Exemplo de configuração de declaração de NAT e PAT no Cisco Secure ASA Firewall

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar - Várias instruções NAT com NAT manual e automático](#)
[Diagrama de Rede](#)
[ASA versão 8.3 e posterior](#)
[Configurar - Vários pools globais](#)
[Diagrama de Rede](#)
[ASA versão 8.3 e posterior](#)
[Configurar - Misturar instruções NAT e PAT](#)
[Diagrama de Rede](#)
[ASA versão 8.3 e posterior](#)
[Configurar - Várias instruções NAT com instruções manuais](#)
[Diagrama de Rede](#)
[ASA versão 8.3 e posterior](#)
[Configurar - Usar NAT de política](#)
[Diagrama de Rede](#)
[ASA versão 8.3 e posterior](#)
[Verificar](#)
[Conexão](#)
[Syslog](#)
[Conversões de NAT (Xlate)](#)
[Troubleshoot](#)

Introduction

Este documento fornece exemplos de configurações básicas de Conversão de Endereço de Rede (NAT - Network Address Translation) e Conversão de Endereço de Porta (PAT - Port Address Translation) no firewall Cisco Secure Adaptive Security Appliance (ASA - Cisco Secure Adaptive Security Appliance). Este documento também fornece diagramas de rede simplificados. Consulte a documentação do ASA para obter informações mais detalhadas sobre a versão do software ASA.

Este documento oferece análise personalizada do seu dispositivo Cisco.

Consulte a configuração de NAT no ASA nos dispositivos de segurança ASA 5500/5500-X Series

para obter mais informações.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do Cisco Secure ASA Firewall.

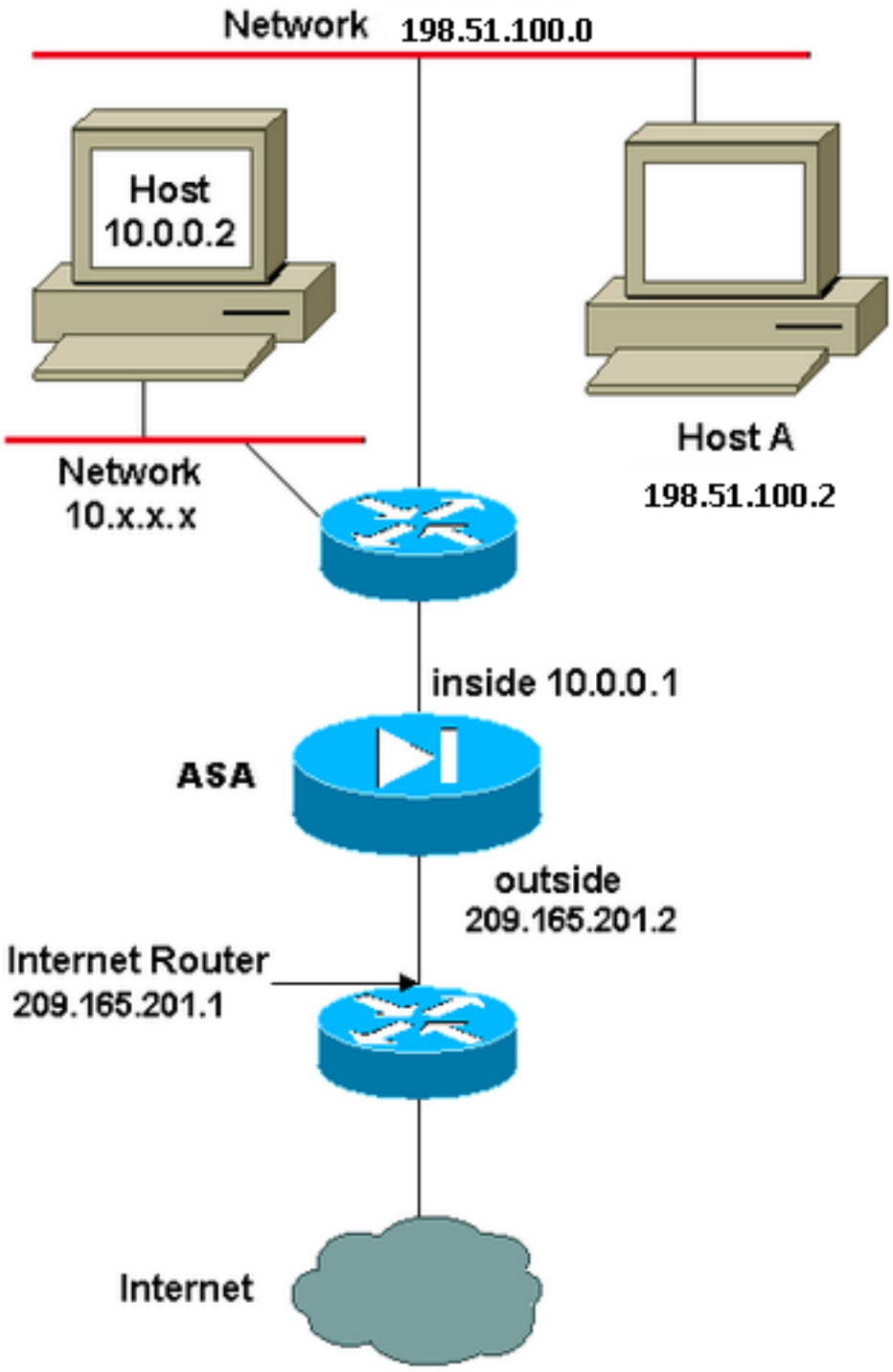
Componentes Utilizados

As informações neste documento são baseadas no software Cisco Secure ASA Firewall versão 8.4.2 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar - Várias instruções NAT com NAT manual e automático

Diagrama de Rede



Neste exemplo, o ISP fornece ao gerente de rede um bloco de endereços IP 209.165.201.0/27 que varia de 209.165.201.1 a 209.165.201.30. O gerente de rede decide atribuir 209.165.201.1 à interface interna no roteador da Internet e 209.165.201.2 à interface externa do ASA.

O administrador de rede já tem um endereço de classe C atribuído à rede, 198.51.100.0/24, e tem algumas estações de trabalho que usam esses endereços para acessar a Internet. Essas estações de trabalho não exigem nenhuma conversão de endereço porque já têm endereços válidos. No entanto, novas estações de trabalho recebem endereços na rede 10.0.0.0/8 e precisam ser convertidas (porque 10.x.x.x é um dos espaços de endereços não roteáveis por RFC 1918.

Para acomodar esse projeto de rede, o administrador de rede deve usar duas instruções NAT e um pool global na configuração do ASA:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

Essa configuração não converte o endereço de origem de nenhum tráfego de saída da rede 198.51.100.0/24. Ele converte um endereço de origem na rede 10.0.0.0/8 em um endereço do intervalo 209.165.201.3 a 209.165.201.30.

> **Note**: Quando você tem uma interface com uma política de NAT e se não há pool global para outra interface, você precisa usar nat 0 para configurar a exceção de NAT.

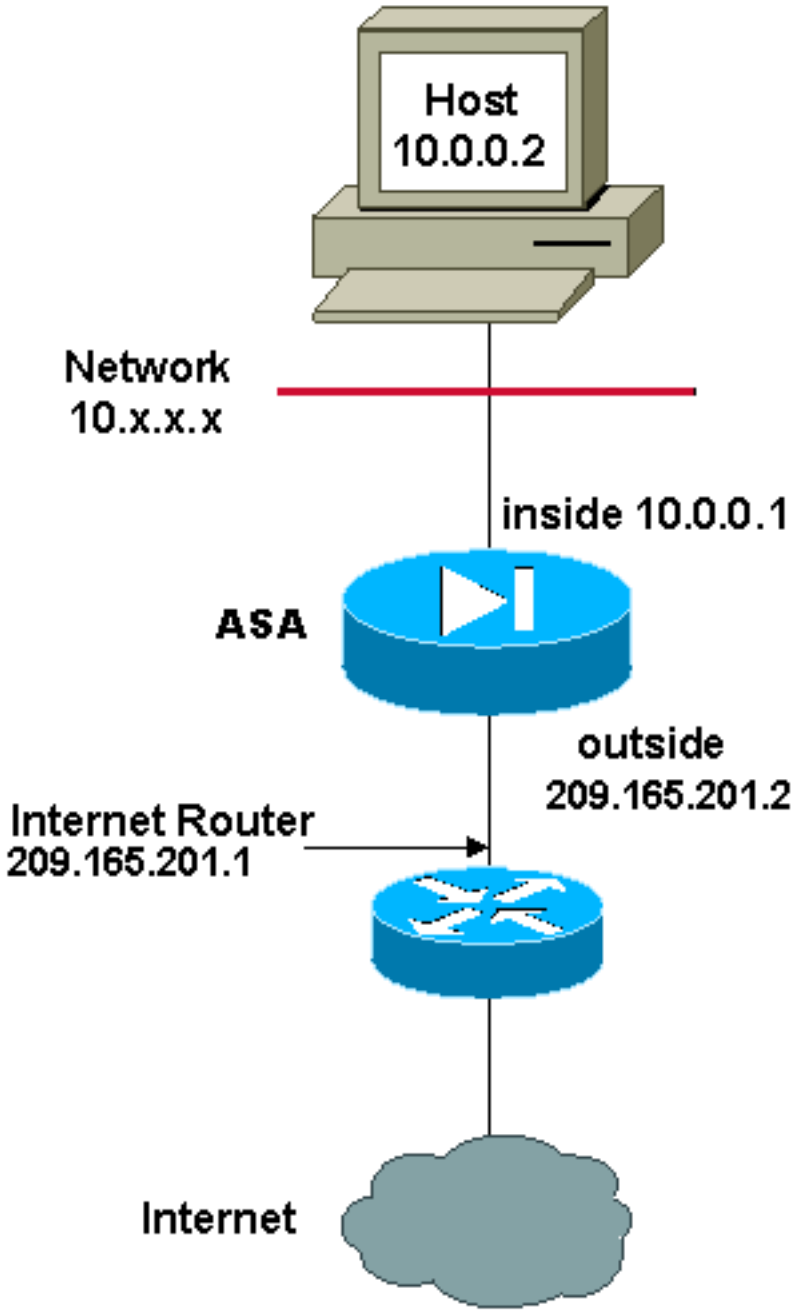
ASA versão 8.3 e posterior

Está aqui a configuração.

```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

Configurar - Vários pools globais

Diagrama de Rede



Neste exemplo, o gerenciador de rede tem dois intervalos de endereços IP registrados na Internet. O gerenciador de rede deve converter todos os endereços internos, que estão no intervalo 10.0.0.0/8, em endereços registrados. Os intervalos de endereços IP que o gerenciador de rede deve usar são 209.165.201.1 a 209.165.201.30 e 209.165.200.225 a 209.165.200.25 4. O gerente de rede pode fazer isso com:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

> **Note**: Um esquema de endereçamento curinga é usado na instrução NAT. Essa instrução instrui o ASA a converter qualquer endereço de origem interno quando ele sair para a Internet. O endereço nesse comando pode ser mais específico, se desejado.

ASA versão 8.3 e posterior

Está aqui a configuração.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

Using the Manual Nat statements:

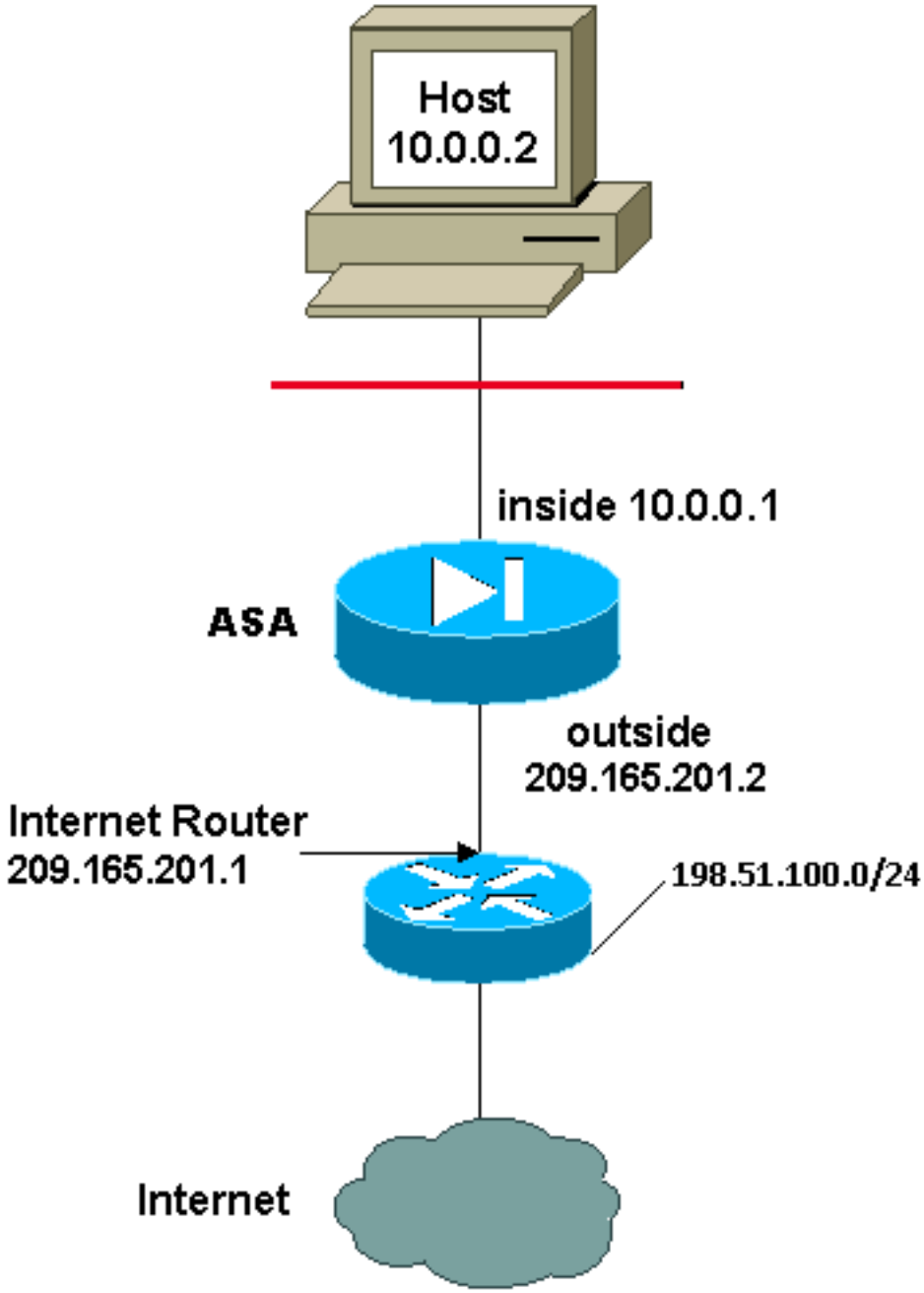
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

Using the Auto Nat statements:

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurar - Misturar instruções NAT e PAT

Diagrama de Rede



Neste exemplo, o ISP fornece ao gerente de rede um intervalo de endereços de 209.165.201.1 a 209.165.201.30 para que a empresa use. O gerente de rede decidiu usar 209.165.201.1 para a interface interna no roteador Internet e 209.165.201.2 para a interface externa no ASA. Você será deixado com 209.165.201.3 a 209.165.201.30 para usar o pool NAT. No entanto, o gerente de rede sabe que, a qualquer momento, pode haver mais de 28 pessoas tentando sair do ASA. O gerente de rede decidiu pegar 209.165.201.30 e torná-lo um endereço PAT para que vários usuários possam compartilhar um endereço ao mesmo tempo.

Esses comandos instruem o ASA a converter o endereço de origem em 209.165.201.3 a 209.165.201.29 para que os 27 primeiros usuários internos passem pelo ASA. Depois que esses endereços forem esgotados, o ASA converterá todos os endereços de origem subsequentes em 209.165.201.30 até que um dos endereços no pool NAT se torne livre.

> **Note**: Um esquema de endereçamento curinga é usado na instrução NAT. Essa instrução instrui o ASA a converter qualquer endereço de origem interno quando ele sair para a Internet. O endereço nesse comando pode ser mais específico, se desejado.

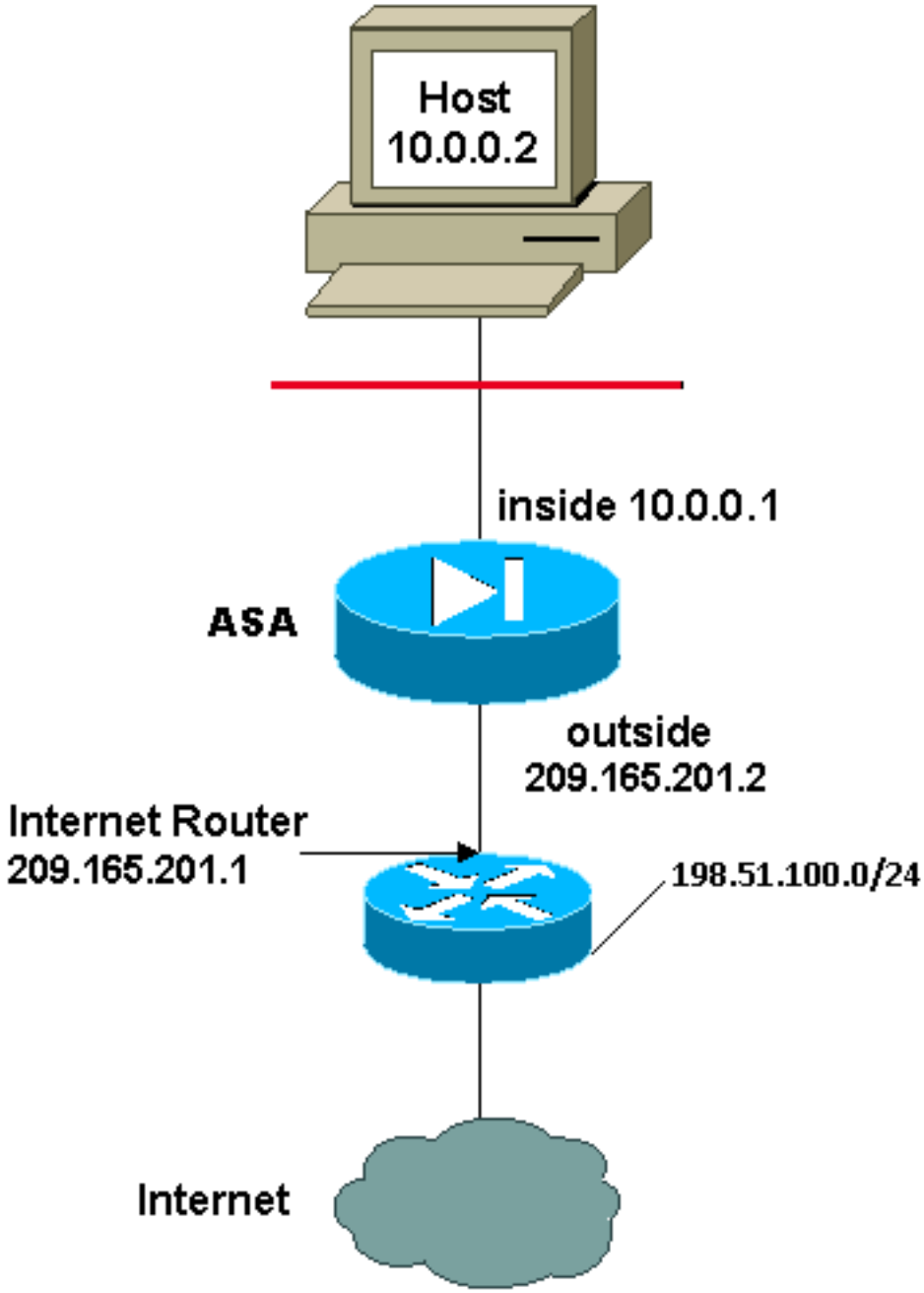
ASA versão 8.3 e posterior

Está aqui a configuração.

```
Using the Manual Nat statements:
object network any-1
subnet 0.0.0.0 0.0.0.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
subnet 209.165.201.30 255.255.255.224

nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

Using the Auto Nat statements:

object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

Configurar - Várias instruções NAT com instruções manuais

Diagrama de Rede



Neste exemplo, o ISP fornece novamente ao gerenciador de rede um intervalo de endereços de 209.165.201.1 a 209.165.201.30. O gerente de rede decide atribuir 209.165.201.1 à interface interna no roteador da Internet e 209.165.201.2 à interface externa do ASA.

No entanto, nesse cenário, outro segmento de LAN privado é colocado fora do roteador da Internet. O gerenciador de rede prefere não desperdiçar endereços do pool global quando os hosts nessas duas redes se comunicam entre si. O gerenciador de rede ainda precisa converter o endereço de origem para todos os usuários internos (10.0.0.0/8) quando ele sai para a Internet.

Essa configuração não converte esses endereços com um endereço de origem 10.0.0.0/8 e um endereço de destino 198.51.100.0/24. Ele converte o endereço de origem de qualquer tráfego iniciado na rede 10.0.0.0/8 e destinado para qualquer outro lugar que não 198.51.100.0/24 em um endereço do intervalo de 209.165.201.3 a 209.165.201.30.

Se você tiver a saída de um comando **write terminal** de seu dispositivo Cisco, poderá usar a Output Interpreter Tool (somente clientes registrados).

ASA versão 8.3 e posterior

Está aqui a configuração.

Using the Manual Nat statements:

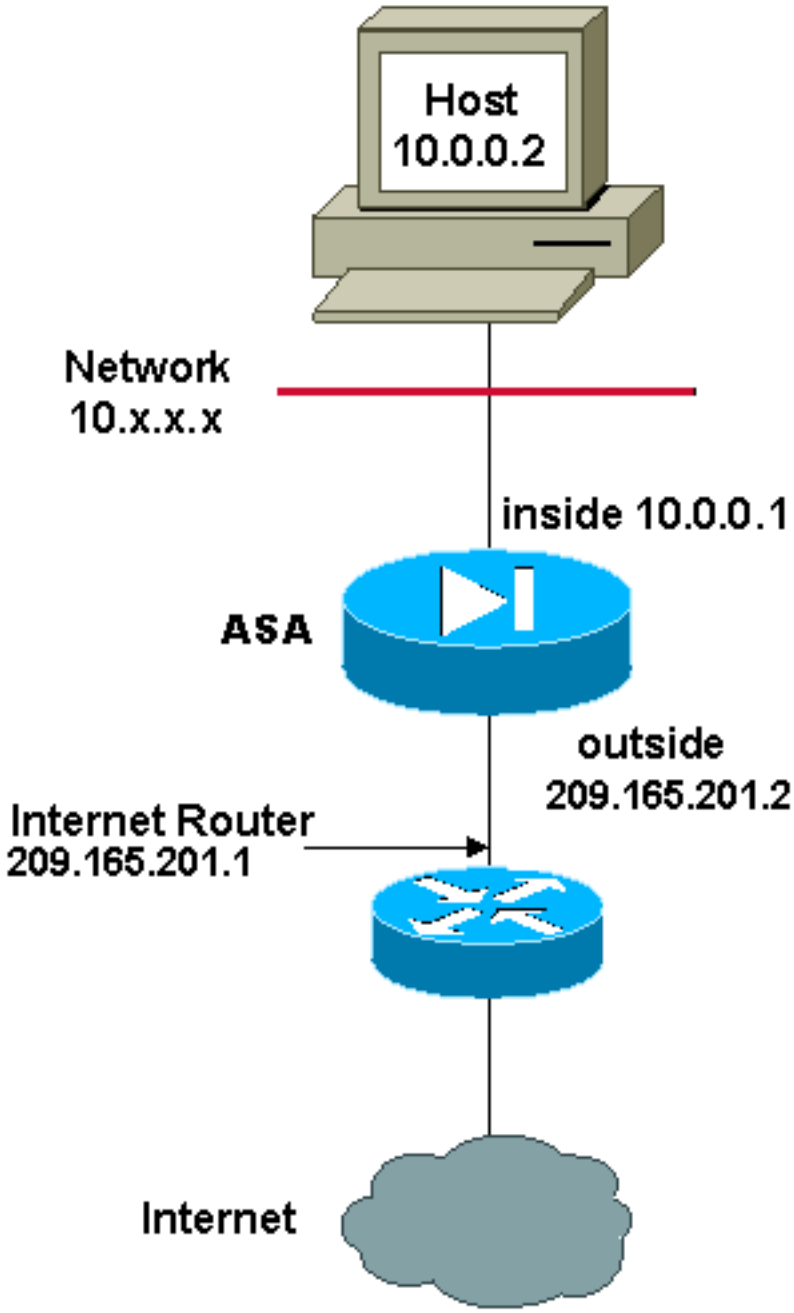
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

Using the Auto Nat statements:

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

Configurar - Usar NAT de política

Diagrama de Rede



Quando você usa uma lista de acesso com o comando **nat** para qualquer ID NAT diferente de 0, você habilita a política NAT.

O NAT de política permite identificar o tráfego local para tradução de endereços pela especificação dos endereços de origem e destino (ou portas) em uma lista de acesso. O NAT regular usa somente endereços/portas de origem. O NAT de política usa endereços/portas origem e destino.

> **Note**: Todos os tipos de NAT de política de suporte NAT, exceto para isenção de NAT (lista de acesso nat 0). A isenção de NAT usa uma ACL (Access Control List, lista de controle de acesso) para identificar os endereços locais, mas difere da NAT de política porque as portas não são consideradas.

Com a política NAT, você pode criar várias instruções NAT ou estáticas que identificam o mesmo endereço local, desde que a combinação origem/porta e destino/porta seja exclusiva para cada instrução. Em seguida, você pode combinar endereços globais diferentes para cada par origem/porta e destino/porta.

Neste exemplo, o gerenciador de rede deve fornecer acesso para o endereço IP destino 172.30.1.11 para a porta 80 (Web) e a porta 23 (Telnet), mas deve usar dois endereços IP diferentes como endereço origem. 209.165.201.3 é usado como um endereço de origem para a Web e 209.165.201.4 é usado para Telnet e deve converter todos os endereços internos, que estão no intervalo 10.0.0.0/8. O gerente de rede pode fazer isso com:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
172.30.1.11 255.255.255.255 eq 80
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
255.255.255.255 eq 23

nat (inside) 1 access-list WEB
nat (inside) 2 access-list TELNET
global (outside) 1 209.165.201.3 255.255.255.224
global (outside) 2 209.165.201.4 255.255.255.224
```

ASA versão 8.3 e posterior

Está aqui a configuração.

```
Using the Manual Nat statements:

object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

object network obj-172.30.1.11
host 172.30.1.11

object network obj-209.165.201.3
host 209.165.201.3

object network obj-209.165.201.4
host 209.165.201.4

object service obj-23
service tcp destination eq telnet

object service obj-80
service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

> **Note**: Para obter mais informações sobre a configuração de NAT e PAT no ASA versão 8.4, consulte Informações sobre NAT.
>
> Para obter mais informações sobre a configuração de listas de acesso no ASA versão 8.4, consulte Informações sobre listas de acesso.

Verificar

Tente acessar um site via HTTP com um navegador da Web. Este exemplo usa um site

hospedado em 198.51.100.100. Se a conexão for bem-sucedida, a saída na próxima seção pode ser vista na CLI do ASA.

Conexão

```
ASA(config)# show connection address 10.0.0.2
16 in use, 19 most used
TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137,
flags UIO
```

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

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

Syslog

```
ASA(config)# show log | in 10.0.0.2

Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.0.0.2/57431 to outside:209.165.201.3/57431

Jun 28 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.0.0.2/57431 (209.165.201.3/57431)
```

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

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

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

Conversões de NAT (Xlate)

```
ASA(config)# show xlate local 10.0.0.2
```

```
3 1in use, 810 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
0:12:22 timeout 0:00:30
```

Como parte dessa configuração, o PAT é configurado para converter os endereços IP do host interno em endereços roteáveis na Internet. Para confirmar se essas traduções foram criadas, você pode verificar a tabela xlate (tradução). O comando **show xlate,** quando combinado com a palavra-chave **local** e o endereço IP do host interno, mostra todas as entradas presentes na tabela de tradução para esse host. A saída anterior mostra que há uma conversão atualmente criada para esse host entre as interfaces interna e externa. O IP e a porta do host interno são convertidos para o endereço 10.165.200.226 por configuração.

Os flags listados, **r i** , indicam que a tradução é **dinâmica** e um **mapa**. Mais informações sobre diferentes configurações de NAT podem ser encontradas em Information About NAT.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.