# Solucionar problemas de configuração de conversão de endereço de rede (NAT) ASA

## Contents



## Introdução

Este documento descreve como solucionar problemas de configuração da conversão de endereço de rede (NAT) na plataforma Cisco Adaptive Security Appliance (ASA).

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

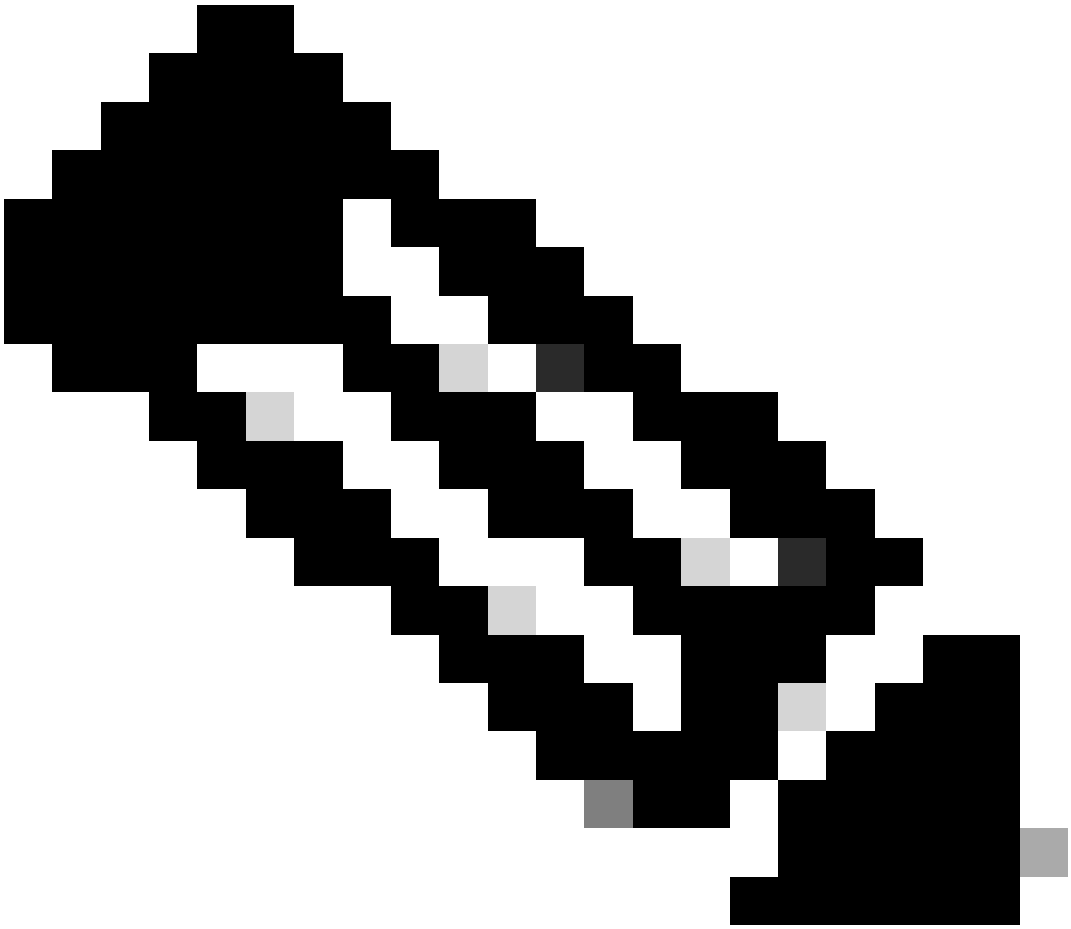
### Componentes Utilizados

As informações neste documento são baseadas no ASA versão 8.3 e posterior.

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 rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

## Solucionar problemas de configuração de NAT no ASA



> Observação: para obter alguns exemplos básicos de configurações NAT, que incluem um vídeo que mostra uma configuração NAT básica, consulte a seção Informações Relacionadas na parte inferior deste documento.

Ao solucionar problemas de configurações de NAT, é importante entender como a configuração de NAT no ASA é usada para criar a tabela de políticas de NAT.

Esses erros de configuração são responsáveis pela maioria dos problemas de NAT encontrados pelos administradores do ASA:

- As regras de configuração do NAT estão fora de ordem. Por exemplo, uma regra NAT manual é colocada na parte superior da tabela NAT, o que faz com que regras mais específicas colocadas mais abaixo na tabela NAT nunca sejam atingidas.

- Os objetos de rede usados na configuração NAT são muito amplos, o que faz com que o tráfego corresponda inadvertidamente a essas regras NAT e perca regras NAT mais específicas.

O utilitário packet tracer pode ser usado para diagnosticar a maioria dos problemas relacionados ao NAT no ASA. Consulte a próxima seção para obter mais informações sobre como a configuração de NAT é usada para criar a tabela de política de NAT e como solucionar problemas específicos de NAT.

Além disso, o comando show nat detail pode ser usado para entender quais regras de NAT são atingidas por novas conexões.

# Como a configuração do ASA é usada para criar a tabela de políticas de NAT

Todos os pacotes processados pelo ASA são avaliados na tabela NAT. Essa avaliação começa na parte superior (Seção 1) e funciona até que uma regra de NAT seja correspondida.

Em geral, uma vez que uma regra de NAT é correspondida, essa regra de NAT é aplicada à conexão e nenhuma outra política de NAT é verificada em relação ao pacote, mas há algumas advertências explicadas a seguir.

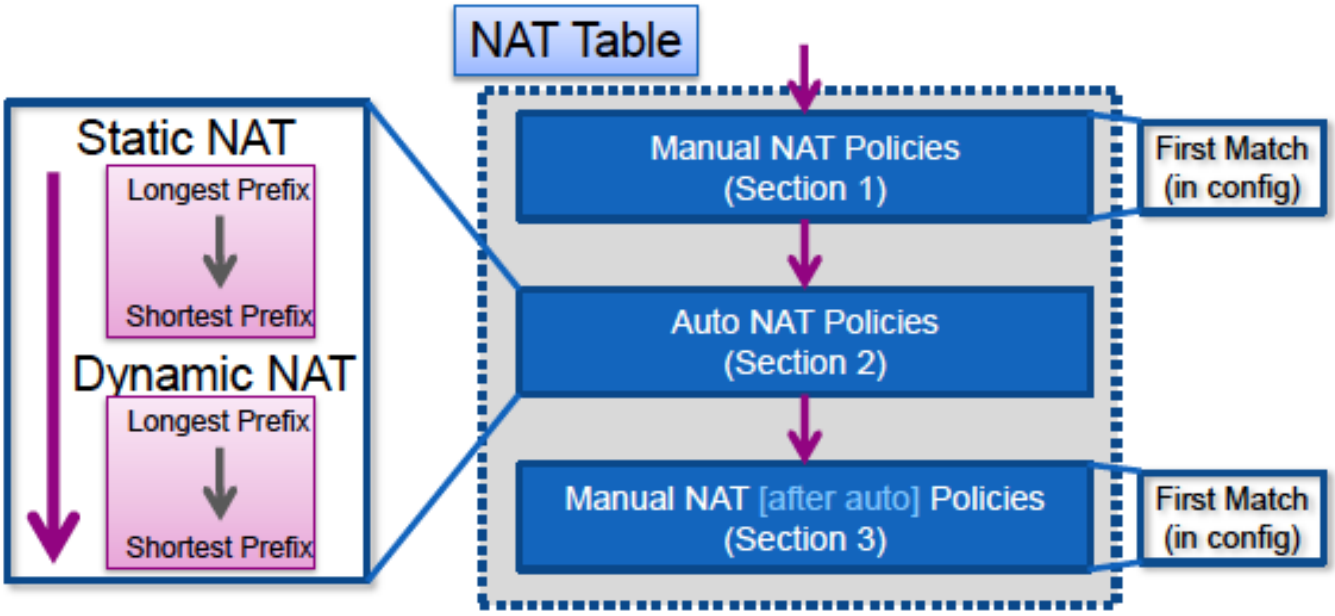
A tabela de políticas de NAT

A política NAT no ASA é criada a partir da configuração NAT.

As três seções da tabela NAT do ASA são:

| | |
|---|---|
| Seção 1 | Políticas manuais de NAT<br>Eles são processados na ordem em que aparecem na configuração. |
| Seção 2 | Políticas de NAT automático<br>Eles são processados com base no tipo de NAT (estático ou dinâmico) e no comprimento do prefixo (máscara de sub-rede) no objeto. |
| Seção 3 | Políticas de NAT manual pós-automático<br>Eles são processados na ordem em que aparecem na configuração. |

Este diagrama mostra as diferentes seções de NAT e como elas são ordenadas:




Correspondência de regra NAT

Seção 1

- Um fluxo é avaliado primeiro em relação à seção 1 da tabela NAT que começa com a primeira regra.
    - Se o IP origem e destino do pacote corresponderem aos parâmetros da regra NAT manual, a conversão será aplicada e o processo será interrompido, e nenhuma outra regra NAT em nenhuma seção será avaliada.
    - Se nenhuma regra NAT for correspondida, o fluxo será avaliado em relação à seção 2 da tabela NAT.

Seção 2

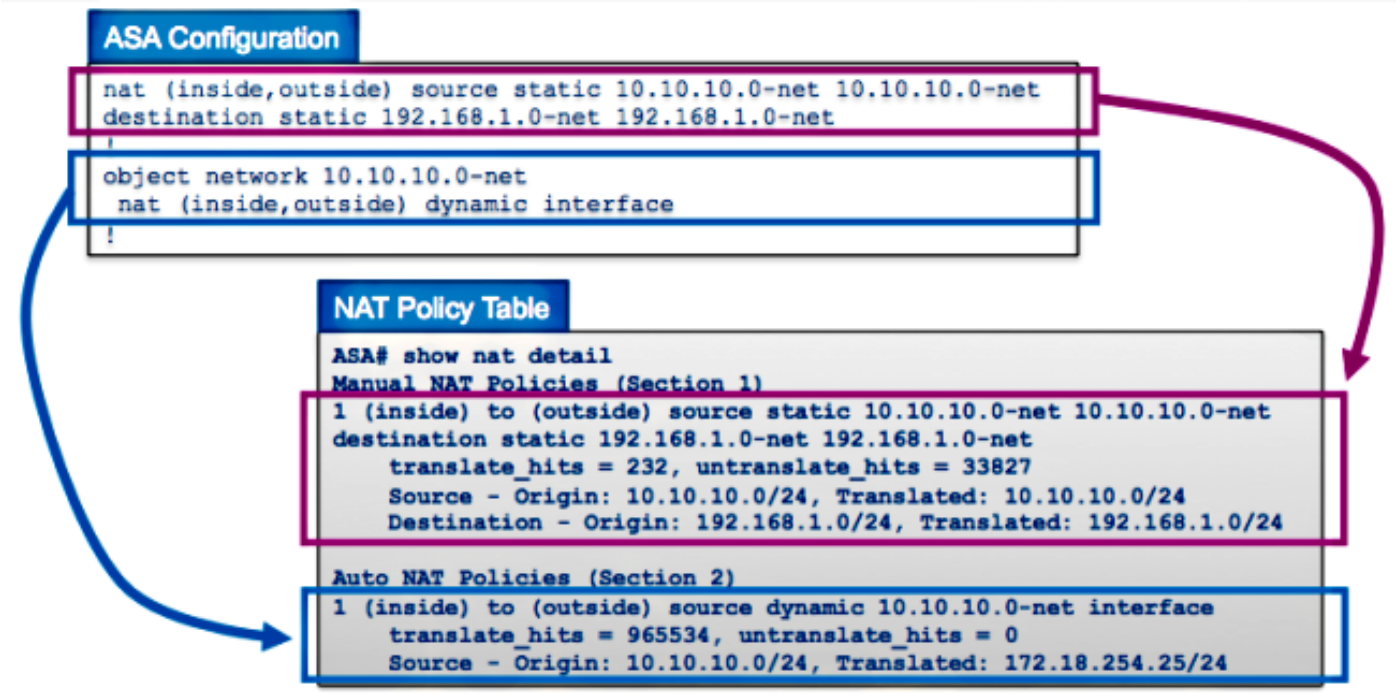
- Um fluxo é avaliado em relação às regras de NAT da seção 2 na ordem especificada anteriormente, primeiro as regras de NAT estático e, em seguida, as regras de NAT dinâmico.
    - Se uma regra de conversão corresponder ao IP de origem ou de destino do fluxo, a conversão poderá ser aplicada e o restante das regras poderá continuar a ser avaliado para ver se elas correspondem ao outro IP no fluxo. Por exemplo, uma regra de NAT automático pode converter o IP de origem e outra regra de NAT automático pode converter o destino.
    - Se o fluxo corresponder a uma regra de NAT automático, quando o final da seção 2 for alcançado, a pesquisa de NAT será interrompida e as regras da seção 3 não serão avaliadas.
    - Se nenhuma regra de NAT da seção 2 corresponder ao fluxo, a pesquisa prosseguirá para a seção 3

Seção 3

- O processo descrito na seção 3 é essencialmente o mesmo que o descrito na seção 1. Se o

IP origem e destino do pacote corresponderem aos parâmetros da regra NAT manual, a conversão será aplicada e o processo será interrompido, e nenhuma outra regra NAT em nenhuma seção será avaliada.

Este exemplo mostra como a configuração NAT do ASA com duas regras (uma instrução NAT manual e uma configuração NAT automática) são representadas na tabela NAT:




# Como solucionar problemas de NAT

## Usar o utilitário Packet Tracer

Para solucionar problemas com as configurações de NAT, use o utilitário packet tracer para verificar se um pacote atinge a política de NAT. O Packet Tracer permite especificar um pacote de exemplo que entra no ASA, e o ASA indica qual configuração se aplica ao pacote e se é permitido ou não.

No próximo exemplo, um pacote TCP de exemplo que entra na interface interna e é destinado a um host na Internet é fornecido. O utilitário packet tracer mostra que o pacote corresponde a uma regra NAT dinâmica e é convertido no endereço IP externo de 172.16.123.4:

<#root>

ASA#

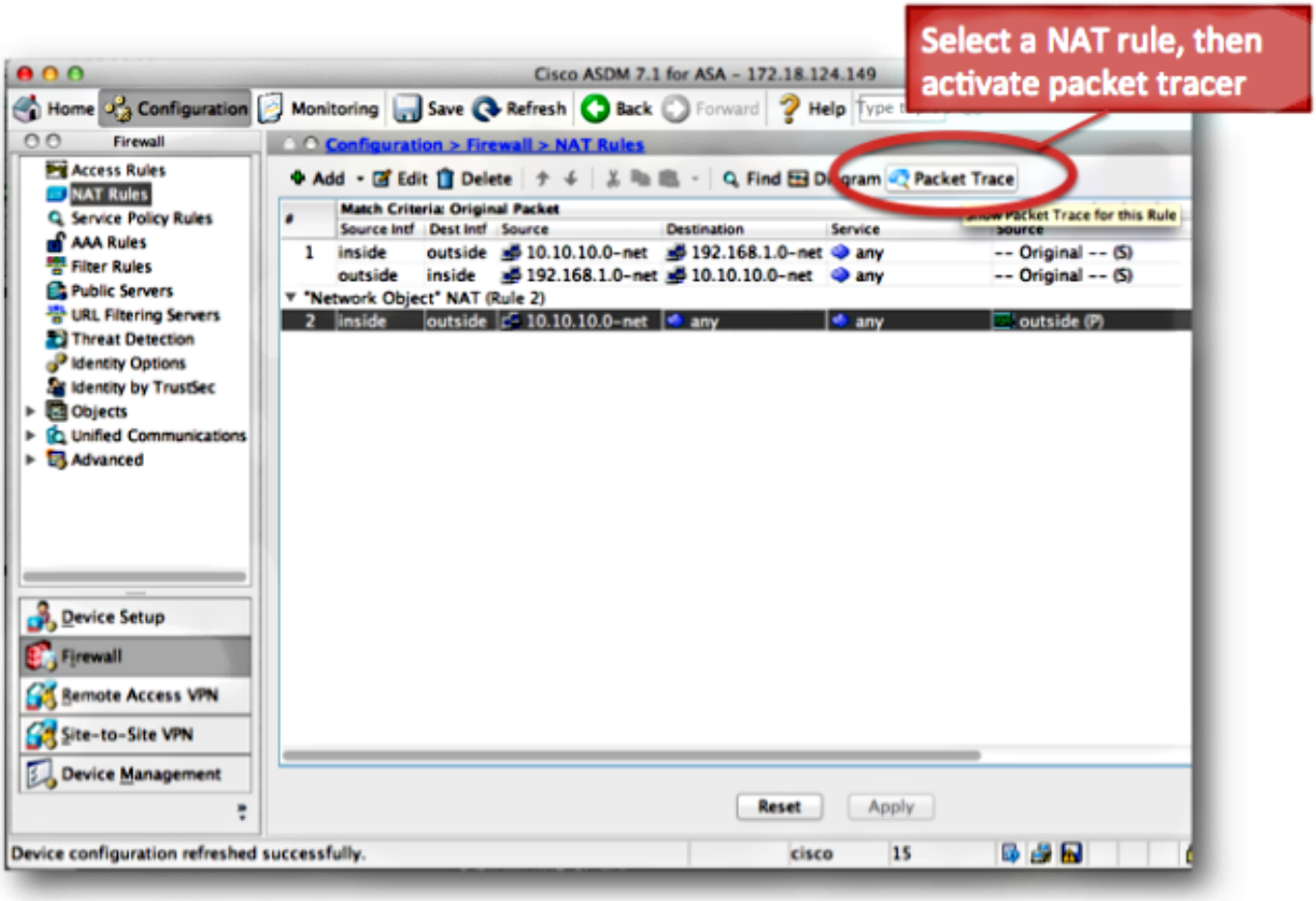
**packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80**

...(output omitted)...

Phase: 2
Type: NAT

```
Subtype:
Result: ALLOW
Config:

object network 10.10.10.0-net
 nat (inside,outside) dynamic interface


Additional Information:
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345

...(output omitted)...

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up

Action: allow


ASA#
```

Escolha a regra NAT e clique em Packet Trace para ativar o packet tracer no Cisco Adaptive Security Device Manager (ASDM). Isso usa os endereços IP especificados na regra NAT como as entradas para a ferramenta packet tracer:

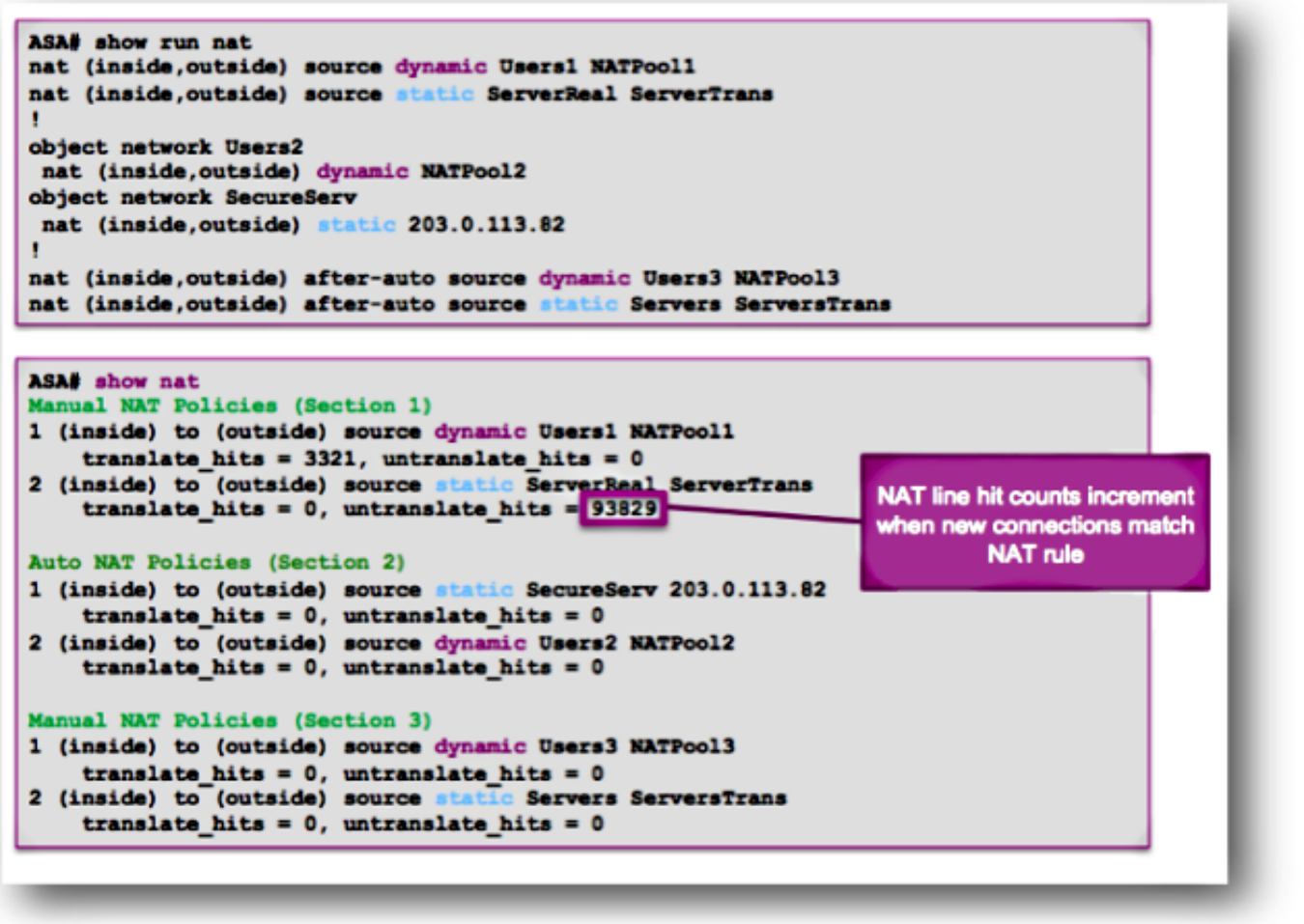



## Visualizar a saída do comando show nat

A saída do comando show nat detail pode ser usada para exibir a tabela de políticas de NAT. Especificamente, os contadores translate_hits e untranslate_hits podem ser usados para determinar quais entradas NAT são usadas no ASA.

Se você vir que sua nova regra de NAT não tem translate_hits ou untranslate_hits, isso significa que o tráfego não chega ao ASA ou talvez uma regra diferente que tenha uma prioridade mais alta na tabela de NAT corresponda ao tráfego.

Aqui está a configuração NAT e a tabela de política NAT de uma configuração ASA diferente:




No exemplo anterior, há seis regras de NAT configuradas nesse ASA. A saída do comando show nat mostra como essas regras são usadas para criar a tabela de política NAT, bem como o número de translate_hits e untranslate_hits para cada regra.

Esses contadores de ocorrências incrementam apenas uma vez por conexão. Depois que a conexão é criada por meio do ASA, os pacotes subsequentes que correspondem a essa conexão atual não incrementam as linhas NAT (assim como as contagens de acessos à lista de acesso funcionam no ASA).

Translate_hits: o número de novas conexões que correspondem à regra NAT na direção forward.

"Direção de encaminhamento" significa que a conexão foi criada através do ASA na direção das interfaces especificadas na regra NAT.

Se uma regra NAT especificar que o servidor interno é convertido para a interface externa, a ordem das interfaces na regra NAT é "nat (inside,outside)..."; se esse servidor iniciar uma nova conexão com um host externo, o contador translate_hit será incrementado.

Untranslate_hits: O número de novas conexões que correspondem à regra NAT na direção inversa.

Se uma regra NAT especifica que o servidor interno é convertido para a interface externa, a ordem das interfaces na regra NAT é "nat (inside,outside)..."; se um cliente na parte externa do

ASA inicia uma nova conexão com o servidor na parte interna, o contador untranslate_hit é incrementado.

Novamente, se você vir que sua nova regra de NAT não tem translate_hits ou untranslate_hits, isso significa que o tráfego não chega ao ASA ou talvez uma regra diferente que tenha uma prioridade mais alta na tabela de NAT corresponda ao tráfego.

### Metodologia de Troubleshooting de NAT

Use o packet tracer para confirmar se um pacote de exemplo corresponde à regra de configuração de NAT apropriada no ASA. Use o comando show nat detail para entender quais regras de política de NAT são atingidas. Se uma conexão corresponder a uma configuração de NAT diferente da esperada, solucione os problemas com estas perguntas:

- Há uma regra NAT diferente que tenha precedência sobre a regra NAT que você pretendia que o tráfego atingisse?
- Existe uma regra NAT diferente com definições de objeto muito amplas (a máscara de sub-rede é muito curta, como 255.0.0.0) que faz com que esse tráfego corresponda à regra errada?
- As políticas manuais de NAT estão fora de ordem, o que faz com que o pacote corresponda à regra errada?
- Sua regra NAT está configurada incorretamente, o que faz com que a regra não corresponda ao seu tráfego?

Consulte a próxima seção para obter exemplos de problemas e soluções.

## Problemas comuns com configurações de NAT

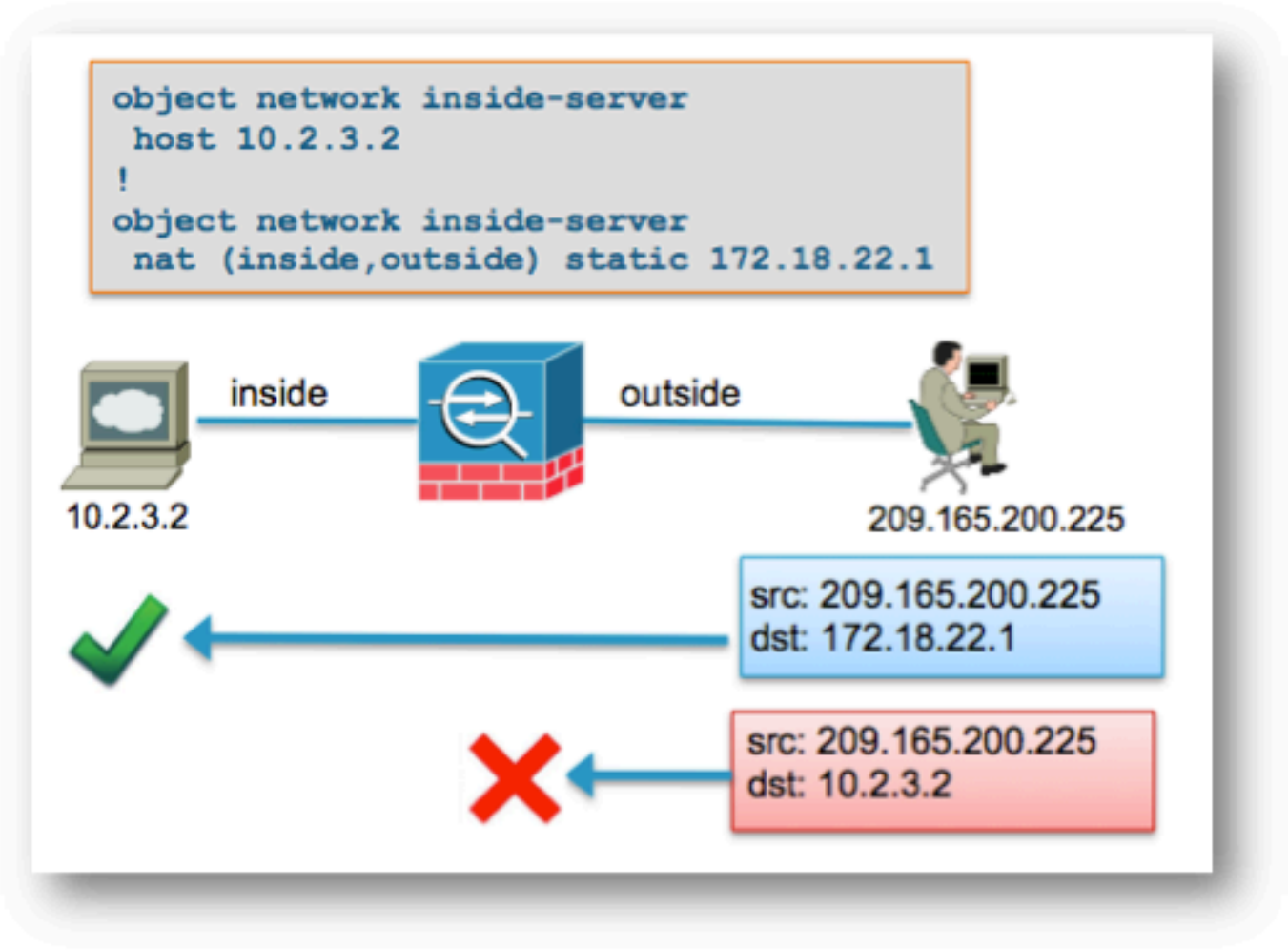
Aqui estão alguns problemas comuns enfrentados quando você configura o NAT no ASA.

### Problema: o tráfego falha devido a RPF (falha de caminho reverso) de NAT Erro: Regras de NAT assimétricas correspondentes para fluxos de encaminhamento e de retorno

A verificação de RPF de NAT garante que uma conexão que é convertida pelo ASA na direção de encaminhamento, como a sincronização de TCP (SYN), seja convertida pela mesma regra de NAT na direção inversa, como a SYN/confirmação TCP (ACK).

Mais comumente, esse problema é causado por conexões de entrada destinadas ao endereço local (não traduzido) em uma instrução NAT. Em um nível básico, o NAT RPF verifica se a conexão reversa do servidor para o cliente corresponde à mesma regra NAT; se não corresponder, a verificação do NAT RPF falhará.

Exemplo: 209.165.200.225




Quando o host externo em 192.168.200.225 envia um pacote destinado diretamente ao endereço IP local (não convertido) de 10.2.3.2, o ASA descarta o pacote e registra este syslog:

```
%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure
```

Solução:

Primeiro, certifique-se de que o host envie dados para o endereço NAT global correto. Se o host enviar pacotes destinados ao endereço correto, verifique as regras de NAT que são atingidas pela conexão.

Verifique se as regras de NAT estão definidas corretamente e se os objetos referenciados nas regras de NAT estão corretos. Verifique também se a ordem das regras de NAT é apropriada.

Use o utilitário packet tracer para especificar os detalhes do pacote negado. O Packet Tracer deve mostrar o pacote descartado devido à falha de verificação de RPF.

Em seguida, observe a saída do packet tracer para ver quais regras de NAT são atingidas na fase

NAT e na fase NAT-RPF.

Se um pacote corresponder a uma regra de NAT na fase de verificação de RPF de NAT, que indica que o fluxo reverso atingiria uma conversão de NAT, mas não corresponde a uma regra na fase de NAT, que indica que o fluxo de encaminhamento NÃO atingiria uma regra de NAT, o pacote será descartado.

Essa saída corresponde ao cenário mostrado no diagrama anterior, em que o host externo envia incorretamente o tráfego para o endereço IP local do servidor e não para o endereço IP global (convertido):

```
<#root>

ASA#

packet-tracer input outside tcp 192.168.200.225 1234 10.2.3.2 80



    .....

Phase: 8
Type: NAT
Subtype: rpf-check
Result:

DROP


Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

Quando o pacote é destinado ao endereço IP mapeado correto de 172.18.22.1, o pacote corresponde à regra NAT correta na fase UN-NAT na direção de encaminhamento e à mesma regra na fase de verificação de RPF de NAT:

```
<#root>

ASA(config)#

packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80


...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
```

```
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result:
```

**ALLOW**

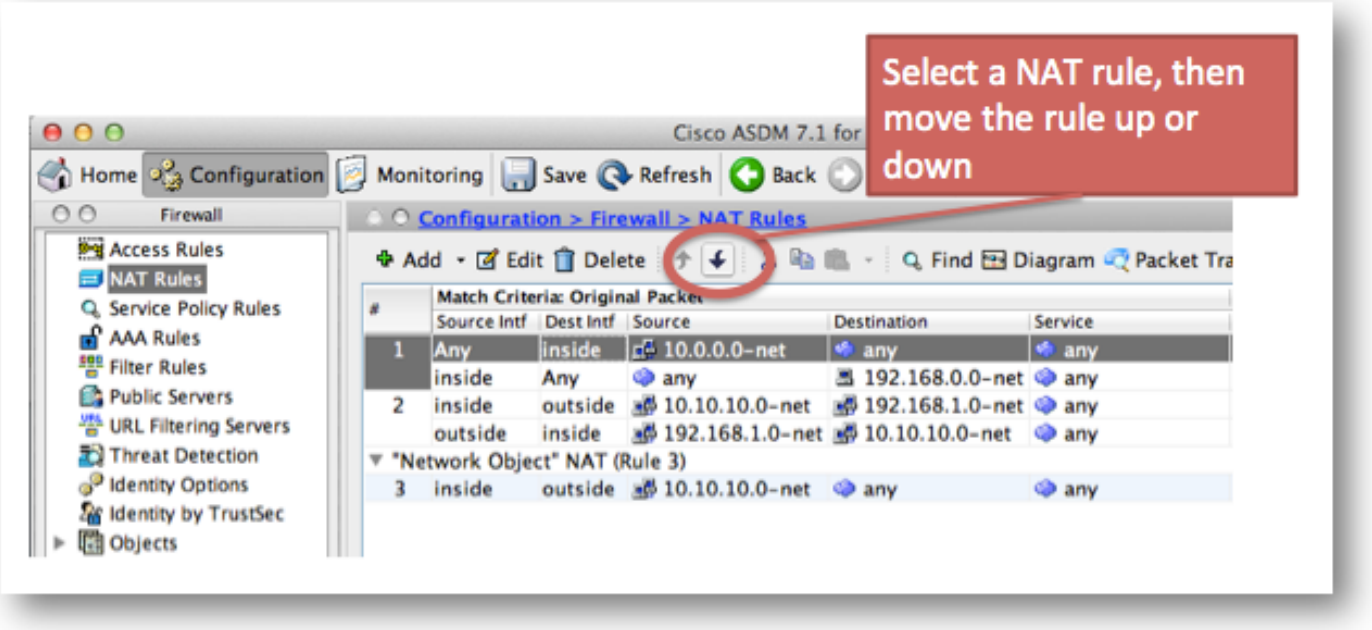
```
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

## Problema: as regras de NAT manual estão fora de ordem, o que causa correspondências de pacotes incorretas

As regras de NAT manuais são processadas com base em sua aparência na configuração. Se uma regra NAT muito ampla for listada primeiro na configuração, ela poderá substituir outra regra mais específica na tabela NAT. Use o packet tracer para verificar qual regra de NAT seu tráfego atinge; pode ser necessário reorganizar as entradas de NAT manuais em uma ordem diferente.

Solução:

Reordene as regras de NAT com o ASDM.




Solução:

As regras de NAT podem ser reordenadas com a CLI se você remover a regra e reinseri-la em um número de linha específico. Para inserir uma nova regra em uma linha específica, insira o número da linha logo após as interfaces serem especificadas.

Exemplo:

<#root>

ASA(config)#

**nat (inside,outside) *1* source static 10.10.10.0-net**
**10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net**

## Problema

Uma regra NAT é muito ampla e corresponde a algum tráfego inadvertidamente. Às vezes, são criadas regras de NAT que usam objetos muito amplos. Se essas regras forem colocadas perto da parte superior da tabela NAT (na parte superior da Seção 1, por exemplo), elas poderão corresponder mais tráfego do que o esperado e fazer com que as regras NAT mais abaixo na tabela nunca sejam atingidas.

Solução

Use o packet tracer para determinar se o tráfego corresponde a uma regra com definições de objeto muito amplas. Se esse for o caso, você deve reduzir o escopo desses objetos ou mover as regras para mais longe na tabela NAT ou para a seção after-auto (Seção 3) da tabela NAT.

## Problema

Uma regra NAT desvia o tráfego para uma interface incorreta. As regras de NAT podem ter precedência sobre a tabela de roteamento quando determinam qual interface um pacote sai do ASA. Se um pacote de entrada corresponder a um endereço IP convertido em uma instrução NAT, a regra NAT será usada para determinar a interface de saída.

A verificação de desvio de NAT (que é o que pode substituir a tabela de roteamento) verifica se há alguma regra de NAT que especifique a conversão do endereço de destino para um pacote de entrada que chega em uma interface.

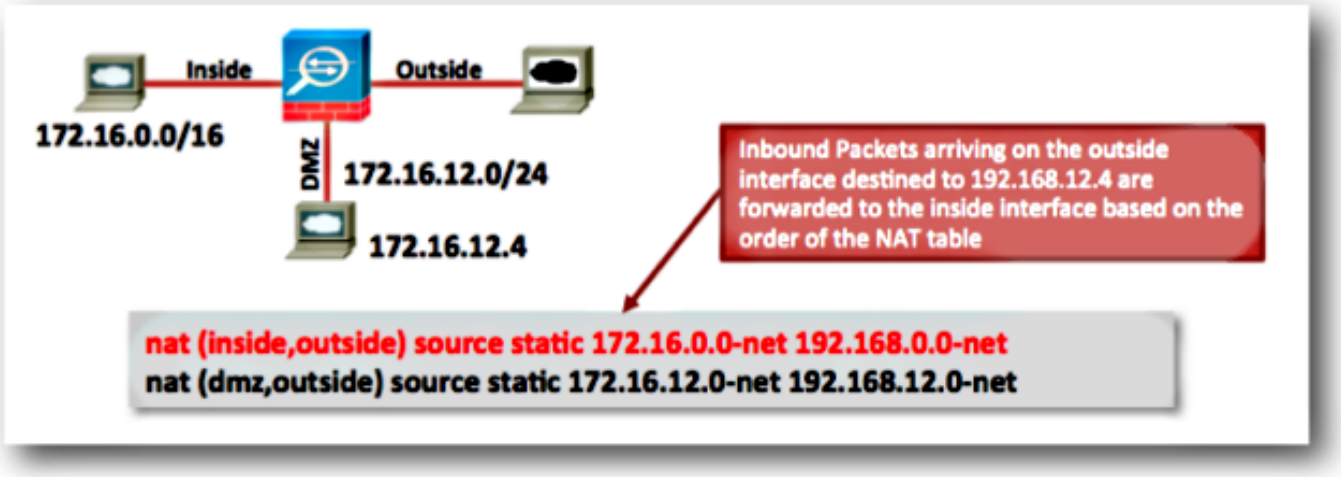
Se não houver uma regra que especifique explicitamente como converter esse endereço IP de destino do pacote, a tabela de roteamento global será consultada para determinar a interface de saída.

Se houver uma regra que especifique explicitamente como converter o endereço IP de destino do pacote, a regra NAT extrairá o pacote para a outra interface na conversão e a tabela de roteamento global será efetivamente ignorada.

Esse problema é visto com mais frequência no tráfego de entrada, que chega à interface externa,

e geralmente é devido a regras de NAT fora de ordem que desviam o tráfego para interfaces não intencionais.

Exemplo:




Soluções:

Esse problema pode ser resolvido com uma destas ações:

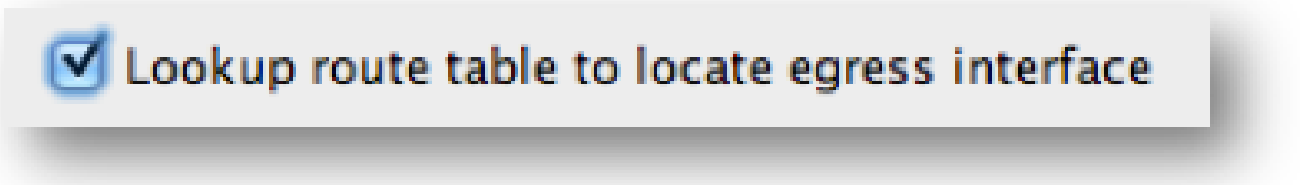
- Reordene a tabela NAT para que a entrada mais específica seja listada primeiro.
- Use intervalos de endereços IP globais sem sobreposição para as instruções NAT.

Observe que, se a regra NAT for uma regra de identidade (o que significa que os endereços IP não são alterados pela regra), a palavra-chave route-lookup poderá ser usada (essa palavra-chave não é aplicável ao exemplo anterior, já que a regra NAT não é uma regra de identidade).

A palavra-chave route-lookup faz com que o ASA execute uma verificação extra quando ele corresponder a uma regra de NAT. Verifica se a tabela de roteamento do ASA encaminha o pacote para a mesma interface de saída para a qual essa configuração de NAT desvia o pacote.

Se a interface de saída da tabela de roteamento não corresponder à interface de desvio NAT, a regra NAT não será correspondida (a regra será ignorada) e o pacote continuará na tabela NAT para ser processado por uma regra NAT posterior.

A opção route-lookup só estará disponível se a regra NAT for uma regra NAT de identidade, o que significa que os endereços IP não são alterados pela regra. A opção route-lookup pode ser habilitada por regra NAT se você adicionar route-lookup ao final da linha NAT ou se você marcar a caixa de seleção Lookup route table para localizar a interface de saída na configuração de regra NAT no ASDM:




## Problema: uma regra de NAT faz com que o ASA use o Proxy Address Resolution Protocol (ARP) para o tráfego na interface mapeada

O ASA Proxy ARPs para o intervalo de endereço IP global em uma instrução NAT na interface global. Essa funcionalidade Proxy ARP pode ser desativada em uma base de regra por NAT se você adicionar a palavra-chave no-proxy-arp à instrução NAT.

Esse problema também é visto quando a sub-rede de endereço global é inadvertidamente criada para ser muito maior do que deveria ser.

Solução

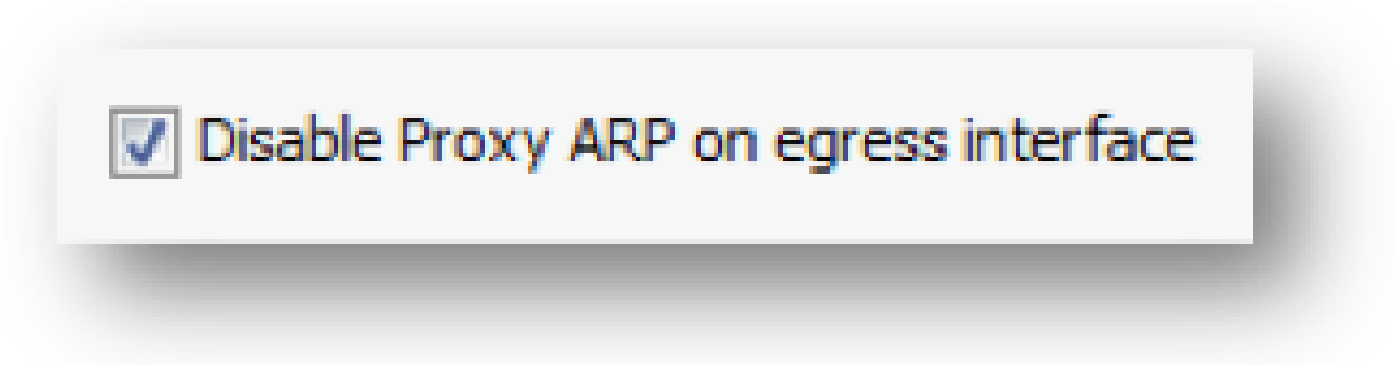
Adicione a palavra-chave no-proxy-arp à linha NAT, se possível.

Exemplo:

<#root>

```
ASA(config)#

object network inside-server

ASA(config-network-object)#

nat (inside,outside) static 172.18.22.1 no-proxy-arp

ASA(config-network-object)#

end

ASA#
  ASA#

 show run nat

object network inside-server
 nat (inside,outside) static 172.18.22.1

no-proxy-arp

ASA#
```

Isso também pode ser feito com o ASDM. Na regra NAT, marque a caixa de seleção Disable Proxy ARP on egress interface.




.

## Informações Relacionadas

- VÍDEO: Encaminhamento de porta ASA para acesso ao servidor DMZ (versões 8.3 e 8.4)
- Configuração básica de NAT do ASA: servidor Web no DMZ no ASA versão 8.3 e posterior
- Livro 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1
- 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.