Perguntas frequentes da Tradução de Endereço de Rede (NAT)

Contents

Introduction

Este documento tem respostas para perguntas frequentes sobre a Conversão de Endereço de Rede (NAT, Network Address Translation).

NAT genérico

P. O que é NAT?

R. A Network Address Translation (NAT) foi projetada para a conservação de endereços IP. Ela permite que as redes IP privadas que usam endereços IP não registrados se conectem à Internet. A NAT opera em um roteador, que geralmente conecta duas redes entre si e converte os endereços privados (não exclusivos globalmente) na rede interna em endereços legais, antes que os pacotes sejam encaminhados para outra rede.

Outro aspecto desse recurso é que a NAT pode ser configurada para anunciar para o resto do mundo apenas um endereço para toda a rede, proporcionando segurança adicional ao ocultar o fato de que a rede interna está por trás desse endereço. A NAT disponibiliza funções duplas de segurança e conservação de endereço e é implementada em ambientes de acesso remoto.

P. Como o NAT funciona?

R. Basicamente, o NAT permite que um único dispositivo, como um roteador, atue como um agente entre a Internet (ou rede pública) e uma rede local (ou rede privada), o que significa que apenas um único endereço IP exclusivo é necessário para representar um grupo inteiro de computadores para qualquer coisa fora de sua rede.

P. Como configuro o NAT?

R. Para configurar o NAT tradicional, você precisa fazer pelo menos uma interface em um roteador (NAT externo) e outra interface no roteador (NAT interno) e um conjunto de regras para converter os endereços IP nos cabeçalhos dos pacotes (e payloads, se desejado) precisam ser configurados. Para configurar a Nat Virtual Interface (NVI), você precisa de pelo menos uma interface configurada com NAT habilitada junto com o mesmo conjunto de regras, conforme mencionado acima.

Para obter mais informações, consulte Guia de configuração de serviços de endereçamento IP do Cisco IOS ou Como configurar a interface virtual da NAT.

P. Quais são as principais diferenças entre o Cisco IOS® Software e as implementações de NAT do Cisco PIX Security Appliance?

R. O NAT baseado no software Cisco IOS não é fundamentalmente diferente da função NAT no Cisco PIX Security Appliance. As principais diferenças incluem os tipos distintos de tráfego compatíveis com as implementações. Consulte Exemplos de Configuração de NAT para obter mais informações sobre a configuração de NAT em dispositivos Cisco PIX (inclui os tipos de tráfego suportados).

Q. Em que hardware de roteamento da Cisco o Cisco IOS NAT está disponível? Como o hardware pode ser encomendado?

R. A ferramenta Cisco Feature Navigator permite que os clientes identifiquem um recurso (NAT) e descubram em qual versão e versão de hardware esse recurso do Cisco IOS Software está disponível. Consulte o Cisco Feature Navigator para utilizar esta ferramenta.

P. O NAT ocorre antes ou após o roteamento?

R. A ordem em que as transações são processadas usando o NAT é baseada em se um pacote está indo da rede interna para a rede externa ou da rede externa para a rede interna. A conversão de dentro para fora ocorre depois do roteamento, e de fora para dentro; a conversão ocorre antes do roteamento. Consulte Pedido de Operação da NAT para obter mais informações.

P. O NAT pode ser implantado em um ambiente de LAN sem fio público?

R. Sim. A NAT - o recurso de suporte a IP estático oferece apoio aos usuários com endereços IP estáticos, o que permite que os usuários estabeleçam uma sessão IP em um ambiente de LAN sem fio pública.

P. O NAT faz o balanceamento de carga TCP para servidores na rede interna?

R. Sim. Usando a NAT, você pode estabelecer um host virtual no interior da rede que coordena o compartilhamento de carga entre os hosts reais.

P. Posso limitar a taxa do número de conversões NAT?

R. Sim. O recurso de Conversão de NAT com limite de taxa oferece a capacidade de limitar o

número máximo de operações simultâneas de NAT em um roteador. Além de oferecer aos usuários mais controle sobre como os endereços de NAT são usados, o recurso de Conversão de NAT limitado por taxa pode ser usado para limitar os efeitos do vírus, worms e ataques de negação de serviço.

P. Como o roteamento é aprendido ou propagado para sub-redes IP ou endereços que são usados pelo NAT?

R. O roteamento de IP Addresses criados pelo NAT serão reconhecidos se:

- O pool de endereços global interno for derivado da sub-rede de um roteador de próximo salto.
- A entrada de rota estática for configurada no roteador de próximo salto e redistribuída dentro da rede do roteamento.

Quando o endereço global interno corresponde à interface local, a NAT instala um alias de IP e uma entrada ARP, o que significa que o roteador vai usar **proxy-arp para esses endereços.** Caso esse comportamento não seja desejado, use a palavra-chave *no-alias* .

Quando um pool de NAT está configurado, a opção *add-route* pode ser usada para a injeção de rota automática.

P. Quantas sessões de NAT simultâneas têm suporte no Cisco IOS NAT?

R. O limite da sessão de NAT é limitado pela quantidade de DRAM disponível no roteador. Cada conversão NAT consome cerca de 312 bytes da DRAM. Como resultado, 10.000 conversões (mais do que seria geralmente feito em um único roteador) consomem cerca de 3 MB. Sendo assim, o hardware de roteamento típico tem mais memória do que o suficiente para comportar milhares de conversões NAT.

P. Que tipo de desempenho de roteamento pode ser esperado ao usar o NAT do Cisco IOS?

R. O NAT do Cisco IOS suporta switching Cisco Express Forwarding, switching rápida e switching de processo. O caminho de switching rápido não é mais compatível com versões 12.4T e superior. Para a plataforma Cat6k, a ordem de switching é Netflow (caminho de switching de HW), CEF e caminho do processo.

O desempenho depende de vários fatores:

- O tipo de aplicação e o tipo de tráfego
- Se os endereços IP estão incorporados
- Troca e inspeção de várias mensagens
- Porta de origem obrigatória
- O número de conversões
- Outras aplicações em execução no momento
- O tipo de hardware e processador

P. O NAT do Cisco IOS pode ser aplicado a subinterfaces?

R. Sim. Conversões NAT de origem e/ou destino podem ser aplicadas a qualquer interface ou

subinterface que tiver um endereço IP (inclusive interfaces do discador). A NAT não pode ser configurada usando a Interface virtual sem fio. A Interface virtual sem fio não existe no momento da gravação na NVRAM. Assim, após a reinicialização, o roteador perde a configuração da NAT na Interface virtual sem fio.

P. O NAT do Cisco IOS pode ser usado com o Hot Standby Router Protocol (HSRP) para fornecer links redundantes para um ISP?

R. Sim. A NAT oferece HSRP redundante. Entretanto, é diferente da SNAT (Stateful NAT). A NAT com HSRP é um sistema stateless. A sessão atual não é mantida quando ocorre uma falha. Durante a configuração de NAT estática (quando um pacote não coincide com nenhuma configuração de regra ESTÁTICA), o pacote é enviado sem nenhuma conversão.

P. O NAT do Cisco IOS suporta conversões de entrada em uma interface Frame Relay? Ele suporta traduções externas no lado da Ethernet?

R. Sim. O encapsulamento não importa para a NAT. A NAT pode ser feita onde houver um endereço IP em uma interface, e a interface é NAT de dentro ou NAT de fora. Deve haver um interior e um exterior para a NAT funcionar. Se você usar o NVI, deve haver pelo menos uma interface NAT habilitada. Veja Como configurar a NAT? para obter mais detalhes.

P. Um único roteador habilitado para NAT permite que alguns usuários usem NAT e outros usuários na mesma interface Ethernet para continuar a usar seus próprios endereços IP?

R. Sim. Isso pode ser feito através da utilização de uma lista de acesso, descrevendo o conjunto de hosts ou redes que exigem a NAT. Todas as sessões no mesmo host serão convertidas ou passarão através do roteador e não serão convertidas.

Listas de acesso, listas de acesso estendido e mapas de rota podem ser usados para definir *regras pelas quais os dispositivos de IP são convertidos.* O endereço de rede e a máscara de sub-rede adequados sempre devem ser especificados. A palavra-chave *any* não deve ser usada no lugar do endereço de rede ou da máscara de sub-rede. Com a configuração da NAT estática, quando o pacote não corresponde a qualquer configuração de regra ESTÁTICA, o pacote é enviado sem nenhuma conversão.

P. Ao configurar para PAT (sobrecarga), qual é o número máximo de conversões que podem ser criadas por endereço IP global interno?

R. O PAT (sobrecarga) divide as portas disponíveis por endereço IP global em três intervalos: 0-511, 512-1023 e 1024-65535. O PAT atribui uma porta de origem exclusiva para cada sessão UDP ou TCP. Ela tenta atribuir o mesmo valor de porta da solicitação original, mas se a porta de origem já tiver sido usada, ela inicia a verificação no início da faixa determinada da porta até encontrar a primeira porta disponível e atribuí-la para a conversa. Há uma exceção para a base do código 12.2S. A base do código 12.2s usa uma lógica de porta diferente, e não há nenhuma reserva de porta.

P. Como funciona o PAT?

R. O PAT funciona com um endereço IP global ou vários endereços.

PAT com um endereço IP

Condição	Descrição
1	A NAT/PAT inspeciona o tráfego e o correlaciona a uma regra de conversão.
2	A regra corresponde a uma configuração da PAT.
3	Se a PAT conhecer o tipo de tráfego e se esse tipo de tráfego tiver "um conjunto de portas específicas ou portas que negocia" que ela usará, a PAT as separa e não as aloca como identificadores únicos.
4	Se uma sessão sem requisitos especiais de porta tenta conectar-se para fora, a PAT converte o endereço IP de origem e verifica a disponibilidade da porta de origem (433, por exemplo). **Observação:** para o Transmission Control Protocol (TCP) e o User Datagram Protocol (UDP), os intervalos são: 1-511, 512-1023, 1024-65535. Para o Internet Control Message Protocol (ICMP), o primeiro grupo inicia em 0.
5	Se a porta de origem solicitada estiver disponível, a PAT atribui a porta de origem e a sessão continua.
6	Se a porta de origem solicitada não estiver disponível, a PAT começa pesquisando desde o início do grupo relevante (começando em 1 para aplicações de TCP ou UDP e em 0 para ICMP).
7	Se uma porta estiver disponível, ela é atribuída, e a sessão continua.
8	Se nenhuma porta estiver disponível, o pacote será derrubado.

PAT com vários endereços IP

Condição	Descrição
1-7	Para as sete primeiras condições, ocorre o mesmo que com um único endereço IP.
8	Se não houver portas disponíveis no grupo relevante no primeiro endereço IP, a NAT passa para o próximo endereço IP no pool e tenta alocar a porta de origem solicitada.
9	Se a porta de origem solicitada está disponível, a NAT atribui a porta de origem e a sessão continua.
10	Se a porta de origem solicitada não estiver disponível, a NAT começa procurando desde o início do grupo relevante (começando em 1 para aplicações de TCP ou UDP e em 0 para ICMP).

11	Se uma porta estiver disponível, ela será atribuída e a sessão continuará.
12	Se não houver portas disponíveis, o pacote é descartado, a menos que outro endereço IP esteja disponível no pool.

P. O que são pools IP de NAT?

R. Os pools de IP de NAT são um intervalo de endereços IP alocados para conversão de NAT conforme necessário. Para definir um pool, é usado o comando de configuração:

ip nat pool <*name*> <*start-ip*> <*end-ip*> **{netmask** <*netmask*> | **prefix-length** <*prefix-length*>**} [type {rotary}]**

Exemplo 1

O exemplo a seguir converte entre hosts internos direcionados à rede 192.168.1.0 ou à rede 192.168.2.0 para a rede exclusiva globalmente 10.69.233.208/28:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Exemplo 2

No exemplo a seguir, o objetivo é definir um endereço virtual, conexões às quais estão distribuídas entre um conjunto de hosts reais. O pool define os endereços dos hosts reais. A lista de acesso define o endereço virtual. Se uma conversão já não existir, pacotes TCP de interface serial 0 (a interface externa) cujo destino corresponde à lista de acesso são convertidos para um endereço do pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
```

P. Qual é o número máximo de pools IP de NAT configuráveis (ip nat pool "name")?

R. Na prática, o número máximo de pools IP configuráveis é limitado pela quantidade de DRAM disponível no roteador específico. (A Cisco recomenda que você configure um tamanho de pool de 255). Cada pool não deve ter mais de 16 bits. Na versão 12.4(11)T e superior, o IOS apresenta o CCE (Common Classification Engine). Com isso, a NAT foi limitada para ter somente um máximo de 255 pools. Na base de código 12.2S, não há nenhuma restrição máxima de pools.

P. Qual é a vantagem de usar o mapa de rota vs ACL em um pool NAT?

R. Um mapa de rotas está protegendo usuários externos indesejados para acessar os usuários/servidores internos. Ele também tem a capacidade de mapear um único endereço IP interno para diferentes endereços globais internos segundo a regra. Consulte Suporte à NAT para vários pools usando mapas de rotas para obter mais informações.

P. O que é "sobreposição" de endereço IP no contexto do NAT?

R. A sobreposição de endereços IP se refere a uma situação em que dois locais que desejam se interconectar estão usando o mesmo esquema de endereços IP. Essa não é uma situação incomum; costuma acontecer quando empresas se fundem ou são adquiridas. Sem um suporte especial, os dois locais não poderão se conectar e estabelecer sessões. O endereço IP sobreposto pode ser um endereço público atribuído a outra empresa, um endereço privado atribuído a outra empresa ou pode vir do intervalo de endereços privados conforme definido no RFC 1918 .

Endereços IP privados não podem ser roteados e exigem conversões NAT para permitir conexões com o mundo exterior. A solução envolve interceptar respostas de consulta de nome do Domain Name System (DNS) de fora para dentro, configurando uma conversão para o endereço externo e arrumando a resposta DNS antes de encaminhá-lo ao host interno. É necessário que haja envolvimento de um servidor DNS em ambos os lados do dispositivo NAT para atender a usuários que desejam ter conexão entre ambas as redes.

A NAT é capaz de inspecionar e realizar a conversão de endereço sobre o conteúdo do DNS *A e registros do* PTR, conforme mostrado em Como usar a NAT em redes sobrepostas.

P. O que são conversões NAT estáticas?

R. As conversões NAT estáticas têm mapeamento um para um entre endereços locais e globais. Os usuários podem também configurar conversões de endereço estático para o nível da porta e usar o restante do endereço IP para outras conversões. Isso normalmente ocorre onde você está fazendo a Conversão de endereço de porta (PAT, Port Address Translation).

O exemplo a seguir mostra como configurar um mapa de rota para permitir a conversão de fora para dentro para NAT estática:

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10
match ip address ACL-A
```

P. O que significa o termo *sobrecarga* de NAT; é a PAT?

R. Sim. A sobrecarga de NAT é PAT, o que envolve usar um pool com um intervalo com um ou mais endereços ou usar um endereço IP de interface em combinação com a porta. Quando sobrecarregar, você cria uma conversão totalmente estendida. Essa é uma entrada de tabela de conversão que contém o endereço IP e a informação de porta de origem/destino, que geralmente é chamada de PAT ou sobrecarga.

PAT (ou sobrecarga) é uma característica da NAT do Cisco IOS que é usada para converter endereços privados *internos (local interior) para um ou mais endereços IP externos (global interno, geralmente registrado).* Os números exclusivos de porta de origem em cada tradução são usados para diferenciar entre as conversações.

P. O que são conversões NAT dinâmicas?

R. Em conversões NAT dinâmicas, os usuários podem estabelecer mapeamento dinâmico entre endereços locais e globais. O mapeamento dinâmico é realizado definindo os endereços locais que serão convertidos e o pool de endereços, ou o endereço IP de interface do qual deseja alocar endereços globais e associar os dois.

P. O que é ALG?

R. O ALG é um Application Layer Gateway (ALG). A NAT faz serviços de conversão em qualquer tráfego de Transmission Control Protocol/User Datagram Protocol (TCP/UDP) que não tenha endereços IP de origem e/ou destino no fluxo de dados de aplicação.

Esses protocolos incluem FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh, rcp. Protocolos específicos que incorporam informações de endereço IP à carga exigem a ajuda de um ALG.

Consulte Como usar gateways de camada de aplicação com NAT para obter mais informações.

P. É possível criar uma configuração com conversões NAT estáticas e dinâmicas?

R. Sim. No entanto, o mesmo endereço IP não pode ser usado para a configuração estática da NAT ou no pool para configuração dinâmica da NAT. Todos os endereços IP públicos precisam ser exclusivos. Observe que os endereços globais usados em conversões estáticas não são excluídos automaticamente com pools dinâmicos que têm os mesmos endereços globais. Pools dinâmicos devem ser criados para excluir endereços atribuídos por entradas estáticas. Para obter mais informações, consulte Como configurar NATs estática e dinâmica simultaneamente.

P. Quando um traceroute é feito através de um roteador NAT, o traceroute deve mostrar o endereço NAT-Global ou deve vazar o endereço NAT-Local?

R. Traceroute de fora deve sempre retornar o endereço global.

P. Como o PAT aloca a porta?

R. O NAT introduz recursos de porta adicionais: faixa completa e mapa de portas.

- A faixa completa permite que a NAT use todas as portas, independentemente da faixa de portas padrão.
- O mapa de portas permite que a NAT reserve uma faixa de portas definida pelo usuário para aplicações específicas.

Consulte Faixas de portas de origem definidas pelo usuário para PAT para obter mais informações.

Da versão 12.4(20)T2 em diante, a NAT apresenta a randomização de porta para L3/L4 e porta simétrica.

- A randomização de porta permite que a NAT selecione aleatoriamente qualquer porta global para a solicitação de porta de origem.
- A porta simétrica permite que a NAT seja compatível com *endpoint independent*.

P. Qual é a diferença entre a fragmentação IP e a segmentação TCP?

R. A fragmentação de IP ocorre na Camada 3 (IP); A segmentação do TCP ocorre na Camada 4 (TCP). A fragmentação de IP ocorre quando os pacotes que são maiores do que a Unidade máxima de transmissão (MTU, Maximum Transmission Unit) de uma interface são enviados para fora desta interface. Esses pacotes precisarão ser fragmentados ou descartados quando forem enviados para fora da interface. Se o bit Não fragmentar (DF, Don't Fragment) não estiver definido no cabeçalho IP do pacote, o pacote será fragmentado. Se o bit DF estiver definido no cabeçalho IP do pacote, o pacote será descartado e uma mensagem de erro ICMP indicando o valor MTU do próximo salto será retornada para o remetente. Todos os fragmentos de um pacote IP carregam a mesma Ident no cabeçalho IP, o que permite que o receptor final remonte os fragmentos no pacote IP original. Consulte Solucionar problemas de fragmentação de IP, MTU, MSS e PMTUD usando GRE e IPsec para obter mais informações.

A segmentação do TCP ocorre quando uma aplicação em uma estação final está enviando dados. Os dados da aplicação são divididos no que o TCP considera os pedaços de melhor tamanho para enviar. Essa unidade de dados passada de TCP para IP é chamada de um segmento. Segmentos TCP são enviados em datagramas de IP. Esses datagramas de IP podem se tornar fragmentos de IP à medida que passam através da rede e encontram links de MTU menores do que podem fazer caber.

Primeiro, o TCP vai segmentar esses dados em segmentos TCP (com base no valor de TCP MSS), adicionar o cabeçalho TCP e passar este segmento TCP para o IP. Então o IP vai adicionar um cabeçalho IP para enviar o pacote para o host remoto final. Se o pacote IP com o segmento TCP for maior do que o IP MTU em uma interface de saída no caminho entre os hosts TCP, o IP vai fragmentar o pacote TCP/IP. Esses fragmentos de pacote IP serão reagrupados no host remoto por camada IP, e o segmento TCP completo (que foi originalmente enviado) será entregue à camada de TCP. A camada TCP não tem ideia de que o IP tinha fragmentado o pacote durante o trânsito.

A NAT é compatível com fragmentos IP, mas não com segmentos TCP.

P. O NAT oferece suporte fora de serviço para fragmentação de IP e segmentação de TCP?

R. O NAT suporta apenas fragmentos IP fora de ordem devido à **remontagem virtual de IP**.

P. Como depurar a fragmentação IP e a segmentação TCP?

R. O NAT usa a mesma CLI de depuração para a fragmentação de IP e a segmentação de TCP: **debug ip nat frag**.

P. Há um MIB NAT compatível?

R. Não. Não há MIB NAT suportado, incluindo CISCO-IETF-NAT-MIB.

P. O que é o *timeout de TCP* e como ele se relaciona com o temporizador de NAT TCP?

R. Se o handshake triplo não for concluído e o NAT vir um pacote TCP, o NAT iniciará um temporizador de 60 segundos. Quando o handshake de três vias estiver concluído, a NAT usa um temporizador de 24 horas para uma entrada à NAT por padrão. Se um host final enviar um RESET, a NAT muda o temporizador padrão de 24 horas para 60 segundos. No caso de FIN, a NAT muda o temporizador padrão de 24 horas para 60 segundos quando ele recebe FIN e FIN-ACK.

P. Posso alterar a quantidade de tempo que leva para uma conversão NAT expirar da tabela de conversão NAT?

R. Sim. Você pode alterar os valores de tempo limite da NAT para todas as entradas ou para diferentes tipos de conversões NAT (como udp-timeout, dns-timeout, tcp-timeout, finrst-timeout, icmp-timeout, pptp-timeout, syn-timeout, port-timeout e arp-ping-timeout).

P. Como faço para impedir que o Lightweight Diretory Access Protocol (LDAP) anexe bytes extras a cada pacote de resposta LDAP?

R. As configurações LDAP adicionam os bytes extras (resultados de pesquisa LDAP) ao processar mensagens do tipo Search-Res-Entry. O LDAP anexa 10 bytes de resultados de pesquisa para cada um dos pacotes de resposta do LDAP. Se esses 10 bytes extras de resultado de dados no pacote excederem a MTU (Unidade máxima de transmissão) em uma rede, o pacote é descartado. Nesse caso, a Cisco recomenda que você desative esse comportamento de LDAP usando o comando CLI **no ip nat service append-ldap-search-res para que os pacotes sejam enviados e recebidos.**

P. Qual é a recomendação de rota para o endereço IP global interno/local externo na caixa NAT?

R. Uma rota deve ser especificada na caixa configurada de NAT para o endereço IP global interno para recursos como NAT-NVI. Da mesma forma, uma rota também deve ser especificada na caixa NAT para o endereço IP local externo. Nesse caso, qualquer pacote que vai de dentro para fora usando a regra estática exterior vai exigir esse tipo de rota. Em tais situações, ao criar a rota para IG/OL, o endereço IP do próximo salto também deverá ser configurado. Se a configuração de próximo salto estiver faltando, é considerado um erro de configuração e resulta em um comportamento indefinido.

O NVI-NAT só está presente no caminho de recurso de saída. Se você tiver conectado a sub-rede

diretamente com NAT-NVI ou a regra de conversão NAT externa configurada na caixa, então, nesses casos, você precisa apresentar um endereço IP de próximo salto fictício e também um ARP associado para o próximo salto. É necessário para a infraestrutura subjacente entregar o pacote à NAT para conversão.

P. O NAT do Cisco IOS suporta ACLs com uma palavra-chave "log"?

R. Quando você configura o NAT do Cisco IOS para conversão de NAT dinâmico, uma ACL é usada para identificar pacotes que podem ser convertidos. A atual arquitetura NAT não é compatível com ACLs usando uma palavra-chave de "log".

NAT por voz

P. O NAT é compatível com o Skinny Client Control Protocol (SCCP) v17 fornecido com o Cisco Unified Communications Manager (CUCM) V7?

R. O CUCM 7 e todas as cargas de telefone padrão para o CUCM 7 suportam SCCPv17. A versão do SCCP usada é determinada pela versão mais alta comum entre o CUCM e o telefone quando o telefone é registrado.

O NAT ainda não suporta o SCCP v17. Até que o suporte NAT para o SCCP v17 seja implementado, o firmware deve ser rebaixado para a versão 8-3-5 ou inferior para que o SCCP v16 seja negociado. O CUCM6 não encontrará o problema de NAT com qualquer carga de telefone, desde que use o SCCP v16. O Cisco IOS atualmente não suporta o SCCP versão 17.

P. Quais versões de carregamento de CUCM /SCCP/firmware são suportadas pelo NAT?

R. O NAT suporta CUCM versão 6.x e versões anteriores. Essas versões do CUCM são lançadas com a carga de firmware de telefone de versão padrão 8.3.x (ou anterior) de firmware do telefone compatível com SCCP v15 (ou anterior).

A NAT não é compatível com CUCM versões 7.x ou posterior. Essas versões do CUCM são lançados com a carga de firmware de telefone 8.4.x padrão que é compatível com o SCCP v17 (ou posterior).

Se o CUCM 7.x ou posterior for usado, uma carga de firmware mais velha deve ser instalada no servidor CUCM TFTP para que os telefones usem uma carga de firmware com o SCCP v15 ou anterior para serem compatíveis com a NAT.

P. O que é o Service Provider PAT Port Allocation Enhancement para RTP e RTCP?

R. O recurso Aprimoramento de Alocação de Porta PAT do Provedor de Serviços para RTP e RTCP garante que para chamadas de voz SIP, H.323 e Skinny. Os números de porta usados para fluxos RTP são números de porta pares, e os fluxos RTCP são o próximo número da porta ímpar subsequente. O número da porta é convertido para um número dentro do intervalo especificado em conformidade com a RFC-1889. Uma chamada com um número de porta no intervalo resultará em uma conversão PAT para outro número de porta dentro desse intervalo. Da mesma forma, uma conversão PAT para um número de porta fora desse intervalo não vai resultar

em uma conversão de um número dentro do intervalo especificado.

P. O que é o SIP (Session Initiation Protocol) e os pacotes SIP podem ser convertidos em NAT?

R. O SIP (Session Initiation Protocol) é um protocolo de controle da camada de aplicação baseado em ASCII que pode ser usado para estabelecer, manter e terminar chamadas entre dois ou mais pontos finais. O SIP é um protocolo alternativo desenvolvido pela Internet Engineering Task Force (IETF) para conferência multimídia sobre IP. A implementação do Cisco SIP permite que plataformas compatíveis com a Cisco sinalizem a instalação de chamadas de voz e multimídia por redes IP.

Os pacotes de SIP podem ser submetidos à NAT.

P. O que é o suporte Hosted NAT Traversal para Session Border Controller (SBC)?

R. O recurso Cisco IOS Hosted NAT Traversal for SBC permite que um roteador Cisco IOS NAT SIP Application-Level Gateway (ALG) atue como um SBC em um Cisco Multiservice IP-to-IP Gateway, o que ajuda a garantir uma entrega sem problemas de serviços de voz sobre IP (VoIP).

Consulte Configuração do Cisco IOS Hosted NAT Traversal para Session Border Controller para obter mais informações.

P. Quantas chamadas SIP, Skinny e H323 a memória e a CPU de um roteador podem lidar com NAT?

R. O número de chamadas tratadas por um roteador NAT depende da quantidade de memória disponível na caixa e da potência de processamento da CPU.

P. Um roteador NAT suporta segmentação TCP de pacotes Skinny e H323?

R. O IOS-NAT suporta segmentação TCP para H323 em 12.4 Mainline e suporte à segmentação TCP para SKINNY a partir de 12.4(6)T.

P. Há alguma advertência a ser observada ao usar uma configuração de sobrecarga de NAT em uma implantação de voz?

R. Sim. Quando você tem configurações de sobrecarga de NAT e uma implantação de voz, você precisa da mensagem de registro para passar pela NAT e criar uma associação para out->in para chegar a este dispositivo interno. O dispositivo interno envia este registro de forma periódica e a NAT atualiza este pin-hole/associação segundo as informações da mensagem de sinalização.

P. Há algum problema conhecido causado pela emissão do comando clear ip nat trans * ou do comando clear ip nat trans forced em uma implantação de voz?

R. Em implantações de voz, quando você emite um comando **clear ip nat trans *** ou um comando **clear ip nat trans forced e tem um NAT dinâmico, você apagará o pin-hole/associação e deve aguardar o próximo ciclo de registro do dispositivo interno para restabelecer isso.** A Cisco recomenda que você não use esses comandos claros em uma implantação de voz.

P. O NAT é compatível com a solução co-localizada de voz?

R. Não. Não há suporte para a solução colocalizada no momento. A implantação a seguir com NAT (na mesma caixa) é considerada uma solução colocalizada: CME/DSP-Farm/SCCP/H323.

P. O NVI é compatível com Skinny ALG, H323 ALG e TCP SIP ALG?

R. Não. Observe que o ALG UDP SIP (usado pela maioria das implantações) não é afetado.

NAT com VRF/MPLS

P. Um roteador NAT suportará a NAT no mesmo espaço de endereço em um VRF que está sendo NAT em um espaço de endereço global? No momento, estou recebendo este aviso: *"% entrada estática semelhante (1.1.1.1 —> 22.2.2.2) já existe"* quando tento configurar o seguinte:

```
72UUT(config)#ip nat inside
 source static 1.1.1.1 22.2.2.2 72UUT(config)#ip nat inside source static
 1.1.1.1 22.2.2.2 vrf RED
```

R. O NAT legado suporta a sobreposição de configuração de endereço sobre VRFs diferentes. Você teria que configurar a sobreposição em regra com a opção *match-in-vrf* e configurar ip nat inside/outside no mesmo VRF para tráfego sobre esse VRF específico. A compatibilidade de sobreposição não inclui a tabela de roteamento global.

Você deve adicionar a palavra-chave *match-in-vrf* para as sobreposições de entradas de NAT estática de VRF para diferentes VRFs. Entretanto, não é possível sobrepor endereços de NAT global e de vrf.

```
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```

P. O NAT legado suporta VRF-Lite (NATting de um VRF para um VRF diferente)?

R. Não. Você deve usar NVI para NATting entre VRFs diferentes. Você pode usar a NAT legada para fazer NAT de VRF para global ou NAT dentro do mesmo VRF.

NAT NVI

P. O que é NAT NVI?

R. NVI significa NAT Virtual Interface. Ele permite que a NAT converta entre dois VRFs diferentes. Essa solução deve ser usada em vez da Network Address Translation on a Stick.

P. O NAT NVI deve ser usado ao realizar o NAT entre uma interface em global e uma interface em um VRF?

R. A Cisco recomenda que você use NAT legado para VRF para NAT global (ip nat inside/out) e

entre interfaces no mesmo VRF. A NVI é usada para NAT entre VRFs diferentes.

P. A segmentação TCP para NAT-NVI é suportada?

R. Não há suporte para segmentação TCP para NAT-NVI.

P. O NVI é compatível com Skinny ALG, H323 ALG e TCP SIP ALG?

R. Não. Observe que o ALG UDP SIP (usado pela maioria das implantações) não é afetado.

P. A segmentação TCP é compatível com SNAT?

R. O SNAT não suporta nenhum ALG TCP (como SIP, SKINNY, H323 ou DNS). Portanto, a segmentação TCP não é compatível. No entanto, o UDP SIP e DNS são compatíveis.

SNAT

P. O que é o NAT stateful (SNAT)?

R. A SNAT permite que dois ou mais tradutores de endereço de rede funcionem como um grupo de conversão. Um membro do grupo de conversão manipula o tráfego que exige a conversão das informações de endereço IP. Além disso, ele informa o conversor de backup sobre os fluxos ativos à medida que eles ocorrem. O conversor de backup pode usar informações do conversor ativo para preparar entradas da tabela de conversão duplicada. Portanto, se o conversor ativo for prejudicado por uma falha crítica, o tráfego pode rapidamente ser alternado para o backup. O fluxo de tráfego continua, uma vez que as mesmas conversões de endereço de rede são utilizadas e o estado dessas conversões foi definido anteriormente.

P. A segmentação TCP é suportada com SNAT?

R. O SNAT não suporta nenhum ALG TCP (como SIP, SKINNY, H323 ou DNS). Portanto, a segmentação TCP não é compatível. No entanto, o UDP SIP e DNS são compatíveis.

P. O SNAT é compatível com roteamento assimétrico?

R. O roteamento assimétrico suporta NAT, ativando como enfileiramento. Por padrão, o enfileiramento como é habilitar. No entanto, do 12.4(24)T em diante, a fila como não é mais compatível. Os clientes devem se certificar de que os pacotes são roteados corretamente, e um atraso apropriado é adicionado para que o roteamento assimétrico funcione corretamente.

NAT-PT (v6 a v4)

P. O que é NAT-PT?

R. NAT-PT é uma conversão de v4 para v6 para NAT. A Conversão de Protocolo (NAT-PT) é um mecanismo de conversão IPv6-IPv4, como definido no RFC 2765 e no RFC 2766 , permitindo que dispositivos somente IPv6 se comuniquem com dispositivos somente IPv4 e vice-versa.

P. O NAT-PT é suportado no caminho do Cisco Express Forwarding (CEF)?

R. Não há suporte para NAT-PT no caminho CEF.

P. Quais ALGs são suportados no NAT-PT?

R. O NAT-PT suporta TFTP/FTP e DNS. Voz e SNAT não são compatíveis na NAT-PT.

P. O ASR 1004 é compatível com NAT-PT?

R. Os Roteadores de Serviços de Agregação (ASR) usam NAT64.

Cisco 7300/7600/6k dependente de plataforma

P. O NAT stateful (SNAT) está disponível no Catalyst 6500 no trem SX?

R. SNAT não está disponível no Catalyst 6500 no trem SX.

P. O NAT com reconhecimento de VRF é compatível com hardware no 6k?

R. O NAT sensível a VRF não é suportado no hardware nesta plataforma.

P. O 7600 e o Cat6000 suportam NAT sensível a VRF?

R. Na plataforma 65xx/76xx, a NAT sensível a VRF não é suportada e as CLIs são bloqueadas.

Observação: você pode implementar um design aproveitando um FWSM executado no modo transparente de contexto virtual.

Cisco 850 dependente da plataforma

P. O Cisco 850 suporta Skinny NAT ALG na versão 12.4T?

R. Não. Não há suporte para Skinny NAT ALG em 12.4T na série 850.

Implantação de NAT

P. Como implemento o NAT?

R. O NAT permite que redes IP privadas que usam endereços IP não registrados se conectem à Internet. A NAT converte o endereço privado (RFC1918) na rede interna em endereços roteáveis legais antes que os pacotes sejam encaminhados para outra rede.

P. Como faço para implementar NAT com voz?

R. O suporte NAT para o recurso de voz permite que as mensagens incorporadas do SIP que

passam por um roteador configurado com Network Address Translation (NAT) sejam convertidas de volta para o pacote. Um gateway de camada de aplicativo (ALG) é usado com NAT para converter os pacotes de voz.

P. Como posso integrar o NAT com VPNs MPLS?

R. A integração NAT com o recurso VPNs MPLS permite que várias VPNs MPLS sejam configuradas em um único dispositivo para funcionar em conjunto. A NAT pode se diferenciar da VPN MPLS da qual recebe tráfego IP mesmo se todas as VPNs MPLS usarem o mesmo esquema de endereçamento IP. Esse aprimoramento permite que vários clientes de VPN MPLS compartilhem serviços, além de garantir que cada VPN MPLS fique completamente separada da outra.

P. O mapeamento estático de NAT oferece suporte a HSRP para alta disponibilidade?

R. Quando uma consulta Address Resolution Protocol (ARP) é disparada para um endereço configurado com o mapeamento estático NAT (Network Address Translation) e de propriedade do roteador, o NAT responde com o endereço MAC BIA na interface para a qual o ARP está apontando. Dois roteadores atuam como HSRP ativo e em espera. Suas interfaces com NAT no interior devem ser habilitadas e configuradas para pertencer a um grupo.

P. Como implemento NAT NVI?

R. O recurso NAT virtual interface (NVI) remove o requisito de configurar uma interface como NAT interno ou NAT externo.

P. Como faço para implementar o balanceamento de carga com NAT?

R. Há dois tipos de balanceamento de carga que podem ser feitos com o NAT: Você pode balancear a carga de entrada para um conjunto de servidores para distribuir a carga nos servidores e pode balancear a carga do tráfego de usuários para a Internet por dois ou mais ISPs.

Para obter mais informações sobre balanceamento de carga de saída, consulte Balanceamento de carga de NAT do IOS para duas conexões ISP.

P. Como faço para implementar o NAT em conjunto com o IPSec?

R. Há suporte para o IPSec (IP Security Encapsulating Security Payload) (ESP) por meio de NAT e transparência de NAT de IPSec.

O ESP de IPSec, por meio do recurso de NAT, possibilita a compatibilidade com vários túneis ou conexões de ESP de IPSec concomitantes por meio de um dispositivo de NAT do Cisco IOS configurado em modo de sobrecarga ou Conversão de Endereço de Porta (PAT).

O recurso de transparência de NAT do IPSec apresenta a compatibilidade com o tráfego de IPSec para deslocamento através de pontos de NAT ou PAR na rede ao lidar com várias incompatibilidades conhecidas entre NAT e IPSec.

P. Como faço para implementar o NAT-PT?

R. NAT-PT (Network Address Translation—Protocol Translation) é um mecanismo de conversão IPv6-IPv4, conforme definido na RFC 2765 e na RFC 2766 **, que permite que dispositivos somente IPv6 se comuniquem com dispositivos somente IPv4 e vice-versa.**

P. Como implemento o NAT multicast?

R. É possível fazer NAT do IP de origem para um fluxo multicast. Um mapa de rota não pode ser usado ao submeter o multicast à NAT dinâmica; apenas uma lista de acesso é compatível.

Para obter mais informações, consulte Como a NAT Multicast funciona em roteadores Cisco. O grupo de multicast de destino é submetido à NAT por meio de uma solução de Reflexo de serviço Multicast.

P. Como faço para implementar o NAT stateful (SNAT)?

R. A SNAT permite o serviço contínuo para sessões NAT mapeadas dinamicamente. As sessões definidas estaticamente têm o benefício da redundância sem a necessidade de SNAT. Na ausência de SNAT, as sessões que usam mapeamentos de NAT dinâmico serão interrompidas em caso de falha crítica e precisarão ser restabelecidas. Apenas a configuração mínima da SNAT é compatível. Implantações futuras só deverão ser realizadas depois de você falar com sua equipe de contas da Cisco para validar o projeto em relação a restrições atuais.

A SNAT é recomendada para os seguintes cenários:

- Primário/backup não é um modo recomendado, uma vez que alguns recursos estão faltando em relação ao HSRP.
- Para situações de failover e de configuração do roteador 2. Ou seja, se um roteador falhar, o outro roteador assume sem problemas. (A arquitetura da SNAT não é projetada para lidar com oscilação de interface.)
- O cenário de roteamento não assimétrico é compatível. O roteamento assimétrico pode ser tratado apenas se a latência no pacote de resposta for maior do que entre 2 roteadores SNAT para trocar mensagens de SNAT.

Atualmente a arquitetura SNAT não é projetada para lidar com robustez; Portanto, não se espera que esses testes sejam bem-sucedidos:

- Limpar entradas da NAT enquanto há tráfego.
- Alterar parâmetros de interface (como mudança de endereço IP, fechada/não-fechada etc.) enquanto há tráfego.
- Não se espera que comandos **clear ou show específicos da SNAT sejam executados corretamente, e isso não é recomendado.**Alguns dos comandos **clear e show relacionados à SNAT são o seguinte:**

```
clear ip snat sessions *
clear ip snat sessions
```

```
clear ip snat translation distributed *
clear ip snat translation peer < IP address of SNAT peer>
sh ip snat distributed verbose
```

```
sh ip snat peer < IP address of peer>
```

- Se o usuário desejar limpar entradas, os comandos **clear ip nat trans forced ou clear ip nat trans * podem ser usados.**Se o usuário desejar ver as entradas, os comandos, **show ip nat translation**, **show ip nat translations verbose** e **show ip nat stats podem ser usados.** Se *service internal estiver configurado, ele também mostrará informações específicas da SNAT.*
- Não é recomendável limpar as conversões NAT para o roteador back-up. Sempre limpe as entradas NAT no roteador SNAT principal.
- SNAT não é HA; portanto, as configurações em ambos os roteadores devem ser iguais. Ambos os roteadores devem ter a mesma imagem em execução. Também verifique se a plataforma subjacente usada para ambos os roteadores SNAT é igual.

Melhores práticas de NAT

P. Há alguma prática recomendada de NAT?

R. Sim. Estas são as melhores práticas de NAT:

1. Ao usar uma NAT estática e dinâmica, a ACL que define a regra para NAT dinâmica deve excluir os hosts locais estáticos para que não haja sobreposição.
2. Cuidado com o uso da ACL para NAT com **permit ip any any , pois você pode ter resultados imprevisíveis.** Depois da versão 12.4(20)T, a NAT vai converter pacotes de HSRP e de protocolo de roteamento gerados localmente se eles são forem enviados para a interface externa, bem como pacotes criptografados localmente que correspondem à regra da NAT.
3. Quando você tiver redes sobreposta para a NAT, use a palavra-chave **match-in-vrf.**Você deve adicionar a palavra-chave **match-in-vrf para as entradas de NAT estática de VRF sobrepostas para VRFs diferentes, mas não é possível sobrepor endereços de NAT globais e de vrf.**

   ```
   Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf


   Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
   ```

4. Pools de NAT, com o mesmo intervalo de endereços, não podem ser usados em diferentes VRFs, a menos que a palavra-chave **match-in-vrf seja usada.**Por exemplo:

   ```
   ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24
   ip nat pool poolB 171.1.1.1 171.1.1.10 prefix-length 24
   ip nat inside source list 1 poolA vrf A match-in-vrf
   ip nat inside source list 2 poolB vrf B match-in-vrf
   ```

   Note: Embora a configuração da CLI seja válida, sem a palavra-chave **match-in-vrf**, a configuração não é suportada.
5. Ao implantar o balanceamento de carga de ISPs com sobrecarga de interface de NAT, a melhor prática é usar o mapa de rota com correspondência de interface sobre correspondência de ACL.
6. Ao usar o mapeamento de pool, você não deve usar dois mapeamentos diferentes (ACL ou mapa de rota) para compartilhar o mesmo endereço de pool de NAT.
7. Ao implantar as mesmas regras de NAT em dois roteadores diferentes no cenário de

failover, você deve usar redundância HSRP.

8. Não defina o mesmo endereço global interno em NAT estática e um pool dinâmico. Essa ação gerar resultados indesejáveis.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

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.