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

Índice

Introdução

Este documento fornece uma configuração de exemplo para que como permita o PIX de aceitar conexões de IPSec dinâmica. O roteador remoto executa a Tradução de Endereço de Rede (NAT) se a rede privada 10.1.1.x acessa a Internet. O tráfego de 10.1.1.x à rede privada 192.168.1.x atrás do PIX é excluído do processo NAT. O roteador pode iniciar conexões com o PIX, mas a recíproca não é verdadeira.

Esta configuração usa um PIX Firewall a fim criar túneis dinâmicos do LAN para LAN do IPsec (L2L) com um roteador de Cisco IOS® que receba endereços IP dinâmicos em sua interface pública (interface externa). O protocolo de configuração dinâmica host (DHCP) fornece um mecanismo a fim atribuir dinamicamente endereços IP de Um ou Mais Servidores Cisco ICM NT do provedor de serviços (ISP). Isto permite que os endereços IP de Um ou Mais Servidores Cisco ICM NT sejam reutilizados quando os anfitriões já não os precisam.

Refira o IPSec dinâmico para estático Roteador-à-PIX com exemplo da configuração de NAT para obter mais informações sobre de uma encenação onde o roteador aceite conexões de IPSec dinâmica de uma ferramenta de segurança PIX que execute 6.x.

Refira o IPsec entre um IOS Router estático e um PIX/ASA dinâmico 7.x com exemplo da configuração de NAT a fim permitir a ferramenta de segurança PIX/ASA de aceitar conexões de IPSec dinâmica do roteador do Cisco IOS.

Refira o IPsec entre um PIX/ASA estático 7.x e um IOS Router dinâmico com exemplo da configuração de NAT a fim aprender uma encenação mais mais ou menos idêntica onde a ferramenta de segurança PIX/ASA execute a versão de software 7.x e mais tarde.

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 12.4
- Liberação de Software do firewall Cisco PIX 6.3.1
- Firewall PIX segura Cisco 515E
- Cisco 7206 Router

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

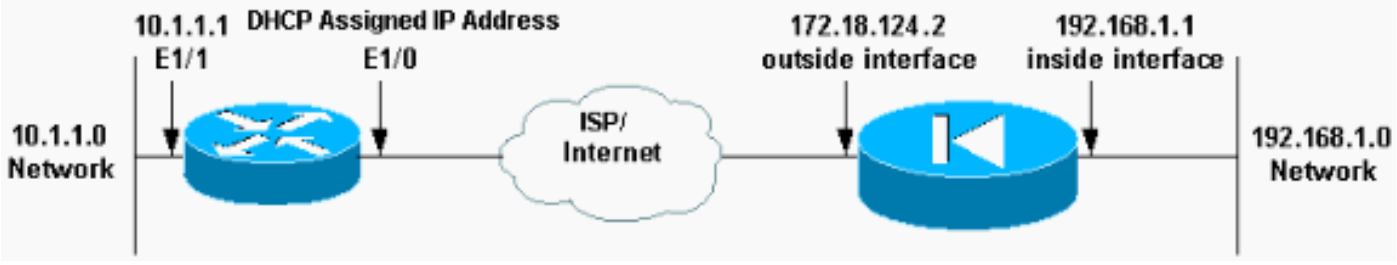
Configurar

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

Nota: Use a ferramenta Command Lookup Tool (apenas para 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 estas configurações.

- Duende (PIX)
- Espanador (Cisco 7204 Router)

Duende (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname elf
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Access control list (ACL) to avoid NAT on the IPsec
packets. access-list nonat permit ip 192.168.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.18.124.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 interface
!-- Binds ACL nonat to the NAT statement to avoid NAT on
the IPsec packets nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
!--- Permits Internet Control Message Protocol (ICMP)
traffic for testing. !--- Do not enable it in a live
network. conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00
h323 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 RADIUS protocol radius
aaa-server LOCAL protocol tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
!--- IPsec configuration crypto ipsec transform-set
router-set esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set router-set
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy for accepting dynamic
connections from remote PIX. !--- Note: In real show run
output, the pre-shared key appears as *******. isakmp
key cisco123 address 0.0.0.0 netmask 0.0.0.0
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
terminal width 80
Cryptochecksum:eeb67d5df47045f7e6ac4aa090aab683
: end
[OK]
elf#
```

Espanador (Cisco 7204 Router)

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

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mop
!
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) policies crypto isakmp
policy 1
```

```
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.2
!
!
!--- IPsec policies crypto ipsec transform-set pix-set
esp-des esp-md5-hmac
!
crypto map pix 10 ipsec-isakmp
 set peer 172.18.124.2
 set transform-set pix-set
 match address 101
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
ip address dhcp
ip nat outside
duplex half
crypto map pix
!
interface Ethernet1/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex half
!
!--- Except the private network from the NAT process. ip
nat inside source route-map nonat interface Ethernet1/0
overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1/0
no ip http server
ip pim bidir-enable
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
!--- Except the private network from the NAT process.
access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0
0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end
```

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.

Você pode executar estes **comandos show no** PIX e no roteador.

- show crypto isakmp sa – Mostra todas as associações de segurança (SAs) IKE atuais no correspondente.
- **mostre IPsec cripto sa** — Mostra os ajustes usados (IPsec) por SA atuais.
- **active do show crypto engine connections** — Conexões atual e informação das mostras em relação aos pacotes criptografado e decriptografado (roteador somente).

Você deve limpar as SAs em ambos os peers.

- Os comandos pix são executados no modo de configuração.**clear crypto isakmp sa** — Cancela as SAs da fase 1.**clear crypto ipsec sa** — Cancela a fase 2 SA.
- Os comandos router são executados no modo enable.**cancele o isakmp cripto** — Cancela a fase 1 SA.**cancele o sa cripto** — Cancela a fase 2 SA.

Troubleshooting

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

Comandos para Troubleshooting

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.

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

- **mostre isakmp cripto sa** — Mostra todo o IKE atual SA em um par.
- **mostre IPsec cripto sa** — Mostra os ajustes usados (IPsec) por SA atuais.
- **active do show crypto engine connections** — Conexões atual e informação das mostras em relação aos pacotes criptografado e decriptografado (roteador somente).

Informações Relacionadas

- Página de Suporte de Negociação IPSec/Protocolos IKE
- Ferramentas de segurança da série PIX 500
- Referências do comando Cisco Secure PIX Firewall
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems