在思科安全 ASA 防火墙使用 NAT 和 PAT 语句的配置示例

目录

简介

本文档介绍思科安全自适应安全设备 (ASA) 防火墙上的基本网络地址转换 (NAT) 和端口地址转换 (PAT) 配置示例。本文档还提供了简化的网络图。有关更多详细信息，请查阅相应 ASA 软件版本的 ASA 文档。

本文档对您的 Cisco 设备进行自定义分析。

有关详细信息，请参阅 ASA 5500/5500-X 系列安全设备上的 ASA 上的 NAT 配置。

先决条件

要求

思科建议您先了解思科安全 ASA 防火墙的知识。

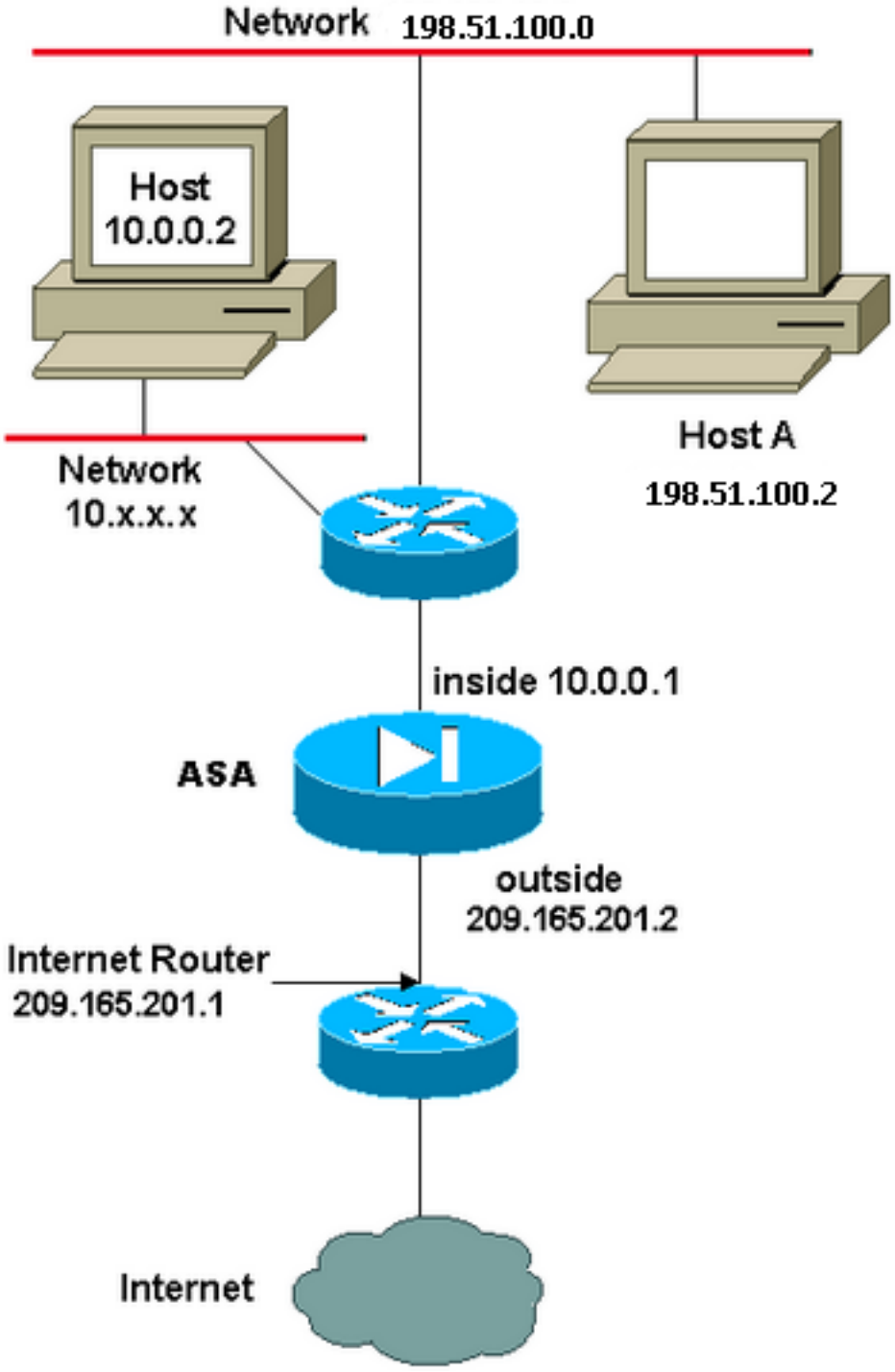
使用的组件

本文档中的信息基于思科安全 ASA 防火墙软件版本 8.4.2 及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置 - 使用手动和自动 NAT 的多个 NAT 语句

网络图



在本例中，ISP为网络管理员提供一个IP地址块209.165.201.0/27，范围为209.165.201.1到209.165.201.30。网络管理员决定将209.165.201.1分配给内部接口，以及209.165.201.2到ASA的外部接口。

网络管理员已为网络分配一个 C 类地址 198.51.100.0/24，并且有一些工作站使用这些地址访问互联网。这些工作站不需要任何地址转换，因为它们已经具有有效地址。但是，新工作站在10.0.0.0/8网络中分配了地址，需要转换这些地址(因为10.x.x.x是RFC 1918不可路由的地址空[间之二](#)。

为了适应此网络设计，网络管理员必须在 ASA 配置中使用两个 NAT 语句和一个全局池：

```
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
```

此配置不会转换来自 198.51.100.0/24 网络的任何出站流量的源地址。它会将 10.0.0.0/8 网络中的

源地址转换为从 209.165.201.3 到 209.165.201.30 范围内的地址。

> **注意**：当您有一个带有 NAT 策略的接口，但另一个接口没有全局池，此时您需要使用 nat 0 来设置 NAT 例外。

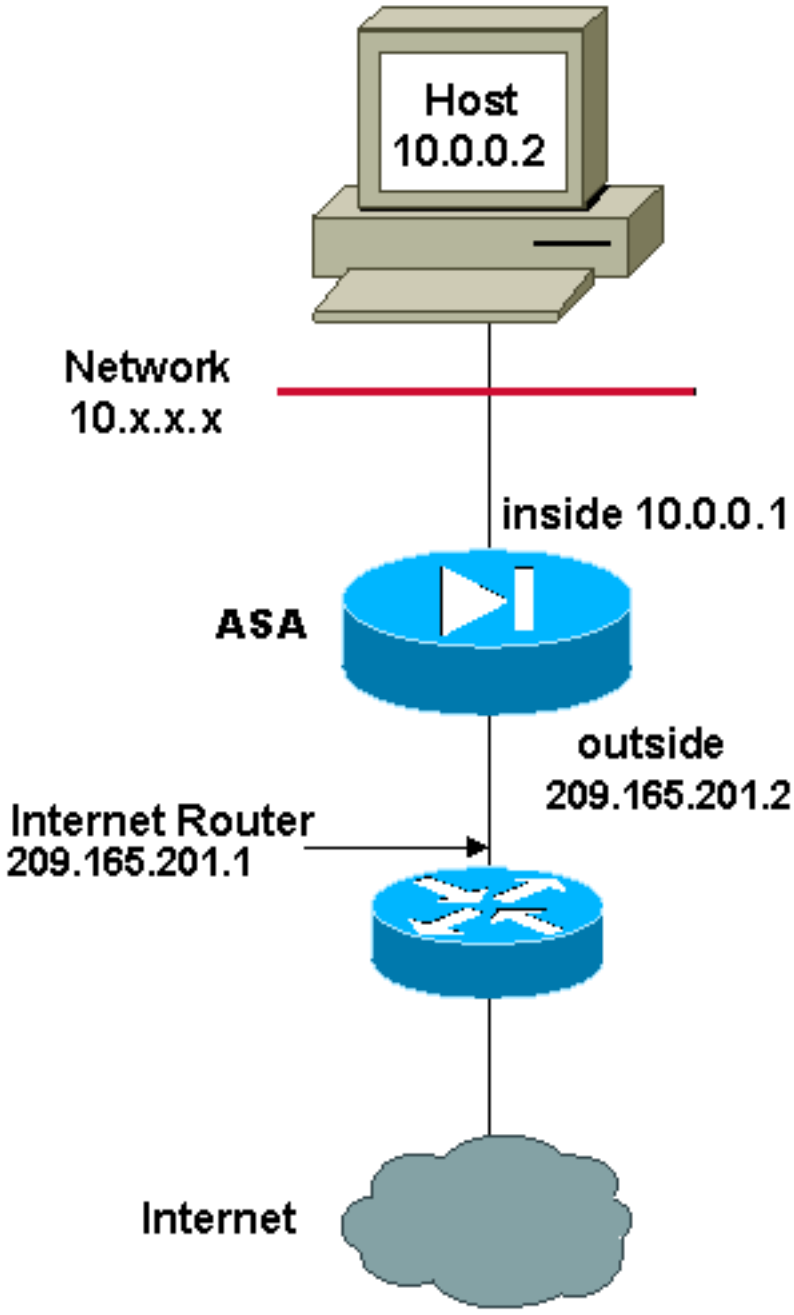
ASA 版本 8.3 及更高版本

配置如下。

```
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
```

配置 - 多个全局池

网络图



在本示例中，网络管理员有两个在 Internet 上注册的 IP 地址范围。网络管理员必须将所有内部地址（位于 10.0.0.0/8 范围中）转换为注册地址。网络管理器必须使用的IP地址范围是209.165.201.1到209.165.201.30和209.165.200.225到209.165.200.254.网络管理员可以通过以下方式实现：

```
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
```

> **注意**：NAT 语句中使用了通配符编址方案。此语句告诉 ASA 在离开互联网时转换任何内部源地址。如果需要，此命令中的地址可以更具体。

ASA 版本 8.3 及更高版本

配置如下。

```
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:

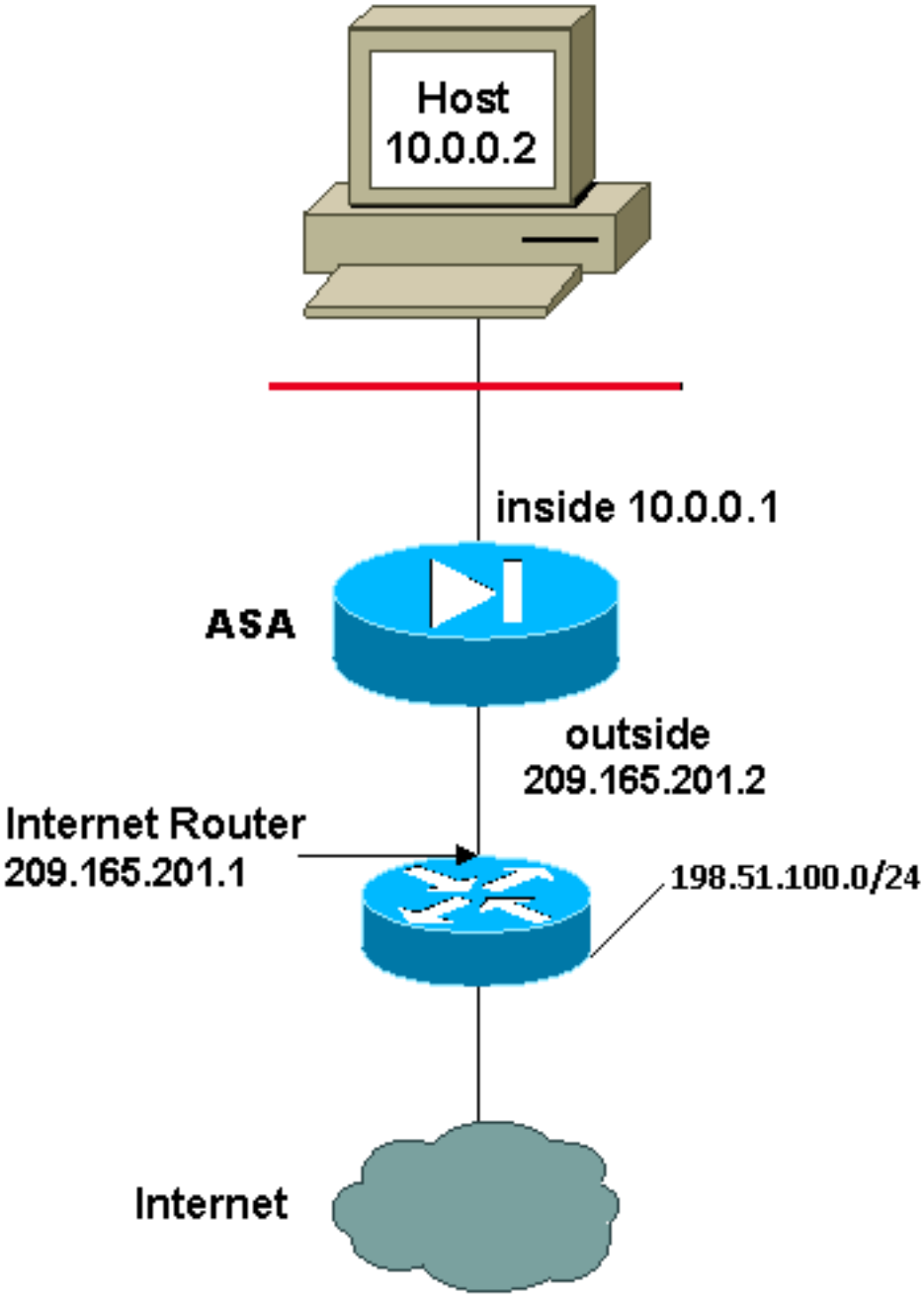
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

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
```

配置 - 混合 NAT 和 PAT 语句

网络图



在本示例中，ISP 为网络管理员提供了从 209.165.201.1 到 209.165.201.30 的地址范围，供公司使用。网络管理器已决定使用 209.165.201.1 作为互联网路由器上的内部接口，使用 209.165.201.2 作为 ASA 上的外部接口。剩下的从 209.165.201.3 到 209.165.201.30 之间的地址可用于 NAT 池。但网络管理员知道，在任何时候，尝试离开 ASA 的人都可能超过 28 人。网络管理员决定拿出 209.165.201.30 并将其设为 PAT 地址，以便多个用户可以同时共享一个地址。

这些命令指示 ASA 将源地址转换为 209.165.201.3 到 209.165.201.29，以便前 27 个内部用户通过 ASA。这些地址用完后，ASA 会将所有后续源地址转换为 209.165.201.30，直到 NAT 池中有一个地址变为空闲状态。

> **注意**：NAT 语句中使用了通配符编址方案。此语句告诉 ASA 在离开互联网时转换任何内部源地址。如果需要，此命令中的地址可以更具体。

ASA 版本 8.3 及更高版本

配置如下。

Using the Manual Nat statements:

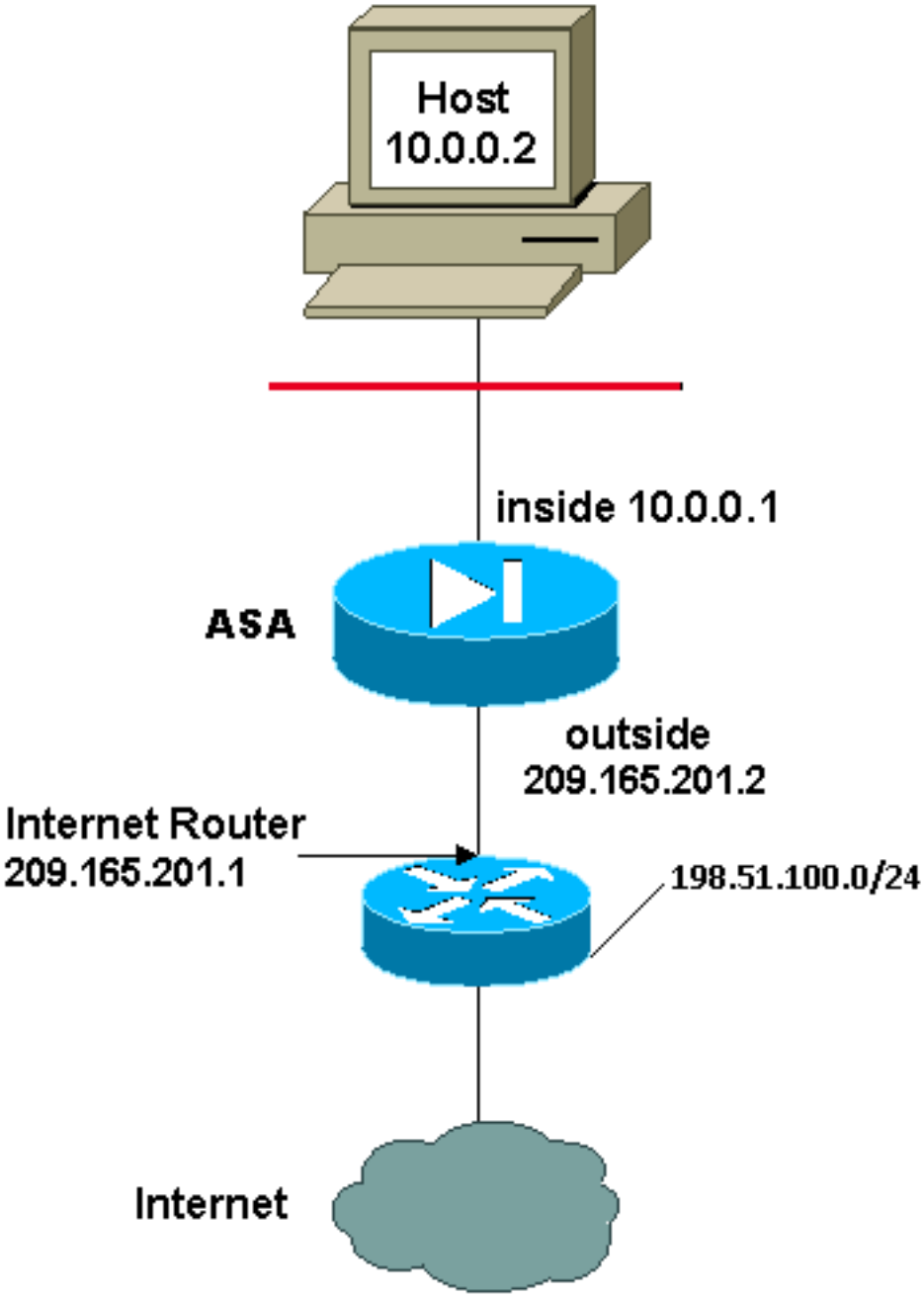
```
object network any-1
subnet 0.0.0.0 0.0.0.0

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
```

配置 - 包含手动语句的多个 NAT 语句

网络图



在本例中，ISP再次为网络管理器提供从209.165.201.1到209.165.201.30的地址范围。网络管理器决定将209.165.201.1分配给Internet路由器和2的内部接口09.165.201.2连接到ASA的外部接口。

但是，在此场景中，有另一个专用 LAN 网段位于 Internet 路由器之外。当这两个网络中的主机相互通信时，网络管理员不愿意浪费全局池中的地址。网络管理员仍然需要在访问 Internet 时转换所有内部用户的源地址 (10.0.0.0/8)。

此配置不会将源地址为10.0.0.0/8且目的地址为198.51.100.0/24的地址转换为地址，它会将源地址从10.0.0.0/8网络内发起且发往198.51.100.0/24以外任何位置的任何流量转换为从209.165.201.3到209.165的地址。201.30。

如果您有来自 Cisco 设备的 **write terminal 命令的输出，则可以使用**命令输出解释程序工具（仅限注册用户）。

ASA 版本 8.3 及更高版本

配置如下。

Using the Manual Nat statements:

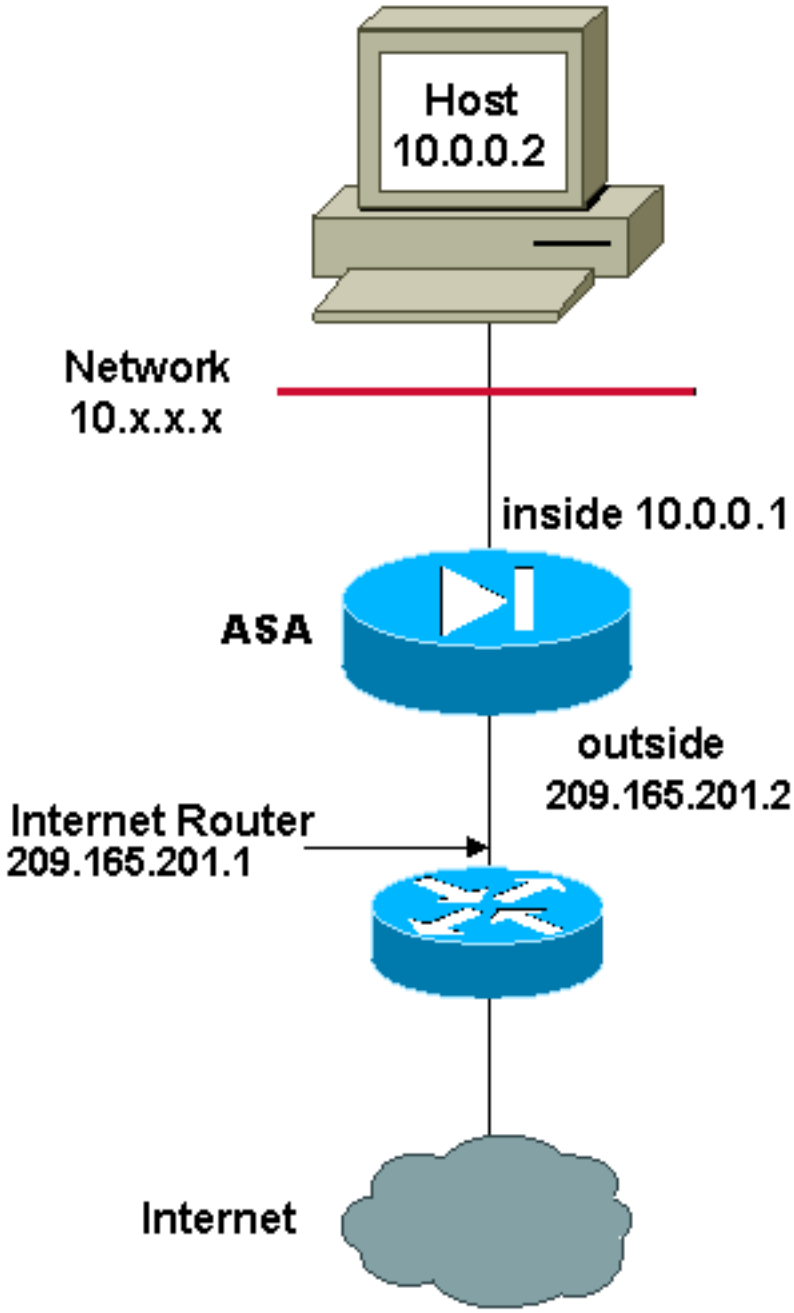
```
object network obj-10.0.0.0/8
subnet 10.0.0.0 255.0.0.0

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
```

配置 - 使用策略 NAT

网络图



当您对 0 以外的任何 NAT ID 配合使用访问列表和 **nat command 时，就会启用策略 NAT。**

策略 NAT 允许您通过在访问列表中指定源地址和目标地址（或端口），标识要进行地址转换的本地流量。常规 NAT 仅使用源地址/端口。策略 NAT 同时使用源和目标地址/端口。

> **注意：**除“NAT 免除”(nat 0 access-list) 以外的所有 NAT 类型都支持策略 NAT。NAT 免除使用访问控制列表 (ACL) 来识别本地地址，但与策略 NAT 不同，因为未考虑端口。

使用策略 NAT，可以创建多条标识同一本地地址的 NAT 或 static 语句（只要源/端口和目标/端口组合对于每条语句是唯一的）。然后，您可以将不同的全局地址匹配到每个源/端口和目标/端口对。

在本示例中，网络管理员需要为端口 80 (Web) 和端口 23 (Telnet) 提供对目标 IP 地址 172.30.1.11 的访问权限，但必须使用两个不同的 IP 地址作为源地址。209.165.201.3 用作 Web 的源地址，209.165.201.4 用作 Telnet，且必须转换 10.0.0.0/8 范围内的所有内部地址。网络管理员可使用以下命令执行此操作：

```
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 版本 8.3 及更高版本

配置如下。

```
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
```

> **注意**：有关在 ASA 版本 8.4 上配置 NAT 和 PAT 的详细信息，请参阅有关 NAT 的信息。
>
> 有关在 ASA 版本 8.4 上配置访问列表的详细信息，请参阅有关访问列表的信息。

验证

尝试使用 Web 浏览器通过 HTTP 访问网站。本示例使用托管于198.51.100.100的站点。如果连接成功，则可在ASA CLI上看到下一节的输出。

连接

```
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
```

ASA 是状态化防火墙，来自 Web 服务器的返回流量会因为与防火墙连接表中的***连接匹配，而被允许通过防火墙。***与既有连接匹配的流量不会被接口 ACL 阻止，即可通过防火墙。

在上面的输出中，内部接口上的客户端已经与外部接口上的主机 198.51.100.100 建立了连接。此连接是通过 TCP 协议建立的，而且已空闲 6 秒。连接标记表明此连接的当前状态。有关连接标记的更多信息，可参阅 ASA TCP 连接标记。

系统日志

```
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)
```

在正常运行期间，ASA 防火墙会生成系统日志。根据日志记录配置，系统日志的内容十分丰富。上面的输入显示了两个第 6 级别（即“信息”级别）的系统日志。

在此示例中，防火墙生成了两个系统日志。第一个系统日志记录的消息表明，防火墙已建立了转换，并明确指出是动态 TCP 转换 (PAT)。 从中可以看出流量从内部接口流向外部接口时的源 IP 地址和端口以及转换 IP 地址和端口。

第二个日志记录表明，防火墙已在其连接表中为该客户端与服务器之间的特定流量创建了一条连接。如果防火墙已配置为阻止此连接尝试，或者有其他因素禁止创建此连接（资源限制或配置错误），防火墙不会生成日志来表明建立了此连接。在这种情况下，防火墙会生成一条日志来说明连接被拒绝的原因，或者指明禁止创建连接的因素。

NAT 转换 (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
```

作为此配置的一部分，配置 PAT 是为了将内部主机 IP 地址转换为可在互联网上路由的地址。为了确认是否创建了这些转换，您可以查看 xlate（转换）表。show xlate 命令与 **local 关键字和内部主机的 IP 地址结合使用时，会显示该主机的转换表中存在的所有条目。**前面的输出显示，此主机当前在内部接口和外部接口之间建立了转换。内部主机 IP 和端口根据配置转换为 10.165.200.226 地址。

列出的标记 **ri 表示转换是动态的，并且是端口映射。**有关不同 NAT 配置的详细信息，请参阅有关 NAT 的信息。

故障排除

目前没有针对此配置的故障排除信息。