Configurar o ASA para redes internas duplas

Contents

Introduction

Este documento descreve como configurar um Cisco Adaptive Security Appliance (ASA) que executa a versão de software 9.x para o uso de duas redes internas.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco ASA que executa o software versão 9.x.

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.

Informações de Apoio

Ao adicionar uma segunda rede interna por trás de um firewall ASA, considere estas informações importantes:

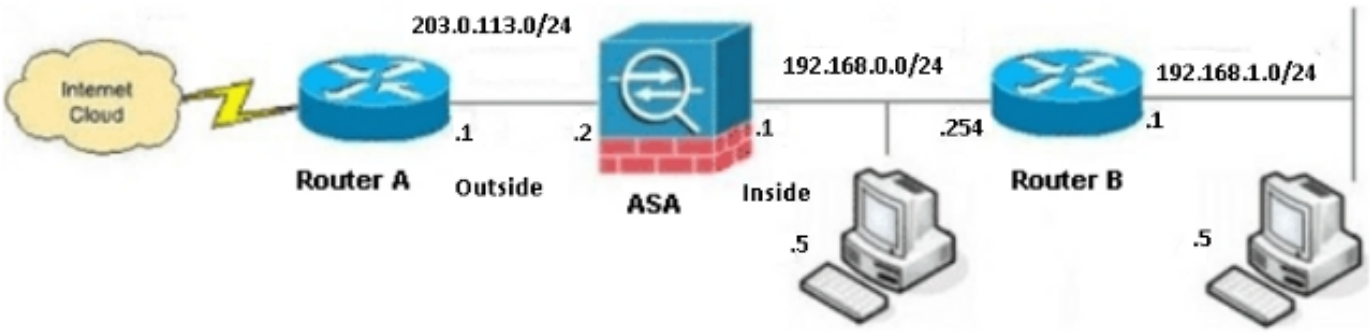
- O ASA não suporta endereçamento secundário.
- Um roteador deve ser usado atrás do ASA para alcançar o roteamento entre a rede atual e a rede recém-adicionada.
- O gateway padrão para todos os hosts deve apontar para o roteador interno.
- Você deve adicionar uma rota padrão no roteador interno que aponte para o ASA.
- Você deve limpar o cache do Address Resolution Protocol (ARP) no roteador interno.

Configurar

Use as informações descritas nesta seção para configurar o ASA.

Diagrama de Rede

Aqui está a topologia usada para os exemplos deste documento:



Note: Os esquemas de endereçamento IP usados nessa configuração não são legalmente roteáveis na Internet. Eles são endereços RFC 1918 que são usados em um ambiente de laboratório.

Configuração do ASA 9.x

Se você tiver a saída do comando **write terminal** de seu dispositivo Cisco, poderá usar a ferramenta Output Interpreter (somente clientes registrados) para exibir possíveis problemas e correções.

Esta é a configuração do ASA que executa o software versão 9.x:

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
```

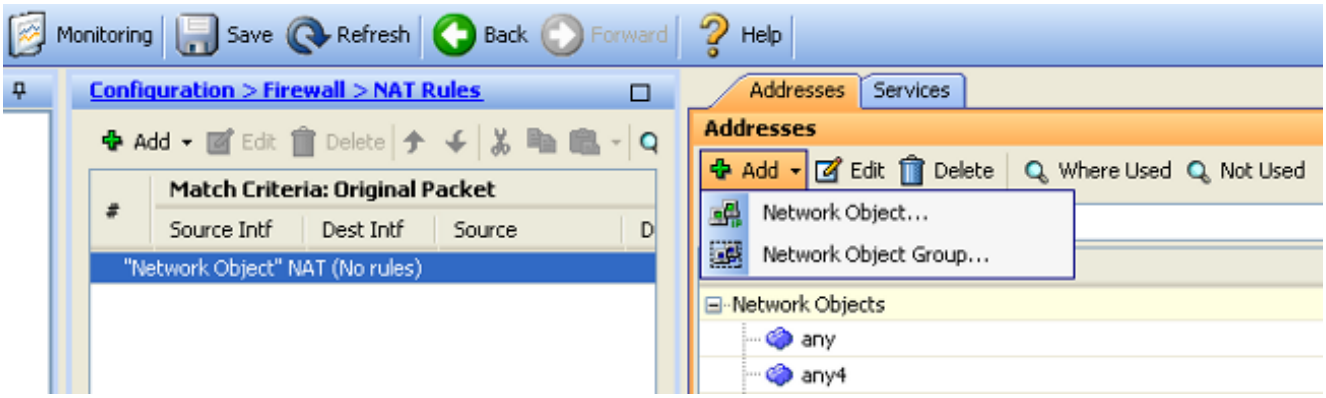
```
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

Permitir acesso de hosts internos a redes externas com PAT

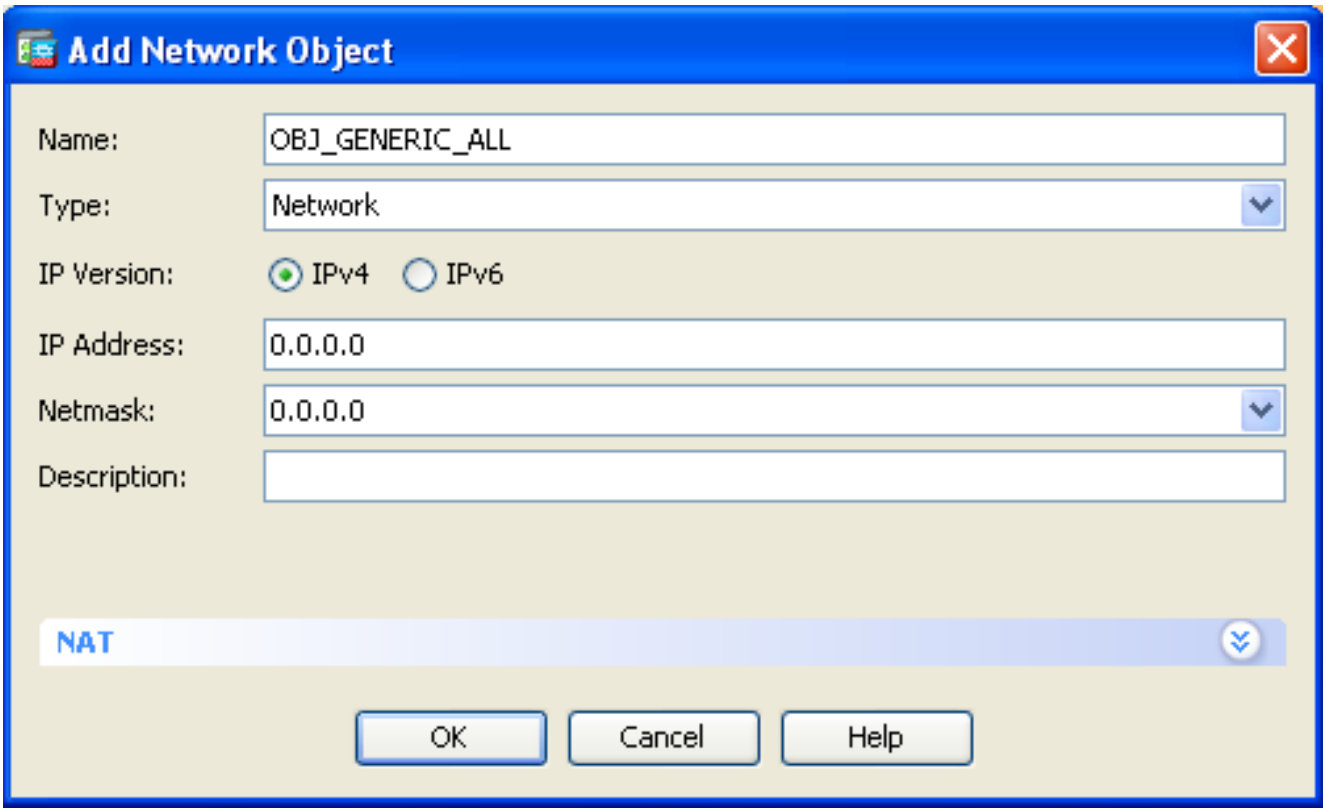
Se você pretende que os hosts internos compartilhem um único endereço público para tradução, use a Conversão de endereço de porta (PAT). Uma das configurações PAT mais simples envolve a conversão de todos os hosts internos para que eles pareçam ser o IP da interface externa. Essa é a configuração PAT típica usada quando o número de endereços IP roteáveis disponíveis no ISP é limitado a apenas alguns, ou apenas um.

Conclua estes passos para permitir que os hosts internos acessem as redes externas com PAT:

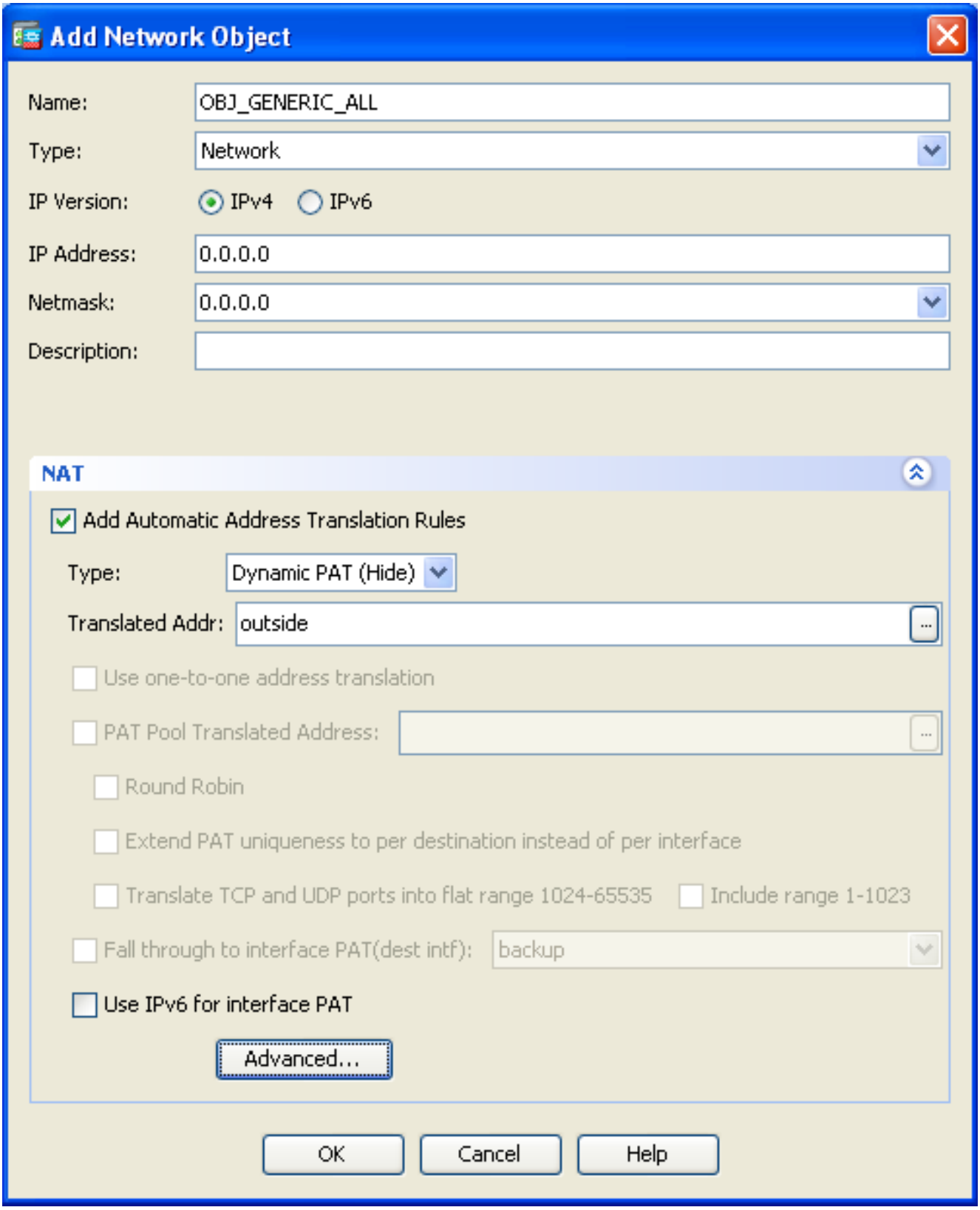
1. Navegue até Configuration > **Firewall** > **NAT Rules**, clique em **Add** e escolha **Network Object** para configurar uma regra de NAT dinâmica:



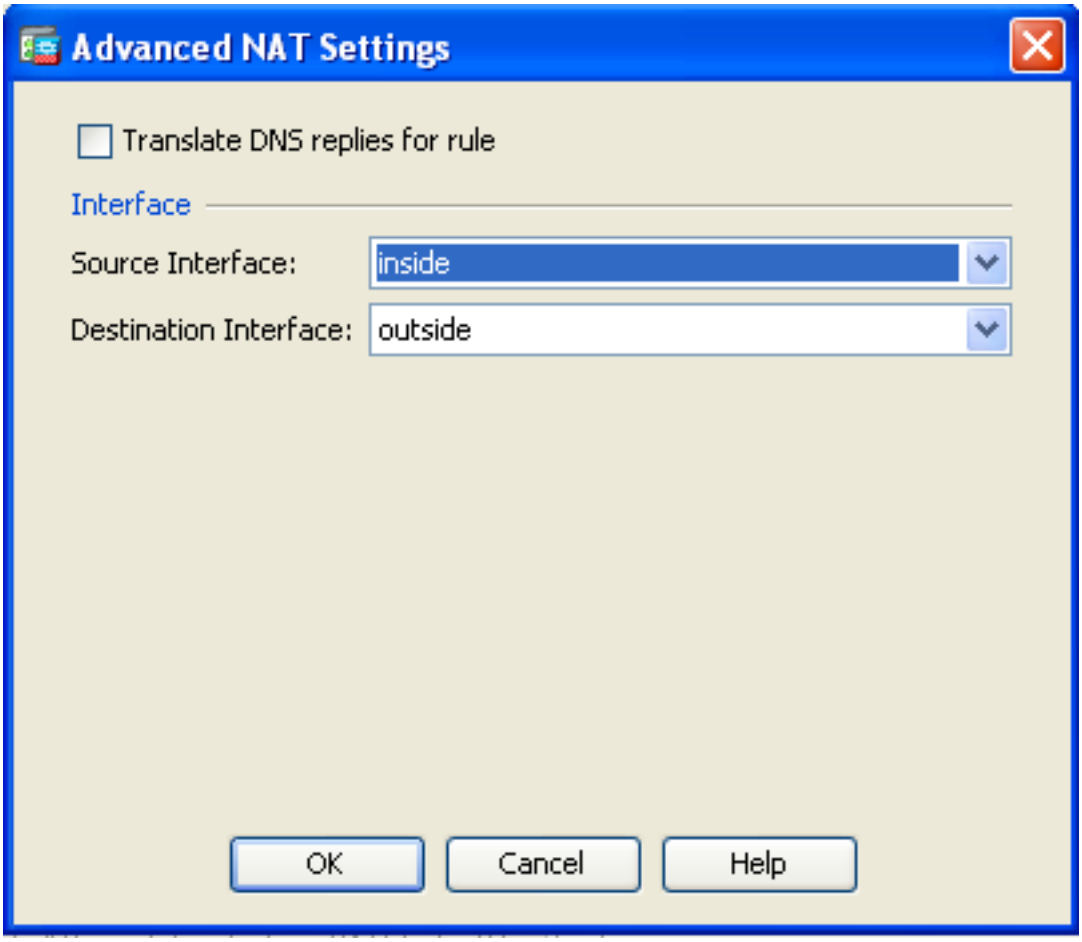
2. Configure a rede/host/intervalo para o qual o PAT dinâmico é necessário. Neste exemplo, todas as sub-redes internas foram selecionadas. Esse processo deve ser repetido para as sub-redes específicas que você deseja traduzir desta maneira:



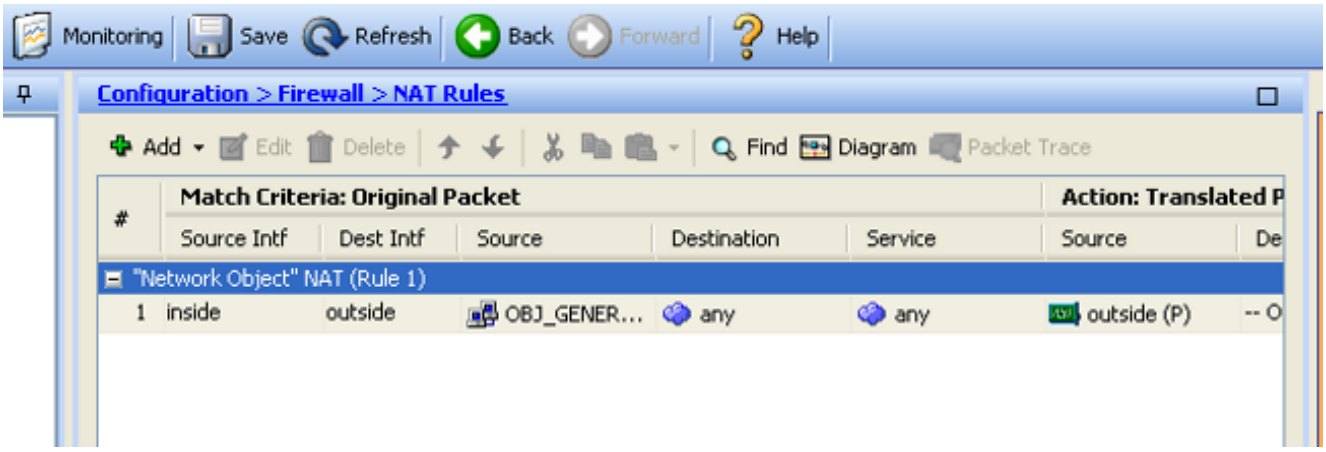
3. Clique em **NAT**, marque a caixa de seleção **Add Automatic Address Translation Rule**, digite **Dynamic (Dinâmico)** e defina a opção **Translated Addr (Endereço traduzido)** para que ela reflita a interface externa. Se você clicar no botão de reticências, ele o ajudará a escolher um objeto pré-configurado, como a interface externa:



4. Clique em **Avançado** para selecionar uma interface de origem e de destino:



5. Clique em **OK** e, em seguida, clique em **Aplicar** para aplicar as alterações. Quando concluído, o Adaptive Security Device Manager (ASDM) mostra a regra de NAT:



Configuração do Roteador B

Esta é a configuração para o Roteador B:

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

Verificar

Acesse um site via HTTP através de um navegador da Web para verificar se sua configuração funciona corretamente.

Este exemplo usa um site hospedado no endereço IP *198.51.100.100*. Se a conexão for bem-sucedida, as saídas fornecidas nas seções a seguir podem ser vistas na CLI do ASA.

Conexão

Insira o comando **show connection address** para verificar a conexão:

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

O ASA é um firewall stateful e o tráfego de retorno do servidor Web é permitido pelo firewall porque corresponde a uma ***conexão*** na tabela de conexão de firewall. O tráfego que corresponde a uma conexão pré-existente é permitido através do firewall sem ser bloqueado por uma ACL (Access Control List, lista de controle de acesso) de interface.

Na saída anterior, o cliente na interface interna estabeleceu uma conexão com o host 198.51.100.100 fora da interface externa. Essa conexão é feita com o protocolo TCP e está ociosa por seis segundos. Os sinalizadores de conexão indicam o estado atual dessa conexão.

> **Note**: Consulte o documento da Cisco ASA TCP Connection Flags (build-up and teardown da conexão) para obter mais informações sobre flags de conexão.

Troubleshoot

Use as informações descritas nesta seção para solucionar problemas de configuração.

Syslogs

Insira o comando **show log** para exibir os syslogs:

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:192.168.1.5/58799 (203.0.113.2/58799)
```

O firewall ASA gera syslogs durante a operação normal. Os syslogs variam na verbosidade com base na configuração de registro. A saída mostra dois syslogs que são vistos no nível seis ou no nível *informativo*.

Neste exemplo, há dois syslogs gerados. A primeira é uma mensagem de registro para indicar que o firewall criou uma tradução; especificamente, uma conversão TCP dinâmica (PAT). Indica o endereço IP origem e a porta, bem como o endereço IP e a porta convertidos, à medida que o tráfego passa de dentro para fora.

O segundo syslog indica que o firewall criou uma conexão em sua tabela de conexão para esse tráfego específico entre o cliente e o servidor. Se o firewall tiver sido configurado para bloquear esta tentativa de conexão, ou se algum outro fator tiver inibido a criação dessa conexão (restrições de recursos ou um possível erro de configuração), o firewall não gerará um log para indicar que a conexão foi criada. Em vez disso, registra um motivo para a conexão ser negada ou uma indicação em relação ao fator que inibiu a criação da conexão.

Packet Tracers

Insira este comando para ativar a funcionalidade do packet tracer:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

A funcionalidade do packet tracer no ASA permite especificar um pacote *simulado* e visualizar todas as várias etapas, verificações e funções que o firewall conclui quando processa o tráfego. Com essa ferramenta, é útil identificar um exemplo do tráfego que você acredita que *deve* ter permissão para passar pelo firewall e usar esse 5 tuplas para simular o tráfego. No exemplo anterior, o packet tracer é usado para simular uma tentativa de conexão que atenda a estes critérios:

- O pacote simulado chega à interface interna.
- O protocolo usado é o TCP.
- O endereço IP do cliente simulado é 192.168.1.5.
- O cliente envia tráfego originado da porta 1234.
- O tráfego é destinado a um servidor no endereço IP 198.51.100.100.
- O tráfego é destinado à porta 80.

Observe que não havia nenhuma menção da interface externa no comando. Isso se deve ao projeto do packet tracer. A ferramenta informa como o firewall processa esse tipo de tentativa de conexão, o que inclui como ele o rotearia e de qual interface.

> **Tip**: Para obter mais informações sobre a funcionalidade do packet tracer, consulte a seção Tracing packets with Packet Tracer do *Cisco ASA 5500 Series Configuration Guide usando CLI, 8.4 e 8.6*.

Captura

Insira estes comandos para aplicar uma captura:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100
```

```
ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

O firewall ASA pode capturar o tráfego que entra ou sai de suas interfaces. Essa funcionalidade de captura é fantástica porque pode provar definitivamente se o tráfego chega ou sai de um firewall. O exemplo anterior mostra a configuração de duas capturas chamadas **capin** e **capout** nas interfaces interna e externa, respectivamente. Os comandos **capture** usam a palavra-chave **match**, que permite especificar o tráfego que você deseja capturar.

Para o exemplo de captura *capin*, é indicado que você deseja corresponder o tráfego visto na interface interna (entrada ou saída) que corresponde ao *host tcp 192.168.1.5 host 198.51.100.100*. Em outras palavras, você deseja capturar qualquer tráfego TCP enviado do host *192.168.1.5* para o host *198.51.100.100*, ou vice-versa. O uso da palavra-chave **match** permite que o firewall capture esse tráfego bidirecionalmente. O comando **capture** definido para a interface externa não faz referência ao endereço IP do cliente interno porque o firewall conduz PAT nesse endereço IP do cliente. Como resultado, você não pode corresponder ao endereço IP do cliente. Em vez disso, este exemplo usa **qualquer um** para indicar que todos os possíveis endereços IP corresponderiam a essa condição.

Depois de configurar as capturas, você pode tentar estabelecer uma conexão novamente e continuar a visualizar as capturas com o comando **show capture*<capture_name>***. Neste exemplo, você pode ver que o cliente é capaz de se conectar ao servidor, como evidente pelo handshake triplo do TCP visto nas capturas.

Informações Relacionadas

- Cisco Adaptive Security Device Manager
- Firewalls de próxima geração Cisco ASA 5500-X Series
- Solicitações de comentários (RFC)
- Guia de configuração da CLI do Cisco ASA Series, 9,0 â Â Â Configurando rotas estáticas e padrão

- Suporte técnico e documentação â Â Cisco Systems