Troubleshooting da configuração da tradução de endereço de rede ASA

Índice

[Introdução](#)
[Pesquise defeitos a configuração de NAT no ASA](#)
[Como a configuração ASA é usada para construir a tabela da política de NAT](#)
[Como pesquisar defeitos problemas NAT](#)
[Use a utilidade do projétil luminoso do pacote](#)
[Veja a saída do comando show nat](#)
[Metodologia de Troubleshooting do problema NAT](#)
[Problemas comuns com configurações de NAT](#)
[Problema: O tráfego falha devido ao erro da falha do caminho reverso NAT (RPF): Regras assimétricas NAT combinadas para dianteiro e fluxos reversos](#)
[Problema: As regras manuais NAT são foras de serviço, que causa fósforos do pacote incorreto](#)
[Problema: Uma regra NAT é demasiado larga e combina algum tráfego inadvertidamente](#)
[Problema: Uma regra NAT desvia o tráfego a uma interface incorreta](#)
[Problema: Uma regra NAT causa o ASA ao protocolo proxy address resolution (ARP) para o tráfego na relação traçada](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como pesquisar defeitos a configuração do Network Address Translation (NAT) na plataforma adaptável da ferramenta de segurança de Cisco (ASA). Este documento é válido para a versão ASA 8.3 e mais atrasado.

> **Note**: Para alguns exemplos básicos das configurações de NAT, que incluem um vídeo que mostre uma configuração de NAT básica, veja a informação relacionada da seção na parte inferior deste documento.

Pesquise defeitos a configuração de NAT no ASA

Quando você pesquisa defeitos configurações de NAT, é importante compreender como a configuração de NAT no ASA é usada para construir a tabela da política de NAT.

Estes erros de configuração esclarecem a maioria dos problemas NAT encontrados por administradores ASA:

- As regras da configuração de NAT são foras de serviço. Por exemplo, uma regra manual NAT é colocada na parte superior da tabela NAT, que causa umas regras mais específicas colocou uma pena mais distante a tabela NAT a ser batida nunca.
- Os objetos de rede usados na configuração de NAT são estas regras NAT, e que falta NAT regras mais específicas da demasiado largas, que faz com o tráfego combine inadvertidamente.

A utilidade do **projétil luminoso do pacote** pode ser usada para diagnosticar a maioria de edições NAT-relacionadas no ASA. Veja a próxima seção para obter mais informações sobre de como a configuração de NAT é usada para construir a tabela da política de NAT, e de como pesquisar defeitos e resolver problemas NAT específicos.

Adicionalmente, o **comando detail nat da mostra** pode ser usado a fim compreender que regras NAT são batidas por novas conexões.

Como a configuração ASA é usada para construir a tabela da política de NAT

Todos os pacotes processados pelo ASA são avaliados contra a tabela NAT. Esta avaliação começa na parte superior (seção 1) e em trabalhos para baixo até que uma regra NAT esteja combinada. Uma vez que uma regra NAT é combinada, essa regra NAT está aplicada à conexão e não mais política de NAT é verificada contra o pacote.

A política de NAT no ASA é construída da configuração de NAT.

As três seções da tabela ASA NAT são:

Seção 1	**Políticas de NAT manuais** Estes são processados na ordem em que aparecem na configuração.
Seção 2	**Auto políticas de NAT** Estes são processados basearam no tipo NAT (estático ou dinâmico) e no comprimento do prefix (máscara de sub-rede) no objeto.
Seção 3	**Após-auto políticas de NAT manuais** Estes são processados na ordem em que aparecem na configuração.

Este diagrama mostra as seções diferentes NAT e como são pedidas:

Este exemplo mostra como a configuração de NAT do ASA com duas regras (uma declaração NAT manual e uma auto configuração de NAT) é representada na tabela NAT:

Como pesquisar defeitos problemas NAT

Use a utilidade do projétil luminoso do pacote

A fim pesquisar defeitos problemas com configurações de NAT, use a utilidade do **projétil luminoso do pacote** a fim verificar que um pacote bate a política de NAT. O projétil luminoso do pacote permite que você especifique um pacote da amostra que incorpore o ASA, e o ASA indica

o que a configuração se aplica ao pacote e se é permitida ou não.

No exemplo abaixo, um pacote de TCP da amostra que incorpore a interface interna e seja destinado a um host no Internet é dado. A utilidade do projétil luminoso do pacote mostra que o pacote combina uma regra dinâmica NAT e está traduzido ao endereço IP externo de **172.16.123.4**:

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 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 o **rastreamento de pacotes** a fim ativar o projétil luminoso do pacote do Cisco Adaptive Security Device Manager (ASDM). Isto usa os endereços IP de Um ou Mais Servidores Cisco ICM NT especificados na regra NAT como as entradas para a ferramenta do projétil luminoso do pacote:

Veja a saída do comando show nat

A saída do **comando detail nat da mostra** pode ser usada a fim ver a tabela da política de NAT. Especificamente, os **translate_hits** e os contadores dos **untranslate_hits** podem ser usados a fim determinar que entradas NAT são usadas no ASA. Se você vê que sua regra nova NAT não tem nenhum **translate_hits** ou **untranslate_hits**, esse significa que ou o tráfego não chega no ASA, ou talvez uma regra diferente que tenha uma prioridade mais alta na tabela NAT combina o tráfego.

Estão aqui a configuração de NAT e a tabela da política de NAT de uma configuração diferente ASA:

No exemplo anterior, há seis regras NAT configuradas neste ASA. A saída **nat da mostra** mostra como estas regras são usadas para construir a tabela da política de NAT, assim como o número de **translate_hits** e de **untranslate_hits** para cada regra. Estes contadores de acertos incrementam somente uma vez pela conexão. Depois que a conexão é construída com o ASA, os pacotes subsequente que combinam essa conexão atual não incrementam as linhas NAT (bem como as contagens da batida da lista de acesso da maneira trabalhe no ASA).

Translate_hits: O número de novas conexões que combinam a regra NAT no sentido dianteiro.

"O sentido dianteiro" significa que a conexão esteve construída com o ASA na direção das relações especificadas na regra NAT. Se uma regra NAT especificou que o server interno está traduzido à interface externa, a ordem das relações na regra NAT é "nat (para dentro, fora)…"; se esse server inicia uma nova conexão a um host na parte externa, o contador do **translate_hit** incrementa.

Untranslate_hits: O número de novas conexões que combinam a regra NAT no sentido reverso.

Se uma regra NAT especifica que o server interno está traduzido à interface externa, a ordem das relações na regra NAT é "nat (para dentro, fora)…"; se um cliente na parte externa do ASA inicia uma nova conexão ao server no interior, o contador do **untranslate_hit** incrementa.

Além disso, se você vê que sua regra nova NAT não tem nenhum **translate_hits** ou **untranslate_hits**, esse significa que ou o tráfego não chega no ASA, ou talvez uma regra diferente que tenha uma prioridade mais alta na tabela NAT combina o tráfego.

Metodologia de Troubleshooting do problema NAT

Use o projétil luminoso do pacote a fim confirmar que um pacote da amostra combina a regra apropriada da configuração de NAT no ASA. Use o **comando detail nat da mostra** a fim compreender que regras da política de NAT são batidas. Se uma conexão combina uma configuração de NAT diferente do que esperada, pesquise defeitos com estas perguntas:

- Há uma regra diferente NAT que tome a precedência sobre a regra que NAT você pretendeu o tráfego bater?
- Há uma regra diferente NAT com definições de objeto que são demasiado largas (a máscara de sub-rede é demasiado curto, como 255.0.0.0) que faz com que este tráfego combine a regra errada?
- São as políticas de NAT manuais foras de serviço, que causas o pacote para combinar a regra errada?
- Ésua regra NAT configurada incorretamente, que causas a regra para não combinar seu tráfego?

Veja a próxima seção para exemplos de problema e soluções.

Problemas comuns com configurações de NAT

Estão aqui alguns problemas comuns experimentados quando você configura o NAT no ASA.

Problema: O tráfego falha devido ao erro da falha do caminho reverso NAT (RPF): Regras assimétricas NAT combinadas para dianteiro e fluxos reversos

A verificação RPF NAT assegura-se de que uma conexão que seja traduzida pelo ASA no sentido dianteiro, tal como o sincronizar TCP (SYN), esteja traduzida pela mesma regra NAT no sentido reverso, tal como o TCP SYN/acknowledge (ACK).

O mais geralmente, este problema é causado pelas conexões de entrada destinadas ao endereço (untranslated) local em uma declaração NAT. A nível básico, o NAT RPF verifica que a conexão reversa do server ao cliente combina a mesma regra NAT; se não faz, a verificação RPF NAT falha.

Exemplo:

Quando o host exterior em 209.165.200.225 envia um pacote destinado diretamente ao endereço IP de Um ou Mais Servidores Cisco ICM NT (untranslated) local de 10.2.3.2, o ASA deixa cair o pacote e registra este Syslog:

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 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#
```

Solução:

Primeiramente, assegure-se de que o host envie dados ao endereço global correto NAT. Se o host envia os pacotes destinados ao endereço correto, verifique as regras NAT que são batidas pela conexão. Verifique que as regras NAT estão definidas corretamente, e que os objetos providos nas regras NAT estão corretos. Igualmente verifique que a ordem das regras NAT é apropriada.

Use a utilidade do projétil luminoso do pacote a fim especificar os detalhes do pacote negado. O projétil luminoso do pacote deve mostrar o pacote descartado devido à falha da verificação RPF. Em seguida, o olhar na saída do projétil luminoso do pacote a fim considerar que NAT ordena é batido na fase NAT e na fase NAT-RPF.

Se um pacote combina uma regra NAT na fase da verificação RPF NAT, que indica que o fluxo reverso bateria uma tradução NAT, mas não combina uma regra na fase NAT, que indica que o fluxo dianteiro não bateria uma regra NAT, o pacote é deixado cair.

Esta saída combina a encenação mostrada no diagrama precedente, onde o host exterior envia incorretamente o tráfego ao endereço IP local do server e não do endereço IP de Um ou Mais

Servidores Cisco ICM NT (traduzido) global:

```
ASA# packet-tracer input outside tcp 209.165.200.225 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 de Um ou Mais Servidores Cisco ICM NT traçado correto de 172.18.22.1, o pacote combina a regra correta NAT na fase UN-NAT no sentido dianteiro, e a mesma regra na fase da verificação RPF NAT:

```
ASA(config)# packet-tracer input outside tcp 209.165.200.225 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 manuais NAT são foras de serviço, que causa fósforos do pacote incorreto

As regras manuais NAT são processadas basearam em sua aparência na configuração. Se uma regra muito larga NAT é alistada primeiramente na configuração, pôde cancelar outra, uma regra mais específica mais distante para baixo na tabela NAT. Use o projétil luminoso do pacote a fim verificar que regra NAT seu tráfego bate; pôde ser necessário rearranjar as entradas NAT manuais a uma ordem diferente.

Solução:

Requisite novamente regras NAT com ASDM.

Solução:

As regras NAT podem ser requisitadas novamente com o CLI se você remove a regra e a reintroduz em um número de linha específico. A fim introduzir uma regra nova em uma linha específica, entre no número de linha imediatamente depois que as relações são especificadas.

Exemplo:

```
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 demasiado larga e combina algum tráfego inadvertidamente

As regras NAT são criadas às vezes que usam os objetos que são demasiado largos. Se estas regras estão colocadas perto da parte superior da tabela NAT (na parte superior da seção 1, por exemplo), puderam combinar mais tráfego do que pretendido e fazer com que as regras NAT mais distante abaixo da tabela estejam batidas nunca.

Solução:

Use o projétil luminoso do pacote a fim determinar se seu tráfego combina uma regra com as definições de objeto que são demasiado largas. Se este é o caso, você deve reduzir o espaço daqueles objetos, ou mova as regras mais distante abaixo da tabela NAT, ou à após-auto seção (seção 3) da tabela NAT.

Problema: Uma regra NAT desvia o tráfego a uma interface incorreta

As regras NAT podem tomar a precedência sobre a tabela de roteamento quando determinam que relação um pacote saída o ASA. Se um pacote de entrada combina um endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido em uma declaração NAT, a regra NAT está usada a fim determinar a interface de saída.

O NAT desvia verificações da verificação (que é o que pode cancelar a tabela de roteamento) para ver se há qualquer regra NAT que especificar a tradução de endereço de destino para um pacote de entrada que chegue em uma relação. Se há nenhuma regra que especifica explicitamente como traduzir o endereço IP de destino, a seguir a tabela de roteamento global desse pacote está consultada para determinar a interface de saída. Se há uma regra que especifique explicitamente como traduzir o endereço IP de destino dos pacotes, a seguir a regra NAT “puxa” o pacote para a outra relação na tradução e na tabela de roteamento global está contorneada eficazmente.

Este problema é considerado o mais frequentemente para o tráfego de entrada, que chega na interface externa, e é geralmente devido às regras foras de serviço NAT que desviam o tráfego às relações sem intenção.

Exemplo:

Soluções:

Este problema pode ser resolvido com a qualquer uma destas ações:

- Requisite novamente a tabela NAT de modo que mais a entrada específica é alistado primeiramente.
- Use escalas de endereço IP global desobreposição para as declarações NAT.

Note que se a regra NAT é uma regra da identidade, (que significa que os endereços IP de Um ou Mais Servidores Cisco ICM NT não estão mudados pela regra) então a palavra-chave da rota-**consulta** pode ser usada (esta palavra-chave não é aplicável ao exemplo acima desde que a regra NAT não é uma regra da identidade). A palavra-chave da rota-**consulta** faz com que o ASA execute uma verificação extra quando combina uma regra NAT. Certifica-se da tabela de roteamento do ASA para a frente o pacote à mesma interface de saída a que esta configuração de NAT desvia o pacote. Se a interface de saída da tabela de roteamento não combina o NAT desvia a relação, a regra NAT não está combinada (a regra está saltada) e o pacote continua abaixo da tabela NAT a ser processada por uma regra mais atrasada NAT.

A opção da rota-consulta está somente disponível se a regra NAT é uma regra NAT da "identidade", assim que significa que os endereços IP de Um ou Mais Servidores Cisco ICM NT não estão mudados pela regra. A opção da rota-**consulta** pode ser permitida pela regra NAT se você adiciona a rota-**consulta à** extremidade da linha NAT, ou se você verifica a **tabela de rota da consulta para encontrar a** caixa de verificação da **interface de saída na** configuração da regra NAT no ASDM:

Problema: Uma regra NAT causa o ASA ao protocolo proxy address resolution (ARP) para o tráfego na relação traçada

Os proxys ARP ASA para a escala de endereço IP global em uma declaração NAT na relação global. Esta funcionalidade do proxy ARP pode ser desabilitada em uma base da regra por-NAT se você adiciona a palavra-chave nenhum-proxy-**ARP à** declaração NAT.

Este problema é considerado igualmente quando a sub-rede do endereço global é criada inadvertidamente para ser muito maior do que ele foi pretendido ser.

Solução:

Adicionar a palavra-chave nenhum-proxy-**ARP à** linha NAT se possível.

Exemplo:

```
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#
```

Isto pode igualmente ser realizado com ASDM. Dentro da regra NAT, verifique o **proxy ARP do desabilitação na** caixa de verificação da **interface de saída**.

Informações Relacionadas

- VÍDEO: Transmissão da porta ASA para o acesso do servidor DMZ (versões 8.3 e 8.4)
- Configuração de NAT básica ASA: Web server no DMZ na versão ASA 8.3 e mais atrasado
- Livro 2: Guia de configuração de CLI do Series Firewall de Cisco ASA, 9.1
- Suporte Técnico e Documentação - Cisco Systems