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** Convencões **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 Limpando 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.

Note: 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 <u>verificação da operação de NAT e do Troubleshooting de NAT básico</u> ou <u>como o NAT trabalha</u>.

Note: 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 <u>transparência de NAT de IPSec</u>. Refira o <u>apoio para o</u> <u>IPsec ESP com o NAT</u> a fim aprender mais sobre estas características no Cisco IOS Software Release 12.2(13)T e Mais Recente.

Note: Antes que você abra um caso com Suporte técnico de Cisco, refira <u>perguntas mais</u> <u>frequentes de NAT</u>, que tem muitas respostas às perguntas comum.

Refira <u>configurar um túnel de IPsec com um Firewall com o NAT</u> 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 <u>transparência de NAT de IPSec</u>.
- 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 <u>Convenções de Dicas Técnicas da Cisco</u> 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.

<u>Configurar</u>

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

características este documento descreve.

Note: 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:





Este documento utiliza as seguintes configurações:

- Configuração do Cisco 2621
- <u>Configuração do Cisco 3660</u>
- 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:
1
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-2621
1
ip subnet-zero
 !
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
1
!--- 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
1
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
1
controller T1 1/0
1
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 1
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
1
```

```
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
1
no scheduler allocate
end
Cisco 3660
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
1
hostname goss-3660
!
ip subnet-zero
!
cns event-service server
1
!--- 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
 Т
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
1
!--- 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
1
!--- 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
0.0.255
access-list 110 permit ip 10.3.3.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
1
line con 0
 transport input none
line aux 0
line vty 0 4
1
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 ADSM (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 <u>configuração construída a mão ASDM do PIX Firewall</u>.
- 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.

| Gisco ASDM 5.0 for PTX - 10.1.1.1 File Rules Bearch Options Tools Wizards Help | |
|---|---|
| Configuration Monitoring Back Forward Search | ch Refresh Seve Help |
| Device Information | Interface Status |
| General License | Interface IP Address/Mask Line Link Current Kops |
| Host Name pixfirewall.cisco.com | inside 10.1.1.1/24 Oup Oup 1 |
| P0(Version: 7.0(0)102 Device Uptime: 0d 0h 3m 53s | |
| ASDM Version: 5.0(0)73 Device Type: PIX 515E | |
| Firewall Mode: Routed Context Mode: Single | |
| Total Flash: 16 MB Total Memory: 64 MB | Select an interface to view input and output Kops |
| VPN Status | Traffic Status |
| IKE Tunnels: 0 IPSec Tunnels: 0 | Connections Per Second Usage |
| System Resources Status | 4 |
| CPU Usage (percent) | 0.9* |
| 00 54 | 10.20:18 |
| 0% 32 | UDP: 0 TCP: 0 Total: 0 |
| 10.20.28 10:20:18 | 'inside' Interface Traffic Usage (Kbps) |
| Memory — Memory Usage (MB) | 21 |
| 84 | 1.9 c |
| 20.8 | |
| 16:20:28 15:20:18 | Input Kaps: 0 Output Kaps: 1 |
| Latest ASDM System Messages | Configure ASDII Suslog Filters |
| Syslog Disabled | |
| | 4 |
| | |
| | |
| Device configuration loaded successfully. | admin> NA (15) |

6. Destaque a **relação do ethernet0** e o clique **edita** a fim configurar a interface externa.

| Cisco ASDM 5 File Rules Ba | .0 for PD satch - C | X - 10.1.1.1 Infions Thols Wizards | Hein | | | | | | _O X |
|--|------------------------|---------------------------------------|---------------|------------|-------------------|-------------------|-------------------|------------------------|---------------------|
| Home | onfigur | ation Monitoring E | Co Back Fo | Orward | Q Search | Refresh : | Save Help | | Cesco Systems |
| Features | Config | uration > Features > Interfa | ces | | | | | | |
| Interfaces | 1 4 5 | £≆ ⊠ ∐ ≯⊅ | | ୍ୟାଙ୍କା | | | | | |
| в. | | Interface | Name | Enabled | Security Level | IP Address | Subnet Mas | k Management M Only | TU Add |
| Security Policy | Ett | hernet1 | inside | Yes | 100 | 10.1.1.1 | 255.255.255.0 | No 150 | Edit |
| in the second se | Ett | hernetü | | No | | | | No | Delete |
| NAT | | | | | | | | | |
| VPN | | | | | | | | | |
| 423 Routing | | | | | | | | | |
| Building Blocks | | | | | | | | | |
| Device Administration | | | | | | | | | |
| Froperties | | | | | | | | | • |
| | | Enable traffic between two | or mare int | erfaces wi | hich are c | onfigured with sa | me security level | 5 | |
| | | | | | Access of | | | | |
| Wizards / | | | | | Abbilit | Re | iset | | |
| | | | | | | admin> NA | (15) | 🖗 🔓 341 | 5/05 4:26:49 PM UTC |

7. APROVAÇÃO do clique na alerta da relação da





8. Incorpore os detalhes da relação e clique a **APROVAÇÃO** quando você é feito.

| 💼 Edit Interface | | X |
|--------------------|------------------------------------|-------------------------------|
| Hardware Port: | EthernetO | Configure Hardware Properties |
| 🔽 Enable Interface | 🗖 Dedicate this interface to manag | jement only |
| | | |
| Interface Name: | outside | |
| Security Level: | 0 | |
| - IP Address | | |
| O Use Static IP | C Obtain Address via DHCP | |
| | | |
| IP Address: | 99.99.99.1 | |
| Subnet Mask: | 255.255.255.0 | |
| | | |
| MTU: | 1500 | |
| | | |
| Description: | | |
| | | |
| | OK Cancel | Help |
| | | |

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.

| Eisco ASDM 5 File Rules Bi | i.O fo sarch | PTX - 10.1.1.1 Options Tool | s Wizards | Help | | | | | | | | _ 🗆 🛛 |
|-------------------------------|-----------------|--------------------------------|----------------|--------------|------------|-------------------|-------------------|--------------|------------------|--------------------|---------|----------------|
| G Home | Conf | aguration Mont | toring | O Back Fi | Orward | Q Search | Refresh | Serve | ? Help | | | CISCO SYSTEMS |
| Features | Ce | nfiguration > Fea | tures > Interf | aces | - A- | | _ | | | _ | | |
| , Interfaces | | ·≗ ≉ ⊠ | TIY AN | 10. 10. 10 | 51691 | | | | | | | |
| <u>e</u> . | | Interfa | ice | Name | Enabled | Security Level | IP Address | Su | bnet Mask | Management Only | MTU | Add |
| Security Policy | | Ethernet1 | | Inside | Yes | 100 | 10.1.1.1 | 255.2 | 255.255.0 | No | 1500 | Edit |
| NAT. | | Ethernetü | | outside | Yes | 0 | 99.99.99.1 | 265.2 | 255.255.0 | No | 1500 | Delete |
| | | | | | | | | | | | | |
| 423 Routing | | | | | | | | | | | | |
| Building Blocks | | | | | | | | | | | | |
| Device Administration | | | | | | | | | | | | |
| Properties | | ×[| | | | | | | | | • | |
| | | 🗆 Enable traffic | between two | or more int | erfaces wi | hich are c | onfigured with s | ame ser | urity levels | | | |
| | | | | | | Apply | R | eset | 1 | | | |
| Wizards - ^ | | | | | | | | | | | | |
| | | | | | | | <admin> N</admin> | A (15) | | | 3/16/05 | 4:28:18 PM UTC |

11. Clique o **roteamento** sob as características aba, destaque a **rota estática**, e o clique **adiciona**.

| Eisco ASDM 5. File Rulas Be | 0 for PTX - 10.1.1.1 arch Options Tools Wizari | ds Help | | | | _ 🗆 × |
|--------------------------------|---|---------------------------|-----------------|--------------|-----------------|------------------------|
| di Home d | Configuration Monitoring | Back Forward | Q Refres | h Save I | ? Нар | CISCO SYSTEMS |
| Features | Configuration - Features - R | outing > Routing > Statio | Route | Gateway IP I | Metric Turneled | Add Edit Delete |
| | | | <admin></admin> | NA (15) | 1 🖉 🔂 🛛 👌 | 3/16/05 4:44:48 PM UTC |

12. Configurar o gateway padrão e clique a

| | 🔂 Add Static Route | | × |
|------------|--------------------|---------------------------|---|
| | Interface Name: | outside | |
| | IP Address: | 0.0.0.0 | |
| | Mask: | 0.0.0.0 | |
| | Gateway IP: | 99.99.99.2 | |
| | Metric | 1 | |
| | C Tunneled (Use | d only for default route) | |
| APROVAÇÃO. | ок | Cancel Help | |

13. O clique adiciona e adiciona as rotas às redes



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 ΝΔΤ

| 🔁 Cisco ASDM 5.1 | 0 for PI | X - 10.1.1 | 1.1 | | | | | | | _0× |
|--------------------------|----------------|------------------------------|-------------|---------|----------------------|---------|-----------------------|-----------------|-----------------|-----------------|
| File Rules Se | arch C | Options | Tools | Wizards | s Help | | | | | |
| Home C | je Sonfigur |) ration | Monitorin | 0 | Back Forwa | rol S | Q Q Search Refresh | Save Help | | Cisco Systems |
| Features | Config | guration = | Feature | is > NA | T > Translation Ru | les | | | | |
| | ٠. | 新売!! | 1 D | 188 | | <u></u> | | | | |
| Interfaces | | Enable t | raffic thru | ough th | e firewall without a | address | translation | | | |
| <u>ě</u> , | • | Translat | ion Rule | 5 | C Translation | n Exemp | tion Rules | | | |
| Security Policy | 8 | how Rule | s for Inte | arface: | All Interfaces | | ▼ Show All | | | |
| NAT | [| Rule | | | Origi | nal | | | Translated | Add |
| <u>8</u> | | Туре | Interfa | ce | Source Netwo | ark | Destination Network | Interface | Address | Edit |
| 43b | | | | | | | | | | Delete |
| Routing | | | | | | | | | | |
| 8 8 | | | | | | | | | | |
| Building Blocks | | | | | | | | | | |
| Device Administration | | | | | | | | | | |
| 2 | | | | | | | | | | |
| Properties | | | | | | | | | | 4 |
| | 1 | Static I | JAT | -88 D | mamic NAT | 🕼 Stati | : Policy NAT 🛛 🖓 (| Marnic Policy N | AT Managa Poole | 1 |
| | | | | | | Г | | | I Nullage Pools | |
| Winorda | | | | | | L | Арріу | Reset |] | |
| wizarus < | 1 | | | | | | Londminn IN | A (15) | | 4-24-40 RM LITE |
| | | | | | | | sauriiris N | A(13) | 🔄 🖸 📔 📄 🖓 🔤 | 4.31:48 PM OTC |

16. Configurar a rede da fonte (este exemplo usa). Clique então controlam associações a fim definir a

PANCADINHA.

| Add Address | Translation R | ule | | | | | | |
|-------------|----------------|------------------------------------|------------------------------|------------|--------|---------|-------------|---|
| Use NA | л си | Ise Policy NAT | | | | | | |
| -Source H | ost/Network- | | | | | | | _ |
| | | Interface: IP Address: Mask: | inside 0.0.0.0 0.0.0.0 | | • • | | | |
| | | | Browse | | | | | |
| | | | | | | | NAT Options | |
| Translate A | ddress on Inte | rface: outsid | ie 🔻 | | | | | |
| — Translate | Address To | | | | | | | |
| C ala | Ptotic | IR Address: | | | 7 | | | |
| 0.1 | Redirects | ne Audress. port | 1 | <u> </u> | | | | |
| | © TCP © UDP | Original port: | | Translated | port: | | | |
| • 1 | Dynamic | Address Pool: | same addre | ss 🔻 | Manag | e Pools | | |
| | Pool ID | | Add | ress | | | | |
| | N/A | No address poo | ol defined | | | | | |
| | | | | | | | | |
| | , | | | | | | | |
| | | | | | | | | |
| | | 0K | Cance | | Help | | | |

17. Selecione a **interface externa** e o clique **adiciona**.

| 🚰 Manage Global Ade | dress Pools | | | | | | × |
|---------------------------------|---------------|-----------|-----------------|--------------|------------|----------|---|
| Global Address P | ools | | | | | | |
| Global Address Po addresses. | ools are used | to config | ure Dynamic Net | work Address | Translatio | on (NAT) | |
| Interface | Pool ID | | IP Addres | s(es) | | | |
| inside outside | | | | | _ | Add | |
| | | | | | | Edit | |
| | | | | | | Delete | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | 1 | | 1 | 1 | | |
| | 0K | | Cancel | He | lp | | |

Este exemplo usa uma PANCADINHA usando o endereço IP de Um ou Mais Servidores Cisco ICM NT da relação.

| 🚰 Add Global Pool Item | × |
|--|---|
| Interface: outside 💌 Pool ID: 1 | |
| O Range | |
| C Port Address Translation (PAT) | |
| Port Address Translation (PAT) using the IP address of the interface | |
| | |
| IP Address: | |
| Network Mask (optional): | |
| OK Cancel Help | |
| | |

18. APROVAÇÃO do clique quando a PANCADINHA for configurada.

| 🚰 Manage Global Ado | iress Pools | | | | | × |
|---------------------------------|---------------|-----------|---------------------|-------------------|--------------|---|
| Global Address P | ools | | | | | |
| Global Address Po addresses. | ools are used | to config | jure Dynamic Netw | ork Address Trans | lation (NAT) | |
| Interface | Pool ID | | IP Address(| es) | | |
| inside outside | 1 | 99.99.99 | 3.1 (interface PAT) | | Add | |
| | | | | | Edit | |
| | | | | | Delete | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | ок | | Cancel | Help | | |

19. O clique **adiciona** a fim configurar a tradução estática.

| 🔁 Add Address 1 | Translation R | ule | | | × |
|-----------------|----------------|--------------------|----------------|---------------|-------------|
| Use NAT | r Cu | se Policy NAT | | | |
| Source Ho | st/Network— | | | | |
| | | Interface: | inside | • | |
| | | IP Address: | 0.0.0.0 | | |
| | | Mask | 0.0.0.0 | Ŧ | |
| | | | Browse | | |
| | | | | | NAT Options |
| Translate Ad | idress on Inte | rface: outsid | ie 💌 | - | |
| Translate | Address To — | | | | |
| C III | Static | IP Address: ort | | * | |
| | C UDP | Original port: | Translate | i port: | |
| • 📲 | Dynamic | Address Pool: | same address 💌 | Manage Pools. | |
| | Pool ID | | Address | | |
| | 1 | 99.99.99.1 (inter | face PAT) | | |
| | | | | | |
| | | | | | |
| | | ок | Cancel | Help | |

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.

| 🕵 Add Address Tra | anslation R | ule | | | | x |
|-------------------|--------------|----------------|------------------|--------------|-------------|---|
| Use NAT | ΟU | se Policy NAT | | | | |
| -Source Host | /Network- | | | | | |
| | | | | | | |
| | | Interface: | inside | • | | |
| | | IP Address: | 10.1.1.2 | _ | | |
| | | Mask: | 255 255 255 255 | - | | |
| | | | 1200.200.200.200 | | | |
| | | | Browse | | | |
| | | | | | NAT Options | |
| Translate Addr | ess on Inter | face: outsid | e 🔻 | | | |
| — Translate Ad | dress To | | _ | | | |
| G 11 9 | Itatic | ID Address: | 00.00.00.12 | - | | |
| | Redirect p | ort | 33.33.33.12 | <u> </u> | | |
| | C TCP | Original port: | Translate | d port: | | |
| | CUDP | | | | | |
| o ¶1 c |)ynamic | Address Pool: | same address 💌 | Manage Pools | | |
| | Pool ID | | Address | | 1 | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | Г | | 1 | | | |
| | _ | OK | Cancel | Help | | |

 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.

| 🖆 Add Access Rule | x | | | | | | | |
|--|-----------------------------|--|--|--|--|--|--|--|
| Action | - Syslog | | | | | | | |
| Select an action: permit | Default Syslog More Options | | | | | | | |
| Apply to Traffic: incoming to src interface | Time Range Not Applied New | | | | | | | |
| Source Host/Network | Destination Host/Network | | | | | | | |
| | ⑦ IP Address C Name C Group | | | | | | | |
| Interface: outside | Interface: Inside | | | | | | | |
| IP address: 99.99.99.2 | IP address: 99.99.99.12 | | | | | | | |
| Mask: 255.255.255 💌 | Mask. 255.255.255.255 💌 | | | | | | | |
| 99.99.99.2 Allow traffic | | | | | | | | |
| Protocol and Service | | | | | | | | |
| C TCP C UDP C ICMP C IP | Manage Service Groups | | | | | | | |
| IP protocol: esp | | | | | | | | |
| Please enter the description below (optional): | | | | | | | | |
| Access Rule to Allow ESP traffic | * | | | | | | | |
| OK Car | ncel Help | | | | | | | |

24. O clique **adiciona** a fim permitir que o tráfego ISAKMP e a **APROVAÇÃO do** clique a fim continuar.

| Edit Access Rule | |
|---|--|
| Action | Syslog |
| Select an action: permit | Default Syslog More Options |
| Apply to Traffic: incoming to src interface | Time Range Not Applied New |
| Source Host/Network | Destination Host/Network |
| | IP Address C Name C Group |
| Interface: Outside | Interface: Inside 💌 |
| IP address: 99.99.99.2 | IP address: 99.99.99.12 |
| Mask: 255.255.255.255 | Mask: 255.255.255.255 |
| 99.99.99.2 outside | 99.99.99.12 |
| Protocol and Service | |
| C TCP C UDP C ICMP C IP Source Port | Manage Service Groups Destination Port Service = any |
| C Service Group | C Service Group |
| Please enter the description below (optional): | |
| Access Rule to allow ISAKMP to host 99.99.99.12 | * |
| ОК Са | ancel Help |

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.

| Edit Access Rule | |
|--|---|
| Action | Syslog |
| Select an action: permit | Default Syslog More Options |
| Apply to Traffic: incoming to src interface | Time Range Time Range: Not Applied INew |
| Source Host/Network | Destination Host/Network |
| | |
| Interface: Outside | Interface: inside |
| IP address: 99.99.99.2 | IP address: 99.99.99.12 |
| Mask: 255.255.255 💌 | Mask: 255.255.255.255 💌 |
| Rule applied to traffic incoming to autiside 99.99.99.2 Allow to | a source interface |
| Protocol and Service | |
| C TCP © UDP C ICMP C IP Source Port © Service = 14500 © Service Group | Manage Service Groups Destination Port Service = any Service Group |
| Please enter the description below (optional): | |
| Access Rule to allow 4500 to host 99.99.99.12 | A. * |
| ОК Са | ncel Help |

26. O clique **aplica-se** a fim aceitar a configuração da interface. A configuração igualmente obtém empurrada no PIX.

| File Rules Search Options Tools Wizards Help | | | | | | | | | | | | |
|--|--|-----------------|---------------|--------------------|--------------|------------------|--------------------|------------------------|--------------|--------------|-------------------|-------------|
| Home C | onfigura | tion Mo |) nitoring | C Beck | O Forward | Q Search | Refresh | Seve | ? Help | | Ces t | CO SYSTEMS |
| Features | Configu | ration > Fe | atures > | Security Policy | > Access R | lules | | | | | | |
| | * * | ¥ 🗹 | 1 | 6 B 🗈 🔂 | ñ 🖇 🛛 | | | | | | | |
| Nerfaces | Ac Ac Ac Ac | cess Rule | s CA | AA Rules C | Filter Rule: | s 🔿 Sen | rice Policy R | ules | | | | |
| | Show | Rules for I | nteríace | All Interfaces | • | Show All | | | | | | |
| Security Policy | # | Rule Enabled | Action | Source HostiNet | Work | Dest Host | ination Network | Rule App To Traffic | lied 1 | nterface | Service | Add |
| NAT | | N | ¥ | 🍳 any | | 🧼 any | | | insi (out | de bound) | ™ ip | Edit |
| 02 | 1 | V | * | A 99.99.89.2 A | | 暑 99.99.9 | 9.12 | 🦈 incom | ing outs | side | ır⁄esp | Delete |
| VPN | 2 | | 1 | 3 99.99.99.2 | | a 99.99.9 | 9.12 | ♣ incom | ing outs | side | Brc: isakmp | |
| 423 Routing | | | | | | | | | | | | |
| Administration | | | | | | | | | | | | |
| Properties | | | | | | | | | | | | |
| | - | Allow traffic | : | O Deny traffic | | | | 6 | Show S | Summary | C Show Detail | |
| Wizards - ^ | | | | | Арріу | | Reset | | Advanced | | | |
| | | | | | | < | admin> | NA (15) | 1 | | 🔒 3/1 6/05 4:54 | 4:58 PM UTC |

27. A configuração está agora completa.Escolha **configuração running do arquivo > da mostra na nova janela** a fim ver a configuração de



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
1
interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
1
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
mqcp-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
1
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 inspeçãos 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 IImitado 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)#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 <u>Output Interpreter Tool</u> (<u>somente clientes registrados</u>) 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

Note: Consulte <u>Informações Importantes sobre Comandos de Debugação</u> 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.

Limpando 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 <u>Output Interpreter Tool</u> (<u>somente clientes registrados</u>) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Note: Consulte Informações Importantes sobre Comandos de Debugação 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-



 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.

| Log Buff | fer | | | | |
|--|-----------------------|--|--|--|--|
| This scre | en shows syslog mess: | ages in ASDM logging buffer as of now. | | | |
| Find text in messages below: Find Next | | | | | |
| | - , | | | | |
| Severity | Time | 2 | | | |
| <u> 6</u> 6 | Mar 16 2005 17:06:11 | 605005: Login permitted from 10.1.1.3/1247 to inside:10.1.1.1/https for user "enable | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 609001: Built local-host inside:10.1.1.2 | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 609001: Built local-host outside:99.99.99.2 | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enable | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10. | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 605005: Login permitted from 10.1.1.3/1221 to inside:10.1.1.1/https for user "enable | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 302013: Built inbound TCP connection 50 for inside:10.1.1.3/1221 (10.1.1.3/1221) t | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 302014: Teardown TCP connection 48 for inside:10.1.1.3/1220 to NP Identity Ifc:10. | | | |
| <u>8</u> 4 | Mar 16 2005 17:05:47 | 106023: Deny udp src outside:99.99.99.2/4500 dst inside:99.99.99.12/4500 by acce | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 302015: Built inbound UDP connection 49 for outside:99.99.99.2/500 (99.99.99.2/5/ | | | |
| <u>i</u> . 6 | Mar 16 2005 17:05:47 | 609001: Built local-host inside:10.1.1.2 | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 609001: Built local-host outside:99.99.99.2 | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 605005: Login permitted from 10.1.1.3/1220 to inside:10.1.1.1/https for user "enable | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 302013: Built inbound TCP connection 48 for inside:10.1.1.3/1220 (10.1.1.3/1220) t | | | |
| <u>i</u> 6 | Mar 16 2005 17:05:47 | 302014: Teardown TCP connection 47 for inside:10.1.1.3/1219 to NP Identity Ifc:10. | | | |
| <u>i</u> . 6 | Mar 16 2005 17:05:46 | 605005: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enable | | | |
| i 6 | Mar 16 2005 17:05:46 | 302013: Built inbound TCP connection 47 for inside:10.1.1.3/1219 (10.1.1.3/1219) t | | | |
| i 6 | Mar 16 2005 17:05:46 | 302014: Teardown TCP connection 46 for inside:10.1.1.3/1218 to NP Identity Ifc:10. | | | |
| 1.6 | Mar 16 2005 17:05:46 | 605005: Login permitted from 10.1.1.3/1218 to inside:10.1.1.1/https for user "enable | | | |
| 1.6 | Mar 16 2005 17:05:46 | 302013: Built inbound TCP connection 46 for inside:10.1.1.3/1218 (10.1.1.3/1218) t | | | |
| 1.6 | Mar 16 2005 17:05:46 | 302014: Teardown TCP connection 45 for inside:10.1.1.3/1217 to NP Identity Ifc:10. | | | |
| 1.6 | Mar 16 2005 17:05:46 | 505005: Login permitted from 10.1.1.3/1217 to inside:10.1.1.1/https for user "enabli | | | |
| 1.6 | Mar 16 2005 17:05:46 | 302013: Built Inbound TCP connection 45 for Inside:10.1.1.3/1217 (10.1.1.3/1217) t | | | |
| 1.6 | Mar 16 2005 17:05:46 | 302014: Leardown TCP connection 44 for inside:10.1.1.3/1216 to NP Identity Ifc:10. | | | |
| 1.6 | Mar 16 2005 17:05:46 | SUSUUS: Login permitted from 10.1.1.3/1219 to inside:10.1.1.1/https for user "enable | | | |

Refresh

Clear

Close

Help

Informações Relacionadas

• Página de Suporte de Negociação IPSec/Protocolos IKE

Save Log As...

- Página de suporte do PIX
- Referências de comando PIX
- Página de suporte de NAT
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação Cisco Systems