Entender a ordem de operação do NAT

Contents

Introduction

Este documento descreve que as transações de pedido são processadas com o NAT é baseado na direção em que um pacote trafega dentro ou fora da rede.

Prerequisites

Requirements

A Cisco recomenda ter conhecimento deste tópico:

- Tradução de Endereço de Rede (NAT). Para obter mais informações sobre NAT, consulte Como o NAT funciona.

Componentes Utilizados

As informações neste documento são baseadas no Cisco IOS® Software Release 12.2(27).

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

Informações de Apoio

Este documento descreve que a ordem em que as transações são processadas com a Network Address Translation (NAT) é baseada em se um pacote vai da rede interna para a rede externa

ou da rede externa para a rede interna.

Visão geral de NAT

Nesta tabela, quando o NAT executa a conversão de global para local ou de local para global, ela é diferente em cada fluxo.

De dentro para fora

- Se for IPSec, verifique a lista de acesso de entrada
- descriptografia - para CET (Cisco Encryption Technology) ou IPSec
- check input access list
- verificar limites de taxa de entrada
- input accounting
- redirecionar para o cache da Web
- roteamento de política
- roteamento
- **NAT de dentro para fora (tradução de local para global)**
- crypto (verifique o mapa e a marca para criptografia)
- verificar lista de acesso de saída
- inspecionar (Controle de acesso baseado em contexto (CBAC))
- Interceptação de TCP
- criptografia
- fila

De fora para dentro

- Se for IPSec, verifique a lista de acess entrada
- descriptografia - para CET ou IPSec
- check input access list
- verificar limites de taxa de entrada
- input accounting
- redirecionar para o cache da Web
- **NAT de fora para dentro (conversão gl para local)**
- roteamento de política
- roteamento
- crypto (verifique o mapa e a marca par criptografia)
- verificar lista de acesso de saída
- inspecionar CBAC
- Interceptação de TCP
- criptografia
- fila

Configuração e saída de NAT

Este exemplo demonstra como a ordem das operações pode afetar o NAT. Nesse caso, apenas a NAT e o roteamento são mostrados.

No exemplo anterior, o Roteador-A está configurado para converter o endereço local interno 172.31.200.48 em 172.16.47.150, como mostrado nesta configuração.

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
enable password ww
!
ip nat inside source static 172.31.200.48 172.16.47.150

!--- This command creates a static NAT translation
!--- between 172.31.200.48 and 172.16.47.150 ip domain-name cisco.com ip name-server
172.31.2.132 ! interface Ethernet0 no ip address shutdown ! interface Serial0 ip address
172.16.47.161 255.255.255.240 ip nat inside
```

```
!--- Configures Serial0 as the NAT inside interface no ip mroute-cache no ip route-cache no
fair-queue ! interface Serial1 ip address 172.16.47.146 255.255.255.240 ip nat outside

!--- Configures Serial1 as the NAT outside interface no ip mroute-cache no ip route-cache ! no
ip classless ip route 0.0.0.0 0.0.0.0 172.16.47.145

!--- Configures a default route to 172.16.47.145 ip route 172.31.200.0 255.255.255.0
172.16.47.162 ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
```

A tabela de tradução indica que a tradução pretendida existe.

```
Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

Essa saída é obtida do Router-A com **debug ip packet detail** e **debug ip nat** habilitados, e um ping emitido do dispositivo 172.31.200.48 destinado a 172.16.47.142.

> **Observação**: os comandos de depuração geram uma quantidade significativa de saída. Use-os apenas quando o tráfego na rede IP estiver baixo, de modo que outra atividade no sistema não seja afetada de forma desfavorável. Antes de emitir comandos de depuração, consulte Informações importantes sobre Comandos de Depuração.

```
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
```

Como não há mensagens de depuração NAT na saída anterior, a conversão estática atual não é usada e o roteador não tem uma rota para o endereço de destino (172.16.47.142) em sua tabela de roteamento. O resultado de um pacote não roteável é uma mensagem que não chega a seu destino do ICMP, a qual é enviada para o dispositivo interno.

Mas o Roteador-A tem uma rota padrão 172.16.47.145, então por que a rota é considerada não roteável?

O Roteador-A **não tem ip classless** configurado, o que significa que se um pacote destinado a um endereço de rede "principal" (neste caso, 172.16.0.0) para o qual as sub-redes existem na tabela de roteamento, o roteador não confia na rota padrão. Em outras palavras, se você executar o comando **no ip classless**, isso desativará a capacidade do roteador de procurar a rota com a maior correspondência de bits. Para alterar esse comportamento, você precisa configurar **ip classless** no Router-A. O comando **ip classless** é ativado por padrão nos roteadores Cisco com Cisco IOS Software Releases 11.3 e posteriores.

```
Router-A#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Router-A(config)#ip classless
Router-A(config)#end

Router-A#show ip nat translation
%SYS-5-CONFIG_I: Configured from console by console nat tr
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

Quando você repete o mesmo teste de ping feito anteriormente, você vê que o pacote é convertido e o ping é bem-sucedido.

```
Ping Response on device 172.31.200.48

D:\>ping 172.16.47.142
Pinging 172.16.47.142 with 32 bytes of data:

Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.47.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms

Debug messages on Router A indicating that the packets generated by device
172.31.200.48 are getting translated by NAT.

Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=172.31.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
 g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [161]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [162]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [163]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
```

```
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [164]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0

Router-A#undebug all
All possible debugging has been turned off
```

O exemplo anterior mostra que, quando um pacote atravessa de dentro para fora, um roteador NAT verifica sua tabela de roteamento em busca de uma rota para o endereço externo antes de continuar a converter o pacote. Portanto, é importante que o roteador NAT tenha uma rota válida para a rede externa. A rota para a rede destino deve ser conhecida por meio de uma interface definida como NAT externo na configuração do roteador.

Éimportante observar que os pacotes de retorno são convertidos antes de serem roteados. Por isso, o NAT Router também deve ter uma rota válida para o endereço interno local em sua tabela de roteamento.

Informações Relacionadas

- Configurando a tradução de endereço de rede
- Verificando a Operação de NAT e Troubleshooting Básico de NAT
- NAT: Definições locais e globais
- Como o NAT multicast funciona nos roteadores Cisco?
- Página de suporte de NAT
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.