PIX 6.x: IPsec dinâmico entre um roteador IOS endereçado estaticamente e o firewall PIX dinamicamente endereçado com exemplo de configuração de NAT

Contents

Introduction

Este documento fornece um exemplo de configuração que mostra como habilitar o roteador IOS® a aceitar conexões IPsec dinâmicas de um PIX Firewall. O roteador remoto executa a Network Address Translation (NAT) se a rede privada 10.0.0.x acessa a Internet. O tráfego de 10.0.0.x para a rede privada 10.1.0.x atrás do PIX é excluído do processo NAT. O PIX Firewall pode iniciar conexões com o roteador, mas o roteador não pode iniciar conexões com o PIX.

Essa configuração usa um roteador Cisco IOS para criar túneis IPsec LAN-to-LAN (L2L) dinâmicos com um PIX Firewall que recebe endereços IP dinâmicos em sua interface pública (interface externa). O Dynamic Host Configuration Protocol (DHCP) fornece um mecanismo para alocar endereços IP dinamicamente do provedor de serviços de Internet (ISP). Isso permite que os endereços IP sejam reutilizados quando os hosts não precisarem mais deles.

Consulte o PIX 6.x: IPsec dinâmico entre um firewall PIX endereçado estaticamente e o exemplo de configuração do roteador IOS endereçado dinamicamente com NAT para obter mais informações sobre o cenário em que o PIX aceita conexões IPsec dinâmicas do roteador.

Consulte o PIX/ASA 7.x ou posterior: IPsec dinâmico entre um PIX endereçado estaticamente e um roteador IOS dinamicamente endereçado com exemplo de configuração de NAT para permitir que o PIX/ASA Security Appliance aceite conexões IPsec dinâmicas do roteador IOS.

Consulte o PIX/ASA 7.x ou posterior: IPsec dinâmico entre um roteador IOS endereçado estaticamente e um PIX endereçado dinamicamente com exemplo de configuração de NAT para saber mais sobre o mesmo cenário em que o PIX/ASA Security Appliance executa o software versão 7.x e posterior.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Versão do software Cisco IOS 12.4
- Versão 6.3.4 do software Cisco PIX Firewall
- Cisco Secure PIX Firewall 515E
- Cisco 2811 Router

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

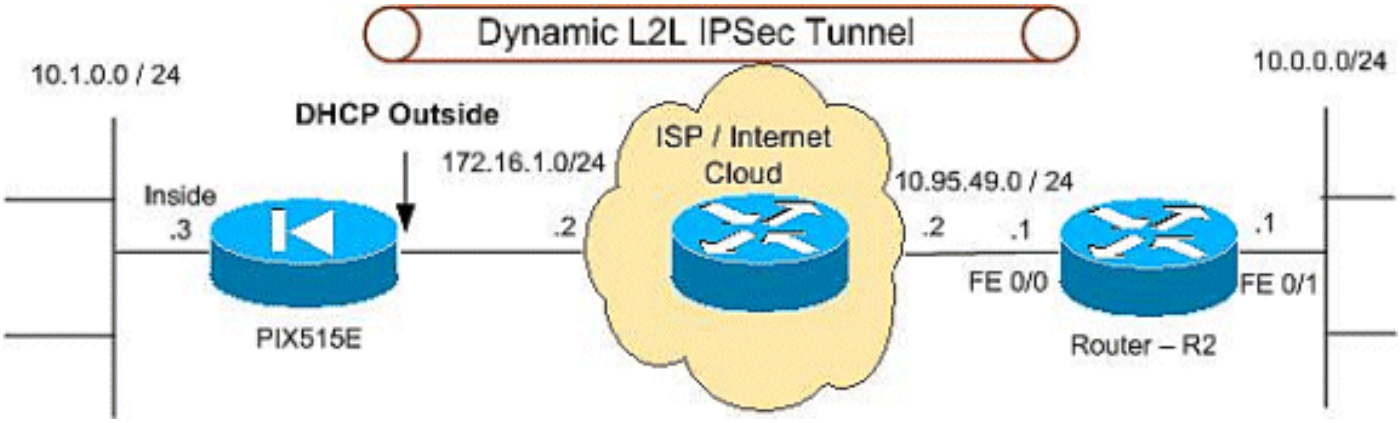
Configurar

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 neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- PIX 515E
- R2 (Roteador Cisco 2811)

PIX 515E

```
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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

!--- The access control list (ACL) to avoid NAT on the
IPsec packets. access-list NO-NAT permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
!--- The ACL to apply on crypto map. !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500
!--- ISP will providthe the Outside IP address.
```

```
ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 10.0.0.0 255.255.255.0 172.16.1.5 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 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
sysopt connection permit-ipsec

!--- IPsec configuration, Phase 2. crypto ipsec
transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy, Phase 1. !--- Note: In
real show run output, the pre-shared key appears as
*******.

isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask
255.255.255.255
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400

telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
: end
```

R2 (Roteador Cisco 2811)

```
R2#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
!--- ISAKMP policy, Phase 1. crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!
!--- IPsec policy, Phase 2. crypto ipsec transform-set
DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
```

```
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server
!--- Except the private network from the NAT process. ip
nat inside source list 102 interface FastEthernet0/0
overload
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

!--- Except the private network from the NAT process.
access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0
0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
login
!
end
```

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** — Mostra todas as associações de segurança (SAs) IKE atuais em um peer.
- **show crypto ipsec sa** — Mostra as configurações usadas por SAs atuais (IPsec).
- **show crypto engine connections ative** —Mostra as conexões atuais e as informações sobre pacotes criptografados e descriptografados (somente roteador).

Você deve limpar as SAs em ambos os peers.

Execute esses comandos PIX no modo de configuração.

- **clear crypto isakmp sa — Cancela as SAs da fase 1.**

- **clear crypto ipsec sa** — Limpa as SAs da Fase 2.

Execute esses comandos do roteador no modo de ativação.

- **clear crypto isakmp** — Limpa as SAs da Fase 1.
- **clear crypto sa** — Limpa as SAs da Fase 2.

Troubleshoot

Use esta seção para resolver problemas de configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

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

- **show crypto isakmp sa** — Exibir todas as SAs IKE atuais em um peer.
- **show crypto ipsec sa** — Mostra as configurações usadas por SAs atuais (IPsec).
- **show crypto engine connections ative** —Mostra as conexões atuais e as informações sobre pacotes criptografados e descriptografados (somente roteador).

Informações Relacionadas

- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Negociação IPsec/Protocolos IKE