PIX/ASA 7.x: Adicionar/remova uma rede em um exemplo existente da configuração de túnel L2L VPN

Índice

Introdução

Este documento fornece uma configuração de exemplo para que como adicione uma rede nova a um túnel existente VPN.

Pré-requisitos

Requisitos

Assegure-se de que você tenha uma ferramenta de segurança PIX/ASA que execute o código 7.x antes que você tente esta configuração.

Componentes Utilizados

A informação neste documento é baseada em dois Cisco 5500 dispositivos da ferramenta de segurança.

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 a ferramenta de segurança PIX 500.

Convenções

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

Informações de Apoio

Há atualmente um túnel do LAN para LAN (L2L) VPN que esteja entre o escritório NY e TN. O escritório NY apenas adicionou uma rede nova a ser usada pelo grupo do desenvolvimento CSI. Este grupo exige o acesso aos recursos que residem no escritório TN. A tarefa à mão é adicionar a rede nova ao túnel já existente VPN.

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 nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Adicionando a rede ao túnel de IPsec

Este documento utiliza esta configuração:

Configuração do Firewall NY (QG)

```
ASA-NY-HQ#show running-config : Saved : ASA Version
7.2(2) ! hostname ASA-NY-HQ domain-name corp2.com enable
password WwXYvtKrnjXqGbu1 encrypted names ! interface
Ethernet0/0 nameif outside security-level 0 ip address
192.168.11.2 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet0/2 nameif Cisco
security-level 70 ip address 172.16.40.2 255.255.255.0 !
interface Ethernet0/3 shutdown no nameif no security-
level no ip address ! interface Management0/0 shutdown
no nameif no security-level no ip address ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name corp2.com access-list
inside_nat0_outbound extended permit ip 172.16.1.0
255.255.255.0 10.10.10.0 255.255.255.0 !--- You must be
sure that you configure the !--- opposite of these
```

```
access control lists !--- on the other end of the VPN
tunnel. access-list inside_nat0_outbound extended permit
ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list outside_20_cryptomap extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0 !---
You must be sure that you configure the !--- opposite of
these access control lists !--- on the other end of the
VPN tunnel. access-list outside_20_cryptomap extended
permit ip 172.16.40.0 255.255.255.0 10.10.10.0
255.255.255.0 !--- Output is suppressed. nat-control
global (outside) 1 interface nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 172.16.1.0
255.255.255.0 !--- The new network is also required to
have access to the Internet. !--- So enter an entry into
the NAT statement for this new network. nat (inside) 1
172.16.40.0 255.255.255.0 route outside 0.0.0.0 0.0.0.0
192.168.11.100 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart crypto ipsec
transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto
map outside_map 20 match address outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10 crypto
map outside_map 20 set transform-set ESP-3DES-SHA crypto
map outside_map interface outside crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp nat-traversal 20 tunnel-group 192.168.10.10 type
ipsec-l2l tunnel-group 192.168.10.10 ipsec-attributes
pre-shared-key * !--- Output is suppressed. : end ASA-
NY-HQ#
```

Removendo a rede do túnel de IPsec

Use isto pisa para remover a rede da configuração do túnel de IPsec. Aqui, considere que a rede 172.16.40.0/24 esteve removida da configuração de ferramenta NY (QG) Secuirty.

1. Antes que remova a rede do túnel, rasgue para baixo a conexão IPSec, que igualmente cancela as associações de segurança relativas à fase 2.
   ASA-NY-HQ# clear crypto ipsec sa Cancela as associações de segurança relativas à fase 1 como segue
   ASA-NY-HQ# clear crypto isakmp sa
2. Remova o tráfego interessante ACL para o túnel de IPsec.
   ASA-NY-HQ(config)# no access-list outside_20_cryptomap extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
3. Remova o ACL (inside_nat0_outbound), desde que o tráfego é excluído do nat.
   ASA-NY-HQ(config)# no access-list inside_nat0_outbound extended permit ip 172.16.40.0 255.255.255.0 10.10.10.0 255.255.255.0
4. Cancele a tradução NAT como mostrado
   ASA-NY-HQ# clear xlate
5. Quando nunca você altera a configuração de túnel, remova e reaplique este os comandos crypto tomar a configuração a mais atrasada na interface externa
   ASA-NY-HQ(config)# crypto map outside_map interface outside ASA-NY-HQ(config)# crypto isakmp enable outside

6. Salvar a configuração ativa ao flash **"escrevem a memória"**.
7. Siga o mesmo procedimento para a outra extremidade - ferramenta de segurança TN para remover as configurações.
8. Inicie o túnel de IPsec e verifique a conexão.

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.

- **sibile dentro de 172.16.40.20**
- show crypto isakmp sa
- **show crypto ipsec sa**

Troubleshooting

Refira estes documentos para mais informação de Troubleshooting:

- IPSec VPN que pesquisa defeitos soluções
- Compreendendo e usando comandos debug
- Troubleshooting de conexões via PIX e ASA

Informações Relacionadas

- **Uma introdução à criptografia do protocolo de segurança IP (IPSEC)**
- **Página do suporte de protocolo do IPsec Negotiation/IKE**
- **Referência de comandos da ferramenta de segurança**
- **Configurando listas de acesso de IP**
- **Suporte Técnico e Documentação - Cisco Systems**