PIX/ASA e cliente VPN para os Internet públicas VPN em um exemplo de configuração da vara

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Produtos Relacionados
Convenções
Informações de Apoio
Hairpinning ou Inversão de Sentido
Configurações
Diagrama de Rede
Configuração de CLI do PIX/ASA
Configurar o ASA/PIX com ASDM
Configuração de cliente de VPN
Verificar
Verificação do cliente VPN
Troubleshooting
Informações Relacionadas

Introdução

Este documento descreve como estabelecer uma ferramenta de segurança 7.2 ASA e mais atrasado para executar o IPsec em uma vara. Esta instalação se aplica a um caso específico onde o ASA não permite o tunelamento dividido e os usuários se conectam diretamente ao ASA antes de receberem permissão para acessar a Internet.

Nota: Na versão 7.2 e mais recente PIX/ASA, a palavra-chave da intra-*relação* permite que todo o tráfego incorpore e retire a mesma relação, e não apenas o tráfego de IPSec.

Refira o roteador e o cliente VPN para Internet públicas em um exemplo de configuração da vara para terminar uma configuração similar em um roteador de site central.

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 PIX de hub reorienta o tráfego do cliente VPN ao spoke PIX.

Nota: A fim evitar uma sobreposição dos endereços IP de Um ou Mais Servidores Cisco ICM NT na rede, atribua um pool completamente diferente dos endereços IP de Um ou Mais Servidores Cisco ICM NT ao cliente VPN (por exemplo, 10.x.x.x, 172.16.x.x, e 192.168.x.x). Este esquema

de endereçamento de IP é útil a fim pesquisar defeitos sua rede.

Pré-requisitos

Requisitos

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

- A ferramenta de segurança do hub PIX/ASA precisa de executar a versão 7.2 ou mais recente
- Versão Cliente VPN Cisco 5.x

Componentes Utilizados

A informação neste documento é baseada a versão 8.0.2 na ferramenta de segurança PIX ou ASA e a Versão Cliente VPN Cisco 5.0.

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.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão 7.2 e mais recente da ferramenta de segurança de Cisco PIX.

Convenções

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

Informações de Apoio

Hairpinning ou Inversão de Sentido

Esta característica é útil para o tráfego VPN que incorpora uma relação mas é então roteado fora dessa mesma relação. Por exemplo, se você tem uma rede VPN do Hub-and-Spoke, onde a ferramenta de segurança seja o hub, e as redes VPN remotas é spokes, para que um falou para se comunicar com um outro spoke, trafica deve sair na ferramenta de segurança e então outra vez ao outro spoke.

Use o comando **same-security-traffic** para permitir que o tráfego entre e saia da mesma interface.

```
securityappliance(config)#same-security-traffic permit intra-interface
```

Nota: O hairpinning ou a inversão de marcha são aplicável para o cliente VPN a uma comunicação do cliente VPN, também.

Configurações

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 nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configuração de CLI do PIX/ASA

- PIX/ASA

Execute a configuração no PIX/ASA

```
PIX Version 8.0(2)
names
!
interface Ethernet0
nameif outside
security-level 0
ip address 172.18.124.98 255.255.255.0
!
interface Ethernet1
nameif inside
security-level 100
ip address 172.16.3.101 255.255.255.0
!
interface Ethernet2
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet3
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
```

```
ftp mode passive
!--- Command that permits IPsec traffic to enter and
exit the same interface. same-security-traffic permit
intra-interface access-list 100 extended permit icmp any
any echo-reply pager lines 24 logging enable logging
buffered debugging mtu outside 1500 mtu inside 1500 ip
local pool vpnpool 192.168.10.1-192.168.10.254 mask
255.255.255.0 no failover monitor-interface outside
monitor-interface inside icmp permit any outside no asdm
history enable arp timeout 14400 nat-control !--- The
address pool for the VPN Clients. !--- The global
address for Internet access used by VPN Clients. !---
Note: Uses an RFC 1918 range for lab setup. !--- Apply
an address from your public range provided by your ISP.
global (outside) 1 172.18.124.166 !--- The NAT statement
to define what to encrypt (the addresses from the vpn-
pool). nat (outside) 1 192.168.10.0 255.255.255.0 nat
(inside) 1 0.0.0.0 0.0.0.0 static (inside,outside)
172.16.3.102 172.16.3.102 netmask 255.255.255.255
access-group 100 in interface outside route outside
0.0.0.0 0.0.0.0 172.18.124.98 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
!--- The configuration of group-policy for VPN Clients.
group-policy clientgroup internal group-policy
clientgroup attributes vpn-idle-timeout 20 !--- Forces
VPN Clients over the tunnel for Internet access. split-
tunnel-policy tunnelall no snmp-server location no snmp-
server contact snmp-server enable traps snmp !---
Configuration of IPsec Phase 2. crypto ipsec transform-
set myset esp-3des esp-sha-hmac !--- Crypto map
configuration for VPN Clients that connect to this PIX.
crypto dynamic-map rtpdynmap 20 set transform-set myset
!--- Binds the dynamic map to the crypto map process.
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap !---
Crypto map applied to the outside interface. crypto map
mymap interface outside !--- Enable ISAKMP on the
outside interface. isakmp identity address isakmp enable
outside !--- Configuration of ISAKMP policy. isakmp
policy 10 authentication pre-share isakmp policy 10
encryption 3des isakmp policy 10 hash sha isakmp policy
10 group 2 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
telnet timeout 5 ssh timeout 5 console timeout 0 !---
Configuration of tunnel-group with group information for
VPN Clients. tunnel-group rtptacvpn type ipsec-ra !---
Configuration of group parameters for the VPN Clients.
tunnel-group rtptacvpn general-attributes address-pool
vpnpool !--- Disable user authentication.
authentication-server-group none !--- Bind group-policy
parameters to the tunnel-group for VPN Clients. default-
group-policy clientgroup tunnel-group rtptacvpn ipsec-
attributes pre-shared-key * ! 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 esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
service-policy global_policy global
```

```
Cryptochecksum:1a1ad58226e700404e1053159f0c5fb0 : end
```

Configurar o ASA/PIX com ASDM

Termine estas etapas a fim configurar Cisco ASA como um servidor de VPN remoto com ASDM:

1. Escolha **assistentes > assistente do IPSec VPN do** indicador home.
2. Escolha o tipo de túnel do **acesso remoto VPN**, e assegure-se de que a interface de túnel VPN esteja ajustada como desejada.
3. O único tipo do cliente VPN disponível é escolhido já. Clique em Next.
4. Dê entrada com um nome para o nome de grupo de túneis. Forneça a informação da autenticação para usar-se.**A chave pré-compartilhada** é escolhida neste exemplo.**Nota:** Não há uma maneira de esconder/cifra a chave pré-compartilhada no ASDM. A razão é que o ASDM deve somente ser usado pelos povos que configuram o ASA ou pelos povos que ajudam ao cliente com esta configuração.
5. Escolha se você quer usuários remotos ser autenticado à base de dados de usuário local ou a um Grupo de servidores AAA externo.**Nota:** Você adiciona usuários à base de dados de usuário local na etapa 6.**Nota:** Refira grupos de servidor da authentication e autorização PIX/ASA 7.x para usuários VPN através do exemplo da configuração ASDM para obter informações sobre de como configurar um Grupo de servidores AAA externo com o ASDM.
6. Adicionar usuários ao base de dados local, caso necessário.**Nota:** Não remova os usuários atuais deste indicador. Escolha a **configuração > a administração do dispositivo > a administração > as contas de usuário na janela principal de ASDM** para editar entradas existentes no base de dados ou para removê-las do base de dados.
7. Defina um pool dos endereços locais a ser atribuídos dinamicamente aos clientes VPN remotos quando conectam.
8. *Opcional:* Especifique o DNS e GANHE a informação do servidor e um Domain Name do padrão a ser empurrado para clientes VPN remotos.
9. Especifique os parâmetros para o IKE, igualmente conhecidos como a fase 1. IKE.As configurações em ambos os lados do túnel devem combinar exatamente, mas o Cisco VPN Client escolhe automaticamente a configuração apropriada para se. Nenhuma configuração de IKE é necessária no PC cliente.
10. Especifique os parâmetros para o IPsec, igualmente conhecidos como a fase 2. IKE.As configurações em ambos os lados do túnel devem combinar exatamente, mas o Cisco VPN Client escolhe automaticamente a configuração apropriada para se. Nenhuma configuração de IKE é necessária no PC cliente.
11. Especifique qual, eventualmente, os host internos ou as redes podem ser expostos aos usuários remotos VPN.Se você deixa esta lista vazia, permite que os usuários remotos VPN alcancem a rede interna inteira do ASA.Você pode igualmente permitir o Split Tunneling neste indicador. O Split Tunneling cifra o tráfego aos recursos definidos mais cedo neste procedimento e fornece acesso unencrypted ao Internet em grande não escavando um túnel esse tráfego. Se o Split Tunneling não é permitido, todo o tráfego dos usuários remotos VPN está escavado um túnel ao ASA. Esta pode transformar-se muito largura de banda e utilização de processador, com base em sua configuração.
12. Este indicador mostra um sumário das ações que você tomou. Clique o **revestimento** se você é satisfeito com sua configuração.
13. Configurar o comando same-security-traffic permitir um tráfego entre dois ou mais anfitriões conectados à mesma relação quando você clicar a caixa de seleção como mostrado:

14. Escolha **regras da configuração > do Firewall >NAT**, e o clique **adiciona a regra dinâmica NAT** a fim criar esta tradução dinâmica com o uso do ASDM.
15. Escolha o **interior** como a interface de origem, e incorpore os endereços que você quer ao NAT. Para o endereço Translate na relação, escolha **fora** e clique a **APROVAÇÃO**.
16. Escolha a **parte externa** como a interface de origem, e incorpore os endereços que você quer ao NAT. Para o endereço Translate na relação, escolha **fora** e clique a **APROVAÇÃO**.
17. A tradução aparece nas Regras de tradução em **regras da configuração > do Firewall >NAT**.

Nota 1: O comando da conexão licença-VPN do sysopt precisa de ser configurado. O comando show running-config sysopt verifica se é configurado.

Nota 2: Adicionar esta saída para o transporte opcional UDP:

```
group-policy clientgroup attributes vpn-idle-timeout 20 ipsec-udp enable ipsec-udp-port 10000
split-tunnel-policy tunnelspecified split-tunnel-network-list value splittunnel
```

Nota 3: Configurar este comando na configuração global da ferramenta de PIX para que os clientes VPN conectem através do IPsec sobre o TCP:

```
isakmp ipsec-over-tcp port 10000
```

Nota: Refira o Hair-Pinning no vídeo de Cisco ASA para obter mais informações sobre das encenações diferentes onde o Hair-Pinning pode ser usado.

Configuração de cliente de VPN

Termine estas etapas para configurar o cliente VPN:

1. Escolha **novo**.
2. Dê entrada com o nome do endereço IP de Um ou Mais Servidores Cisco ICM NT e do grupo de túneis da interface externa PIX junto com a senha de autenticação.
3. O clique (*opcional*) **permite o Tunelamento transparente** sob o guia de transporte. (Isto é opcional e exige a configuração adicional PIX/ASA mencionada na nota 2.)
4. Salvar o perfil.

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.

- **show crypto isakmp sa — Exibe todas as associações de segurança atuais (SAs) de IKE em um peer.**
- **show crypto ipsec sa — Exibe todas as SAs atuais.** Look for cifra e decifra os pacotes no SA que definem o tráfego do cliente VPN.

Tente sibilar ou consultar a um endereço IP público do cliente (por exemplo, www.cisco.com).

Nota: A interface interna do PIX não pode ser sibilada para a formação de um túnel a menos que o comando do **acesso de gerenciamento** for configurado no modo de configuração global.

```
PIX1(config)#management-access inside PIX1(config)# show management-access management-access
inside
```

Verificação do cliente VPN

Termine estas etapas a fim verificar o cliente VPN.

1. Clicar com o botão direito no ícone do fechamento do cliente VPN atual na bandeja do sistema após uma conexão bem sucedida e escolha a opção de estatísticas ver cifra e decifra.
2. Clique sobre a aba dos detalhes da rota a fim não verificar nenhuma lista de túneis em divisão passada para baixo do dispositivo.

Troubleshooting

Nota: Para obter mais informações sobre de como pesquisar defeitos edições VPN, refira soluções do Troubleshooting VPN.

Informações Relacionadas

- Exemplo aumentado da configuração de VPN do Spoke-à-cliente para a versão 7.0 da ferramenta de segurança PIX
- Cisco VPN Client
- Negociação IPsec/Protocolos IKE
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Hair-Pinning em Cisco ASA
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems