NAT和PAT在Cisco Secure ASA防火墙配置示例的语句使用

目录

简介

本文在Cisco Secure可适应安全工具(ASA)防火墙提供基本网络地址转换(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。参考您的ASA软件版本的ASA文档欲知更多详细信息。

本文档对您的 Cisco 设备进行自定义分析。

参考在ASA的NAT配置在ASA 5500/5500-X系列安全工具欲知更多信息。

先决条件

要求

思科建议您有Cisco Secure ASA防火墙的知识。

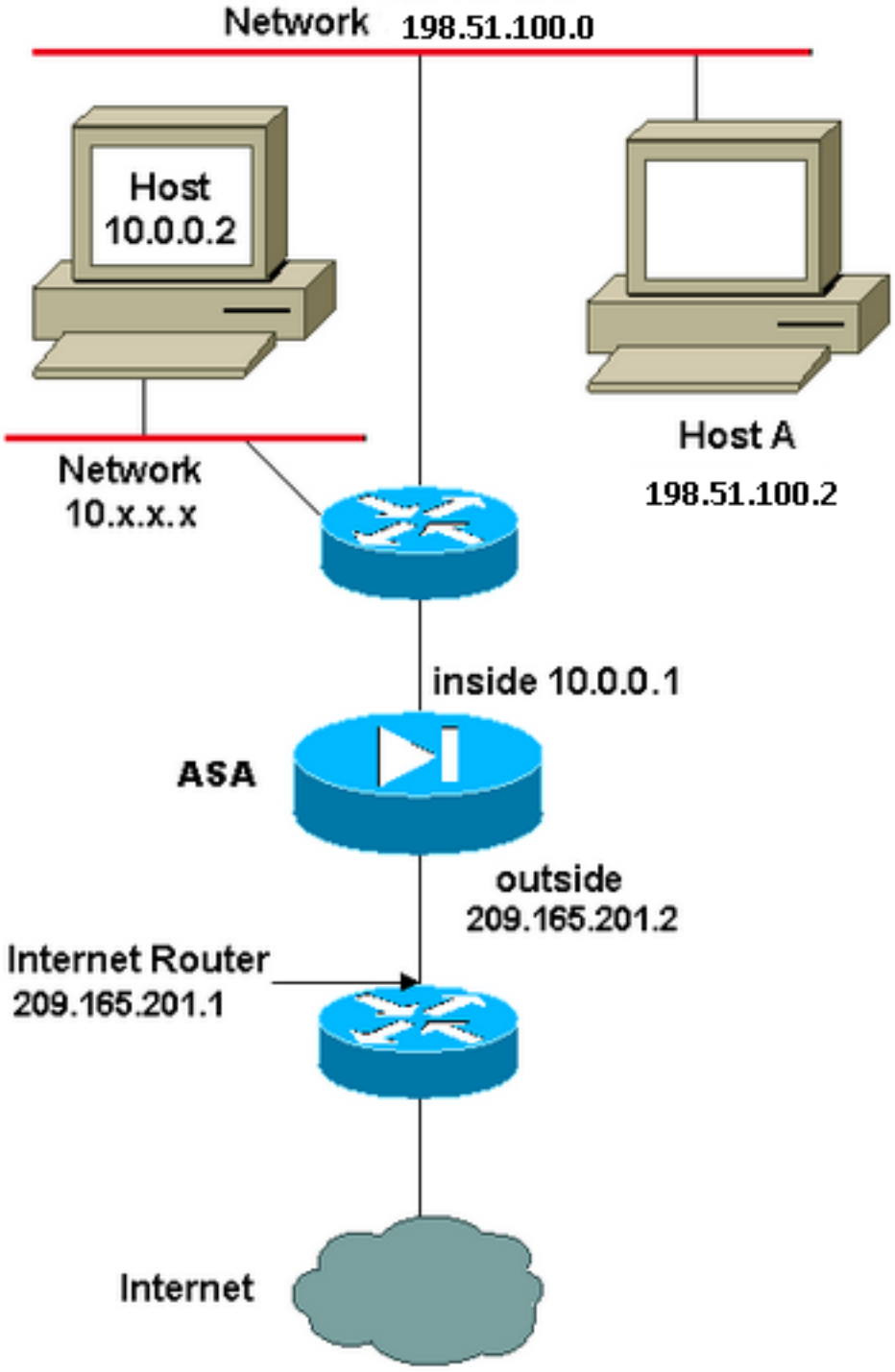
使用的组件

本文档中的信息根据Cisco Secure ASA防火墙软件版本8.4.2及以后。

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-多项NAT语句用手工和自动NAT

网络图



在本示例中，ISP 为网络管理员提供从 209.165.201.1 到 209.165.201.30 的 IP 地址块 209.165.201.0/27。网络管理器决定分配209.165.201.1对在互联网路由器的内部接口和209.165.201.2对ASA的外部接口。

网络管理员已经有C类地址分配到网络， 198.51.100.0/24，并且有使用这些地址为了访问互联网的一些工作站。因为他们已经有有效地址，这些工作站不要求任何地址转换。但是，新工作站被分配 10.0.0.0/8 网络中的地址，因此需要转换地址（因为根据 RFC 1918 ，10.x.x.x 是一个无法路由的地址空间）。

为了适应此网络设计，网络管理员必须在ASA配置里使用两个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
```

此配置不转换任何出站流量源地址从198.51.100.0/24网络的。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和以上

这是配置。

```
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
```

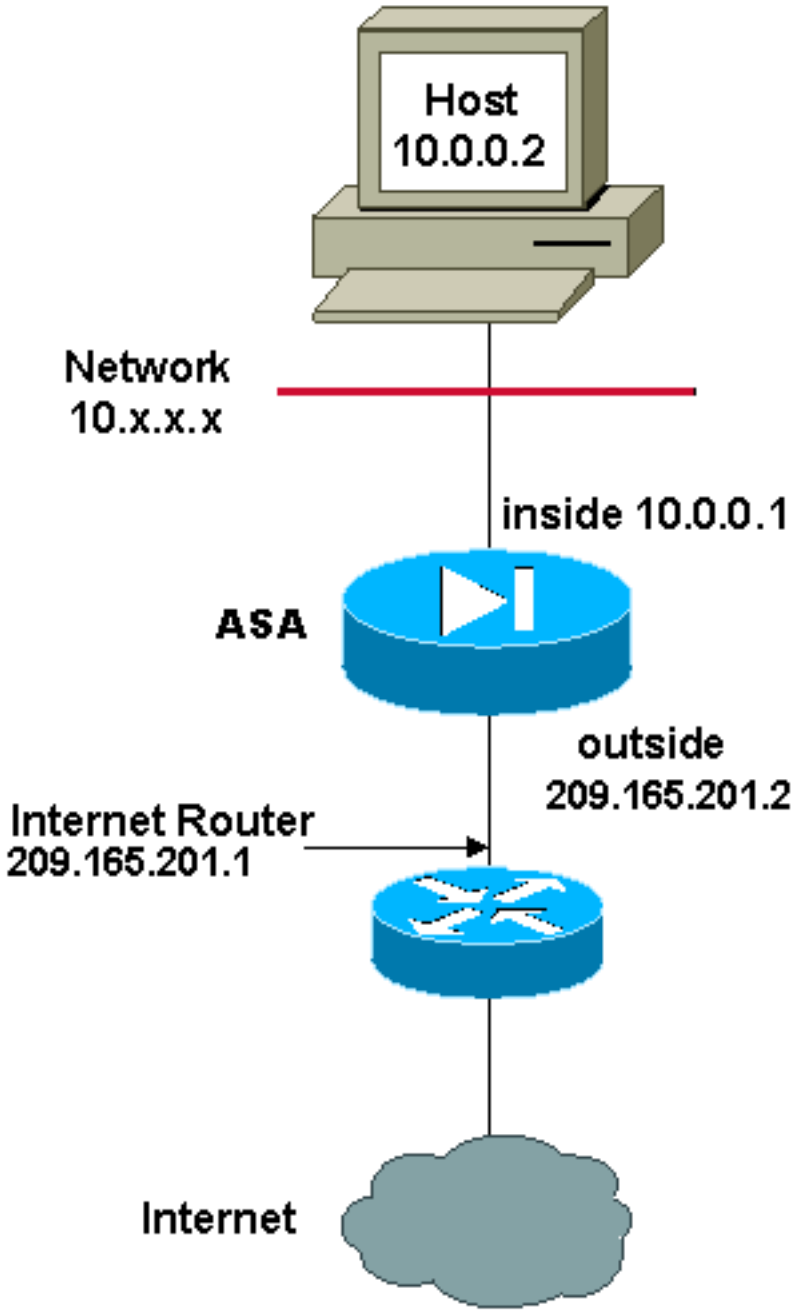
Using the Auto Nat statements:

```
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-多个全局地址池

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。网络管理员必须使用的 IP 地址范围是 209.165.201.1 到 209.165.201.30 以及 209.165.200.225 到 209.165.200.254。网络管理员可使用以下命令执行此操作：

```
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
```

> **注意**：NAT 语句中使用了通配符编址方案。当出去到互联网时，此语句告诉ASA转换所有内部源地址。如果需要，此命令中的地址可以更具体。

ASA版本8.3和以上

这是配置。

```
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
```

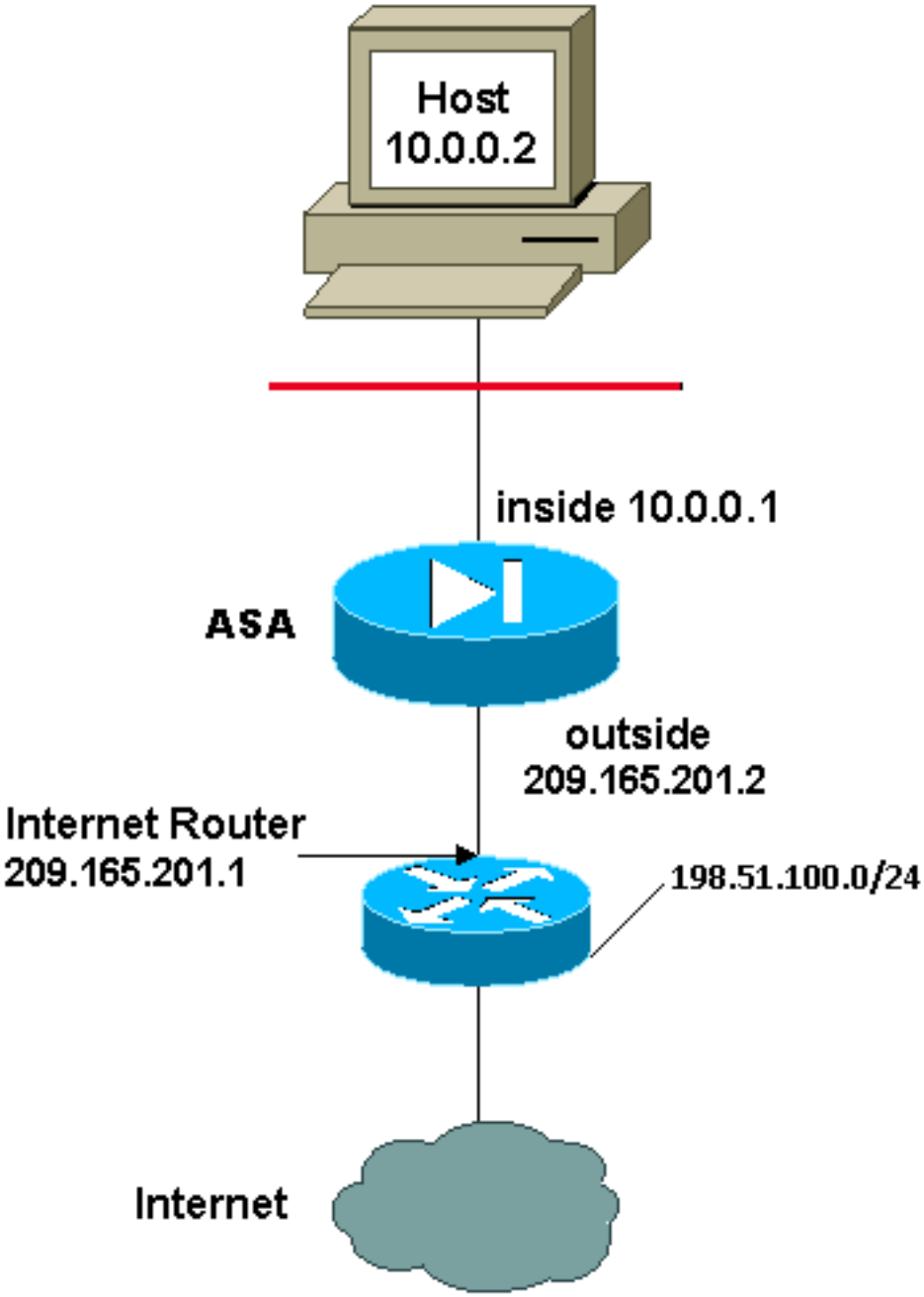
Using the Auto Nat statements:

```
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。网络管理器决定使用209.165.201.1在互联网路由器的内部接口和209.165.201.2在ASA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。然而，网络管理器知道可以，随时，有超过设法出去ASA的28个人。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通过前27个内部用户的209.165.201.29转换对209.165.201.3的源地址能在ASA间通过。在这些地址用尽后，然后ASA转换对209.165.201.30的所有随后的源地址，直到其中一个在NAT池的地址任意变为。

> **注意**：NAT 语句中使用了通配符编址方案。当出去到互联网时，此语句告诉ASA转换所有内部源地址。如果需要，此命令中的地址可以更具体。

ASA版本8.3和以上

这是配置。

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
```

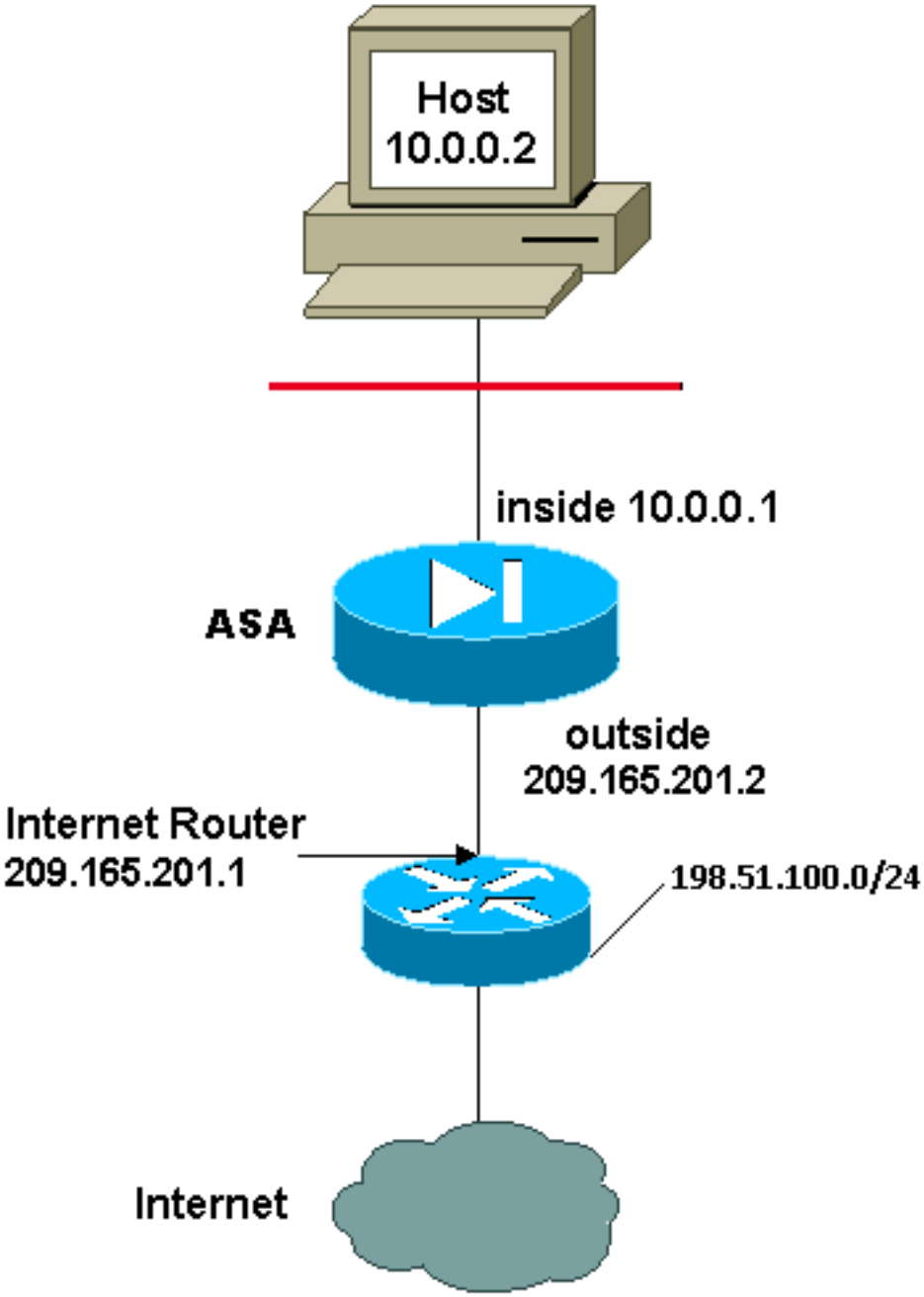
Using the Auto Nat statements:

```
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-与手工的语句的多项NAT语句

网络图



在本示例中，ISP 再次为网络管理员提供了从 209.165.201.1 到 209.165.201.30 的地址范围。网络管理器决定分配209.165.201.1对在互联网路由器的内部接口和209.165.201.2对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)。

此配置不转换与源地址为10.0.0.0/8和目的地址的那些地址为198.51.100.0/24。它转换从所有流量的源地址被初始化从10.0.0.0/8网络的内部和注定为任何地方除198.51.100.0/24之外到从范围209.165.201.3的一个地址通过209.165.201.30。

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和以上

这是配置。

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
```

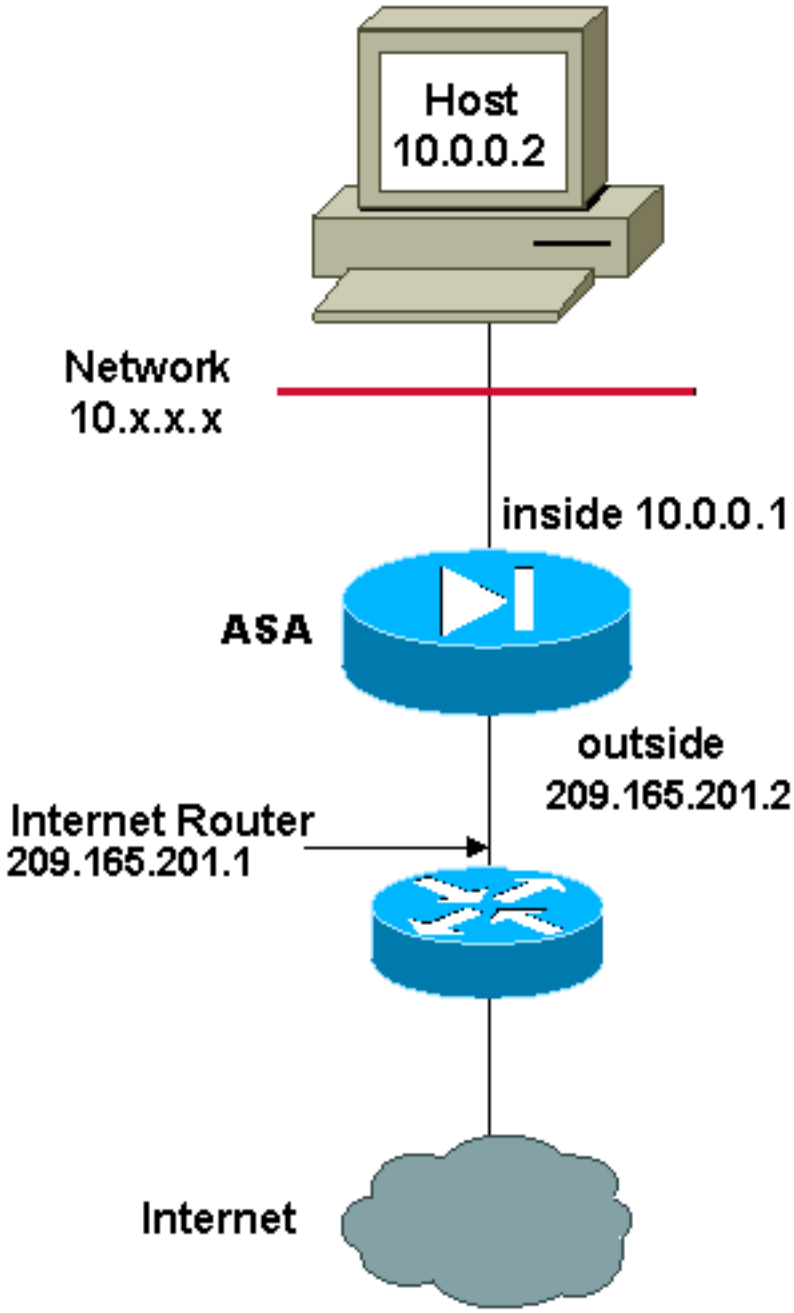
Using the Auto Nat statements:

```
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-请使用策略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。因为端口没有考虑， NAT免税使用访问控制表(ACL)为了识别本地地址，但是与策略NAT有所不同。

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。使用209.165.201.3，当Web和209.165.201.4的源地址使用Telnet，并且必须转换所有内部地址，在10.0.0.0/8范围。网络管理员可使用以下命令执行此操作：

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
```

ASA版本8.3和以上

这是配置。

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：关于NAT和PAT的配置的更多信息在ASA版本8.4，参考信息关于NAT。

关于访问列表的配置的更多信息在ASA版本8.4的，参考关于访问列表的信息。

验证

设法通过与浏览器的HTTP访问网站。此示例使用主机在198.51.100.100的一个站点。如果连接是成功的，在下一部分的输出在ASA CLI能被看到。

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是状态防火墙，并且从Web服务器的回程数据流允许上一步通过防火墙，因为在防火墙连接表里匹配一***连接***。匹配连接事先存在的流量通过防火墙允许，不用阻塞由接口ACL。

在上一个输出中，内部接口的客户端建立了对198.51.100.100主机的连接外部接口。此联系用TCP协议建立和是空闲在六秒。连接标志指示此连接的当前状态。关于连接标志的更多信息可以在ASA TCP连接标志找到。

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)
```

ASA防火墙在正常操作时生成Syslog。Syslog在根据操作日志配置的冗余排列。输出显示被看到在级别六的两Syslog，或者**'信息性'**级别。

在本例中，有生成的两Syslog。第一是表明的日志消息防火墙建立了**转换**，特别地一个动态TCP转换(PAT)。当流量从里面横断到外部接口，它指示源IP地址和端口和转换后的IP地址和端口。

第二Syslog表明防火墙在其此特定的流量的连接表里建立了**连接**在客户端和服务器之间。如果防火墙配置为了阻塞此连接尝试，或者某个其他要素禁止了此连接(资源约束或一可能的误配置)的创建，防火墙不会生成表明的日志连接被建立了。反而它将记录连接的一个原因能拒绝或关于什么要素的一个征兆从创建禁止了连接。

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
```

作为此配置一部分， PAT配置为了翻译内部主机IP地址到是可路由的在互联网的地址。为了确认这些转换创建，您能检查xlate (转换)表。show xlate命令，当与**本地关键字**和内部主机的IP地址结合，显示所有条目现在转换表里为该主机。上一个输出显示有为在内部和外部接口之间的此主机当前建立的转换。内部主机IP和端口翻译对10.165.200.226地址每配置。

标志列出了， **r我**，表明转换是**动态**和**portmap**。关于不同的NAT配置的更多信息可以在关于NAT的信息找到。

故障排除

目前没有针对此配置的故障排除信息。