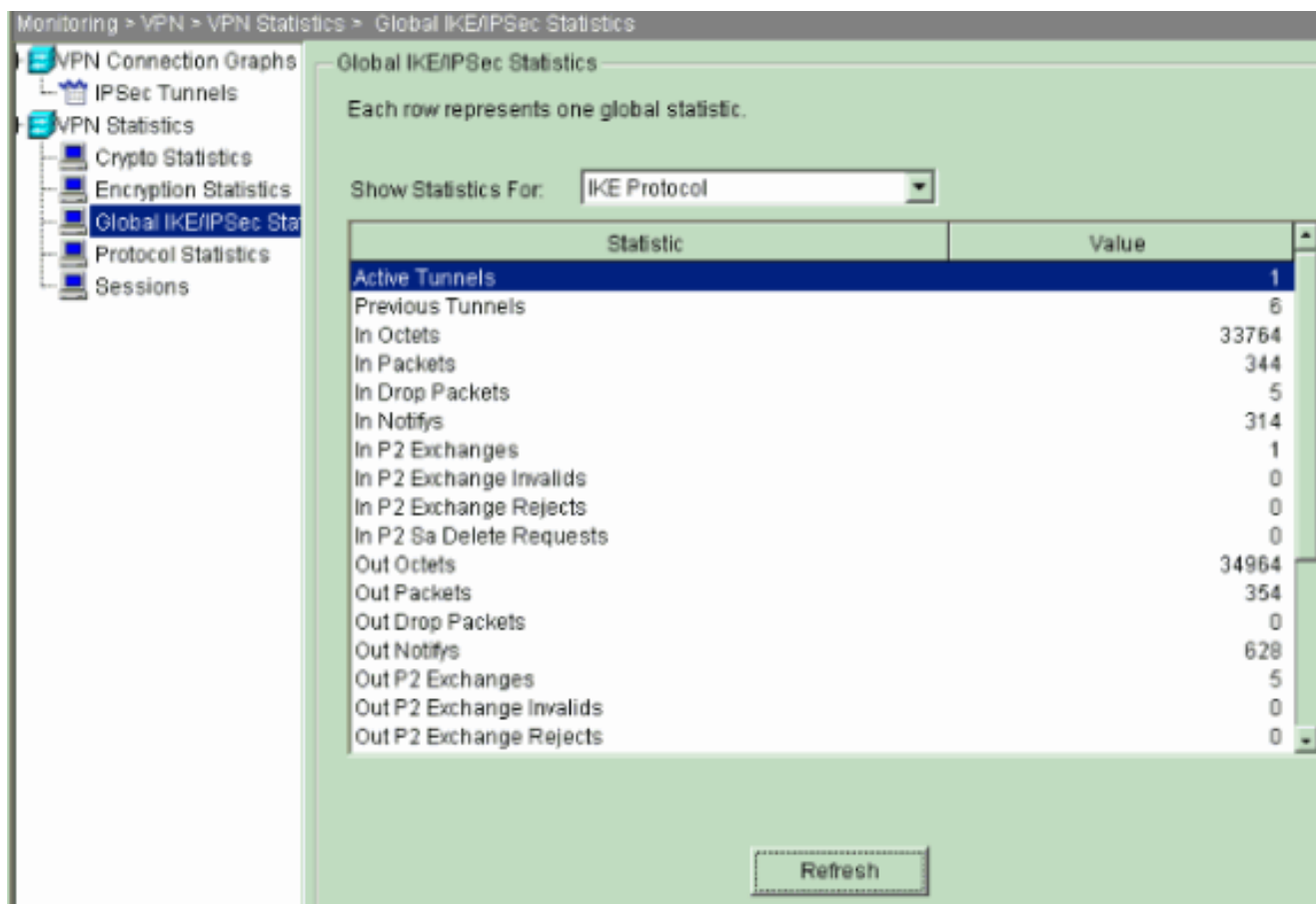


4. Clique **gráficos da mostra** a fim ver os gráficos de túneis ativo IKE e de



IPsec.

5. Escolha a monitoração > o VPN > as estatísticas de VPN > estatísticas globais IKE/IPSec a fim saber sobre a informação estatística do túnel VPN.



Você pode igualmente verificar a formação de túneis usando o CLI. Emita o comando **show crypto isakmp sa** para verificar a formação de túneis e emitir o comando **show crypto ipsec sa** para observar o número de pacotes encapsulados, cifrado, e assim por diante.

```

pix515-704
pixfirewall(config)#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: 10.20.20.1
Type : L2L Role : initiator Rekey : no State : MM_ACTIVE

pix515-704
pixfirewall(config)#show crypto ipsec sa interface:
outside Crypto map tag: outside_map, seq num: 20, local
addr: 10.10.10.1 access-list outside_cryptomap_20 permit
ip 172.22.1.0 255.255.255.0 172.16.1.0 255.255.255.0
local ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)
current_peer: 10.20.20.1 #pkts encaps: 20, #pkts
encrypt: 20, #pkts digest: 20 #pkts decaps: 20, #pkts
decrypt: 20, #pkts verify: 20 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 20, #pkts comp
failed: 0, #pkts decomp failed: 0 #send errors: 0, #rcv
errors: 0 local crypto endpt.: 10.10.10.1, remote crypto
endpt.: 10.20.20.1 path mtu 1500, ipsec overhead 76,
media mtu 1500 current outbound spi: 44532974 inbound
esp sas: spi: 0xA87AD6FA (2826622714) transform: esp-
aes-256 esp-sha-hmac in use settings = {L2L, Tunnel, }
slot: 0, conn_id: 1, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (3824998/28246) IV
size: 16 bytes replay detection support: Y outbound esp
sas: spi: 0x44532974 (1146300788) transform: esp-aes-256
esp-sha-hmac in use settings = {L2L, Tunnel, } slot: 0,
conn_id: 1, crypto-map: outside_map sa timing: remaining

```

```
key lifetime (kB/sec): (3824998/28245) IV size: 16 bytes
replay detection support: Y
```

Troubleshooting

PFS

Nas negociações de IPsec, o Perfect Forward Secrecy (PFS) garante que cada nova chave criptográfica não tenha relação com nenhuma chave anterior. Permita ou desabilite o PFS em ambos os tunnel peer, se não o túnel de IPsec L2L não é estabelecido no PIX/ASA.

O PFS é desabilitado por padrão. A fim permitir o PFS use o comando dos **pfs** com a palavra-chave da *possibilidade* no modo de configuração da grupo-política. 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
```

Acesso de gerenciamento

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

[A interface interna do PIX não poderá responder a pings enviados pela outra extremidade do túnel a menos que o comando management-access seja configurado no modo de configuração global.](#)

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access inside
```

Comandos debug

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

debug crypto isakmp — Exibe informações de depuração sobre conexões de IPSec e mostra o primeiro conjunto de atributos negados devido a incompatibilidades em ambas as extremidades.

debug crypto isakmp

```
pixfirewall(config)#debug crypto isakmp 7 Nov 27
12:01:59 [IKEv1 DEBUG]: Pitcher: received a key acquire
message, spi 0x0 Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE Initiator: New Phase 1, Intf 2, IKE Peer
10.20.20.1 local Proxy Address 172.22.1.0, remote Proxy
Address 172.16.1.0, Crypto map (outside map) Nov 27
12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing
ISAKMP SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP =
10.20.20.1, constructing Fragmentation VID + extended
capabilities payload Nov 27 12:01:59 [IKEv1]: IP =
10.20.20.1, IKE DECODE SENDING Message (msgid=0) with
payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total
```

length : 148 Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE DECODE RECEIVED Message (msgid=0) with payloads : HDR + SA (1) + VENDOR (13) + NONE (0) total length : 112
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing SA payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley proposal is acceptable Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Fragmentation VID Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer included IKE fragmentation capability flags : **Main Mode:** True Aggressive Mode: True Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing Cisco Unity VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing xauth V6 VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, constructing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send Altiga/ Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE SENDING Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE RECEIVED Message (msgid=0) with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 320 Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ke payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing ISA KE payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Cisco Unity client VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received xauth V6 VID Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing VPN3000/ASA spoofing IOS Vendor ID payload (version: 1.0.0, capabilities: 20000001) Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received Altiga/Cisco VPN3000/Cisco ASA GW VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating keys for Initiator... Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Constructing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing dpd vid payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 119 Nov 27

12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE RECEIVED Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE (14) + VENDOR (13) + NONE (0) total length : 96 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Computing hash for ISAKMP Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Processing IOS keep alive payload: proposal=32767/32767 sec. Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing VID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Received DPD VID Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection landed on tunnel group 10.20.20.1 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Oakley begin quick mode Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, **PHASE 1 COMPLETED** Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive type for this connection: DPD Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Starting phase 1 rekey timer: 73440000 (ms) Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, IKE got SPI from key engine: SPI = 0x44ae0956 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, oakley constucting quick mode Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing blank hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPsec SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing IPsec nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing proxy ID Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Transmitting Proxy Id: Local subnet: 172.22.1.0 mask 255.255.255.0 Protocol 0 Port 0 Remote subnet: 172.16.1.0 Mask 255.255.255.0 Protocol 0 Port 0 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, constructing qm hash payload Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE SENDING Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NOTIFY (11) + NONE (0) total length : 200 Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE DECODE RECEIVED Message (msgid=d723766b) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 172 Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing hash payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing SA payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing nonce payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, processing ID payload Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, loading all IPSEC SAs Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP = 10.20.20.1, Generating Quick Mode Key! Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, Security negotiation complete for LAN-to-LAN Group (10.20.20.1) Initiator, Inbound SPI = 0x44ae0956, Outbound SPI =

```
0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group =  
10.20.20.1, IP = 10.20.20.1, oakley constructing final  
quick mode Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1,  
IKE DECODE SENDING Message (msgid=d723766b) with  
payloads : HDR + HASH (8) + NONE (0) total length : 76  
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =  
10.20.20.1, IKE got a KEY ADD msg for SA: SPI =  
0x4a6429ba Nov 27 12:02:00 [IKEv1 DEBUG]: Group =  
10.20.20.1, IP = 10.20.20.1, Pitcher: received  
KEY UPDATE, spi 0x44ae0956 Nov 27 12:02:00 [IKEv1]:  
Group = 10.20.20.1, IP = 10.20.20.1, Starting P2 Rekey  
timer to expire in 24480 seconds Nov 27 12:02:00  
[IKEv1]: Group = 10.20.20.1, IP = 10.20.20.1, PHASE 2  
COMPLETED (msgid=d723766b)
```

debug crypto ipsec — Exibe informações de depuração sobre conexões de IPsec.

debug crypto ipsec

```
pixl(config)#debug crypto ipsec 7 exec mode  
commands/options: <1-255> Specify an optional debug  
level (default is 1) <cr> pixl(config)# debug crypto  
ipsec 7 pixl(config)# IPSEC: New embryonic SA created @  
0x024211B0, SCB: 0x0240AEB0, Direction: inbound SPI :  
0x2A3E12BE Session ID: 0x00000001 VPIF num : 0x00000001  
Tunnel type: 121 Protocol : esp Lifetime : 240 seconds  
IPSEC: New embryonic SA created @ 0x0240B7A0, SCB:  
0x0240B710, Direction: outbound SPI : 0xB283D32F Session  
ID: 0x00000001 VPIF num : 0x00000001 Tunnel type: 121  
Protocol : esp Lifetime : 240 seconds IPSEC: Completed  
host OBSA update, SPI 0xB283D32F IPSEC: Updating  
outbound VPN context 0x02422618, SPI 0xB283D32F Flags:  
0x00000005 SA : 0x0240B7A0 SPI : 0xB283D32F MTU : 1500  
bytes VCID : 0x00000000 Peer : 0x00000000 SCB :  
0x0240B710 Channel: 0x014A45B0 IPSEC: Completed outbound  
VPN context, SPI 0xB283D32F VPN handle: 0x02422618  
IPSEC: Completed outbound inner rule, SPI 0xB283D32F  
Rule ID: 0x01FA0290 IPSEC: New outbound permit rule, SPI  
0xB283D32F Src addr: 10.10.10.1 Src mask:  
255.255.255.255 Dst addr: 10.20.20.1 Dst mask:  
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore  
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use  
protocol: true SPI: 0xB283D32F Use SPI: true IPSEC:  
Completed outbound permit rule, SPI 0xB283D32F Rule ID:  
0x0240AF40 IPSEC: Completed host IBSA update, SPI  
0x2A3E12BE IPSEC: Creating inbound VPN context, SPI  
0x2A3E12BE Flags: 0x00000006 SA : 0x024211B0 SPI :  
0x2A3E12BE MTU : 0 bytes VCID : 0x00000000 Peer :  
0x02422618 SCB : 0x0240AEB0 Channel: 0x014A45B0 IPSEC:  
Completed inbound VPN context, SPI 0x2A3E12BE VPN  
handle: 0x0240BF80 IPSEC: Updating outbound VPN context  
0x02422618, SPI 0xB283D32F Flags: 0x00000005 SA :  
0x0240B7A0 SPI : 0xB283D32F MTU : 1500 bytes VCID :  
0x00000000 Peer : 0x0240BF80 SCB : 0x0240B710 Channel:  
0x014A45B0 IPSEC: Completed outbound VPN context, SPI  
0xB283D32F VPN handle: 0x02422618 IPSEC: Completed  
outbound inner rule, SPI 0xB283D32F Rule ID: 0x01FA0290  
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F  
Rule ID: 0x0240AF40 IPSEC: New inbound tunnel flow rule,  
SPI 0x2A3E12BE Src addr: 172.16.1.0 Src mask:  
255.255.255.0 Dst addr: 172.22.1.0 Dst mask:  
255.255.255.0 Src ports Upper: 0 Lower: 0 Op : ignore  
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 0 Use
```

```
protocol: false SPI: 0x00000000 Use SPI: false IPSEC:
Completed inbound tunnel flow rule, SPI 0x2A3E12BE Rule
ID: 0x0240B108 IPSEC: New inbound decrypt rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound decrypt rule, SPI 0x2A3E12BE Rule ID:
0x02406E98 IPSEC: New inbound permit rule, SPI
0x2A3E12BE Src addr: 10.20.20.1 Src mask:
255.255.255.255 Dst addr: 10.10.10.1 Dst mask:
255.255.255.255 Src ports Upper: 0 Lower: 0 Op : ignore
Dst ports Upper: 0 Lower: 0 Op : ignore Protocol: 50 Use
protocol: true SPI: 0x2A3E12BE Use SPI: true IPSEC:
Completed inbound permit rule, SPI 0x2A3E12BE Rule ID:
0x02422C78
```

Informações Relacionadas

- [Criação de túnel redundante entre Firewall usando o PDM](#)
- [Cisco PIX Firewall Software](#)
- [Cisco Adaptive Security Device Manager](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [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](#)