Túnel de IPsec entre PIX 7.x e exemplo de configuração do VPN 3000 concentrator

Índice

Introdução

Este documento fornece uma configuração de exemplo para que como estabeleça um túnel do IPSec VPN do LAN para LAN entre um PIX Firewall 7.x e um Cisco VPN 3000 Concentrator.

Refira o Spoke-à-cliente aumentado 7.x VPN PIX/ASA com exemplo de configuração da autenticação TACACS+ a fim aprender mais sobre a encenação onde o túnel de LAN para LAN entre as PIXes igualmente permite um cliente VPN alcançar o spoke PIX com o PIX de hub.

Refira a ferramenta de segurança PIX/ASA 7.x a um exemplo de configuração do túnel IPSec de LAN para LAN do IOS Router a fim aprender mais sobre a encenação onde o túnel de LAN para LAN entre o PIX/ASA e um IOS Router.

Pré-requisitos

Requisitos

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

- Este documento exige uma compreensão básica do protocolo IPSec. Refira uma introdução à criptografia IPSec para aprender mais sobre o IPsec.

Componentes Utilizados

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

- Ferramenta de segurança da série do Cisco PIX 500 com versão de software 7.1(1)
- Concentrador Cisco VPN 3060 com versão de software 4.7.2(B)

Note: O PIX 506/506E não apoia 7.x.

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.

A fim configurar PIX 6.x, refira o túnel IPSec de LAN para LAN entre o Cisco VPN 3000 Concentrator e o exemplo de configuração do PIX Firewall.

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.

- Configure o PIX
- Configurar o VPN 3000 Concentrator

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configure o PIX

PIX

```
PIX7#show running-config
: Saved
:
PIX Version 7.1(1)
!
hostname PIX7
enable password 8Ry2YjIyt7RRXU24 encrypted
names
```

```
!
!--- Configures the outside interface of the PIX. !---
By default, the security level for the outside interface
is 0. interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
!--- Configures the inside interface of the PIX. !--- By
default, the security level for the inside interface is
100. interface Ethernet1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
!--- Defines the IP addresses that should not be NATed.
access-list nonat extended permit ip 192.168.1.0
255.255.255.0 172.16.0.0 255.255.0.0
access-list outside extended permit icmp any any
!--- Defines the IP addresses that can communicate via
the IPsec tunnel. access-list 101 extended permit ip
192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0
access-list OUT extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
no failover
asdm image flash:/asdm-504.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list nonat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 10.1.1.2 1
!--- Output is suppressed. !--- These are the IPsec
parameters that are negotiated with the client. crypto
ipsec transform-set my-set esp-aes-256 esp-sha-hmac
crypto map mymap 20 match address 101
crypto map mymap 20 set peer 172.30.1.1
crypto map mymap 20 set transform-set my-set
crypto map mymap interface outside
!--- These are the Phase I parameters negotiated by the
two peers. isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!--- A tunnel group consists of a set of records !---
that contain tunnel connection policies. The two
attributes !--- are General and IPsec. Use the remote
peer IP address as the !--- name of the Tunnel group. In
this example 172.30.1.1 is the peer IP address. !---
Refer to Tunnel Group for more information. tunnel-group
172.30.1.1 type ipsec-l2l
tunnel-group 172.30.1.1 ipsec-attributes
 pre-shared-key *
!--- Output is suppressed. ! : end PIX7#
```

Configurar o VPN 3000 Concentrator

Os concentradores VPN PRE-não são programados com endereços IP de Um ou Mais Servidores Cisco ICM NT em suas configurações de fábrica. Você tem que usar a porta de Console a fim

configurar as configurações inicial que são um comando line interface(cli) menu-baseado. Refira configurar concentradores VPN através do console para obter informações sobre de como configurar através do console.

Depois que você configura o endereço IP de Um ou Mais Servidores Cisco ICM NT na relação (privada) de Ethernet1, você pode configurar o resto com o CLI ou através da interface de navegador. A interface de navegador apoia o HTTP e o HTTP sobre o Secure Socket Layer (SSL).

Estes parâmetros são configurados através do console:

- **Hora/data** — As horas correta e a data são muito importantes. Ajudam a assegurar-se de que o registro e as entradas de relatório sejam exatos, e que o sistema pode criar um Security Certificate válido.
- **Relação (privada) de Ethernet1** — O endereço IP de Um ou Mais Servidores Cisco ICM NT e a máscara (da topologia de rede 172.16.5.100/16).

O concentrador VPN é agora acessível com um navegador de HTML da rede interna. Refira a utilização da interface de linha de comando para a configuração rápida para obter informações sobre de como configurar o concentrador VPN no modo de CLI.

Datilografe o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface confidencial do navegador da Web a fim permitir a interface GUI.

Clique o ícone **necessário salvaguarda** para salvar mudanças à memória. O nome de usuário e senha do padrão de fábrica é o **admin**, que é diferenciando maiúsculas e minúsculas.

1. Lance o GUI e selecione o **configuração > interfaces** para configurar o endereço IP de Um ou Mais Servidores Cisco ICM NT para a interface pública e o gateway padrão.
2. Selecione o **> Add do Configuração > Gerenciamento de Política > Gerenciamento de Tráfego > Listas de Rede ou altere-o** para criar os listes de redes que definem o tráfego a ser cifrado.Adicionar ambas as redes remotas e locais aqui. Os endereços IP de Um ou Mais Servidores Cisco ICM NT devem espelhar aqueles na lista de acessos configurada no PIX remoto.Neste exemplo, os dois listes de redes são **LAN local do remote_network** e do **cliente VPN**.
3. Selecione o **Configuration > System > Tunneling Protocols > > Add do LAN para LAN do IPsec** para configurar o túnel de LAN para LAN de IPSec. Clique em Apply quando tiver concluído.Incorpore o endereço IP do peer, os listes de redes criados em etapa 2, o IPsec e os parâmetros ISAKMP, e a chave pré-compartilhada.Neste exemplo o endereço IP do peer é **10.1.1.1**, os listes de redes são **LAN local do remote_network** e do **cliente VPN**, e **Cisco** é a chave pré-compartilhada.
4. Selecione o **configuration > user management > os grupos > Modify 10.1.1.1** para ver a informação automaticamente gerada do grupo.**Note**: Não modifique essas configurações de grupo.

Verificar

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

- Verifique o PIX

- Verifique o VPN 3000 concentrator

Verifique o PIX

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.

- **mostre isakmp sa** — Indica todas as associações de segurança atuais IKE (SA) em um par. O estado MM_ACTIVE denota que o modo principal está usado para estabelecer o túnel do IPSec VPN.Neste exemplo o PIX Firewall inicia a conexão IPSec. O endereço IP do peer é 172.30.1.1 e usa o modo principal para estabelecer a conexão.

```
PIX7#show 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: 172.30.1.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

- **mostre IPsec sa** — Indica os ajustes usados por SA atuais. Verifique para ver se há os endereços IP do peer, as redes acessíveis no local e em extremidades remotas, e a transformação ajustada que é usada. Há dois ESP SA, um em cada sentido.

```
PIX7#show ipsec sa
interface: outside
    Crypto map tag: mymap, seq num: 20, local addr: 10.1.1.1

      access-list 101 permit ip 192.168.1.0 255.255.255.0 172.16.0.0 255.255.0.0

      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
      current_peer: 172.30.1.1

      #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
      #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.1.1.1, remote crypto endpt.: 172.30.1.1

      path mtu 1500, ipsec overhead 76, media mtu 1500
      current outbound spi: 136580F6

    inbound esp sas:
      spi: 0xF24F4675 (4065281653)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel,}
         slot: 0, conn_id: 1, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (3824999/28747)
         IV size: 16 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x136580F6 (325419254)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel,}
         slot: 0, conn_id: 1, crypto-map: mymap
         sa timing: remaining key lifetime (kB/sec): (3824999/28745)
```

```
IV size: 16 bytes
replay detection support: Y
```

Use IPsec claro sa e comandos clear isakmp sa restaurar o túnel.

Verifique o VPN 3000 concentrator

Selecione a **monitoração > as estatísticas > o IPsec** para verificar se o túnel veio acima no VPN 3000 concentrator. Isto contém as estatísticas para o IKE e os parâmetros IPSec.

Você pode monitora ativamente a sessão no **monitoramento > sessões**. Você pode restaurar o túnel de IPsec aqui.

Troubleshooting

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

- Pesquise defeitos o PIX
- Pesquise defeitos o VPN 3000 concentrator
- PFS

Pesquise defeitos o PIX

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.

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

Os comandos debug no PIX para túneis VPN são:

- **isakmp do debug crypto** — Debuga negociações ISAKMP SA.
- **IPsec do debug crypto** — Debuga negociações IPsec SA.

Pesquise defeitos o VPN 3000 concentrator

Similar aos comandos debug nos roteadores Cisco, você pode configurar classes de evento para ver todos os alarmes. Selecione o **configuração > sistema > eventos > classes > adicionar** para girar sobre o registro das classes de evento.

Selecione a **monitoração > o log filtrável de eventos** para monitorar os eventos permitidos.

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 do LAN para LAN (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
```

Informações Relacionadas

- Dispositivos de segurança Cisco PIX série 500 - Página de suporte
- Página de suporte do concentrador da Cisco VPN 3000 Series
- Referência de comandos da ferramenta de segurança da série do Cisco PIX 500
- Suporte Técnico e Documentação - Cisco Systems