NAT和PAT語句在Cisco Secure ASA防火牆上的使用配置示例

目錄

簡介

本檔案將提供思科安全調適型安全裝置(ASA)防火牆上的基本網路位址轉譯(NAT)和連線埠位址轉譯(PAT)設定範例。本文檔還提供簡化的網路圖。有關更多詳細資訊，請參閱ASA軟體版本的ASA文檔。

本文檔提供您思科裝置的定製分析。

有關詳細資訊，請參閱ASA 5500/5500-X系列安全裝置上的ASA上的NAT配置。

必要條件

需求

思科建議您瞭解Cisco Secure ASA防火牆。

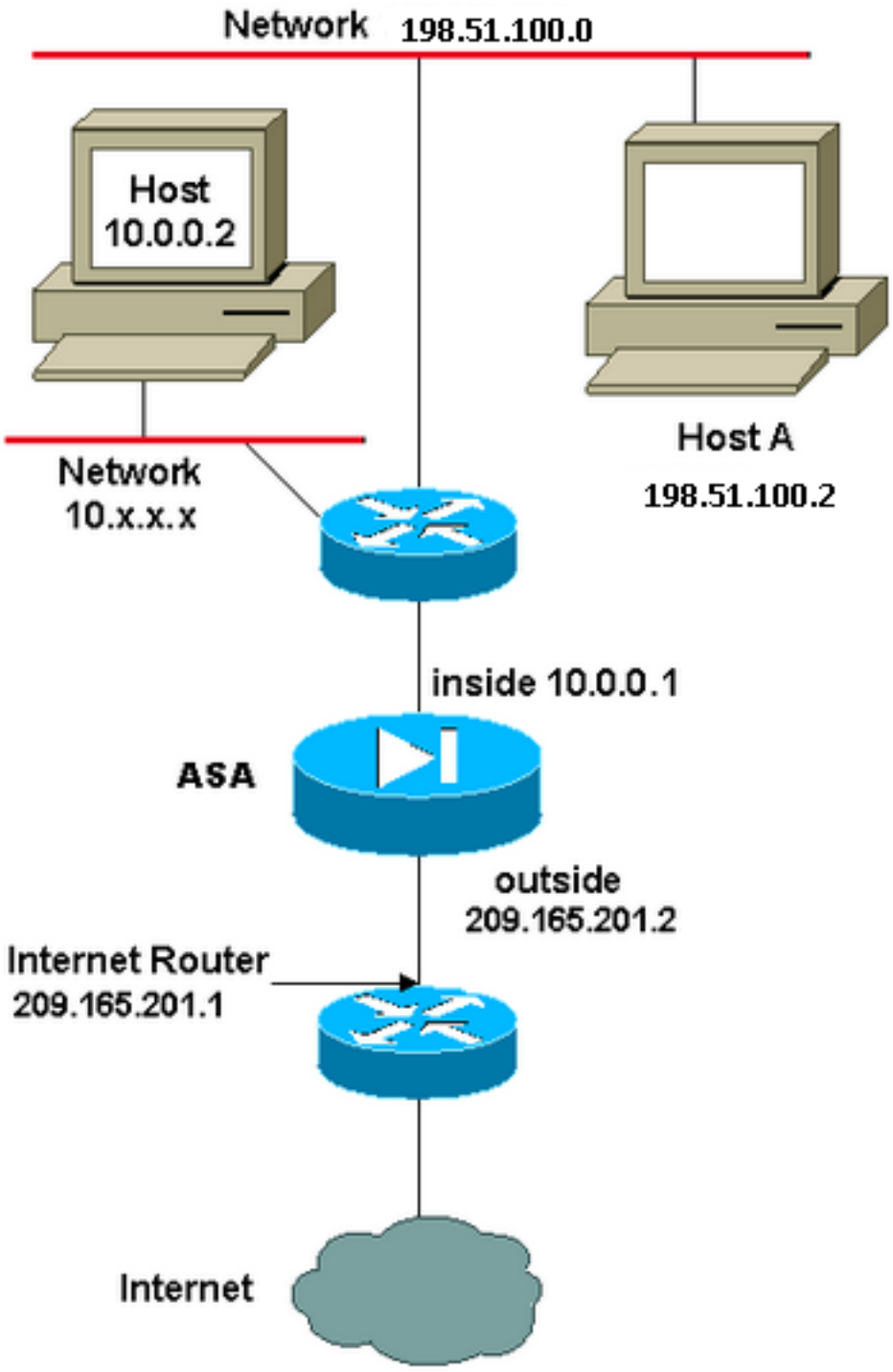
採用元件

本文檔中的資訊基於Cisco Secure ASA防火牆軟體版本8.4.2及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

配置 — 使用手動和自動NAT的多個NAT語句

網路圖表



在本例中，ISP為網路管理員提供範圍從209.165.201.1到209.165.201.30的IP地址塊209.165.201.0/27。網路管理員決定將209.165.201.1分配給Internet路由器上的內部介面，將209.165.201.2分配給ASA的外部介面。

網路管理員已經將一個C類地址分配給網路198.51.100.0/24，並且有一些工作站使用這些地址來訪問Internet。這些工作站已具有有效地址，因此不需要任何地址轉換。但是，在10.0.0.0/8網路中為新工作站分配地址，這些地址需要轉換(因為10.x.x.x是每個RFC 1918中不可路由的地址空間之一。

為了適應此網路設計，網路管理員必須在ASA配置中使用兩個NAT語句和一個全域性池：

```
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
```

此配置不會轉換來自198.51.100.0/24網路的任何出站流量的源地址。它將10.0.0.0/8網路中的源地址轉換為209.165.201.3到209.165.201.30範圍內的地址。

附註：當您有一個具有NAT策略的介面並且沒有到另一個介面的全域性池時，需要使用nat 0來設定NAT異常。

ASA 8.3及更高版本

以下是組態。

```
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
```

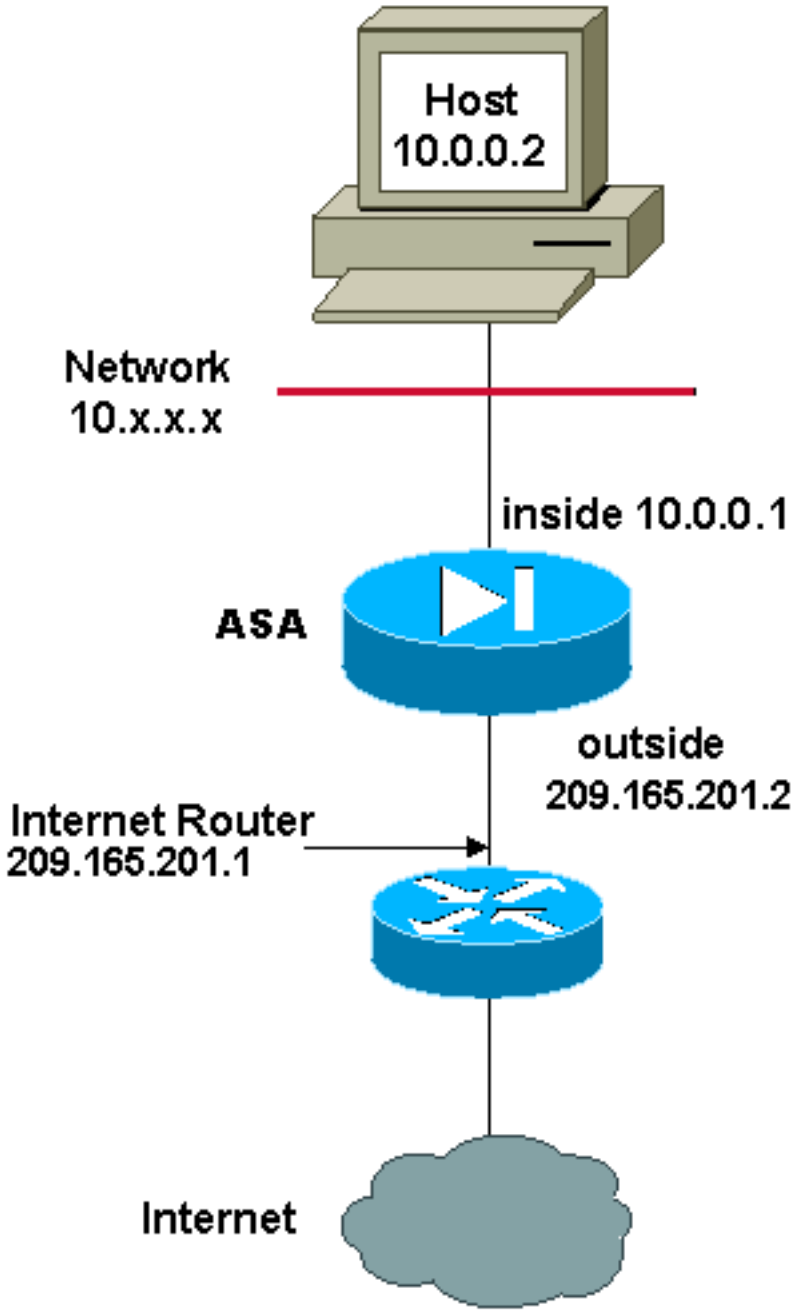
Using the Auto Nat statements:

```
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 — 多個全域性池

網路圖表



在本例中，網路管理器具有在Internet上註冊的兩個範圍的IP地址。網路管理員必須將10.0.0.0/8範圍內的所有內部地址轉換為註冊地址。網路管理員必須使用的IP位址範圍是209.165.201.1到209.165.201.30和209.165.200.225到209.165.200.254。網路管理員可以執行以下操作：

```
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
```

附註：NAT語句中使用了萬用字元定址方案。此語句通知ASA在內部源地址傳出Internet時對其進行轉換。如果需要，此命令中的地址可以更具體一些。

ASA 8.3及更高版本

以下是組態。

```
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
```

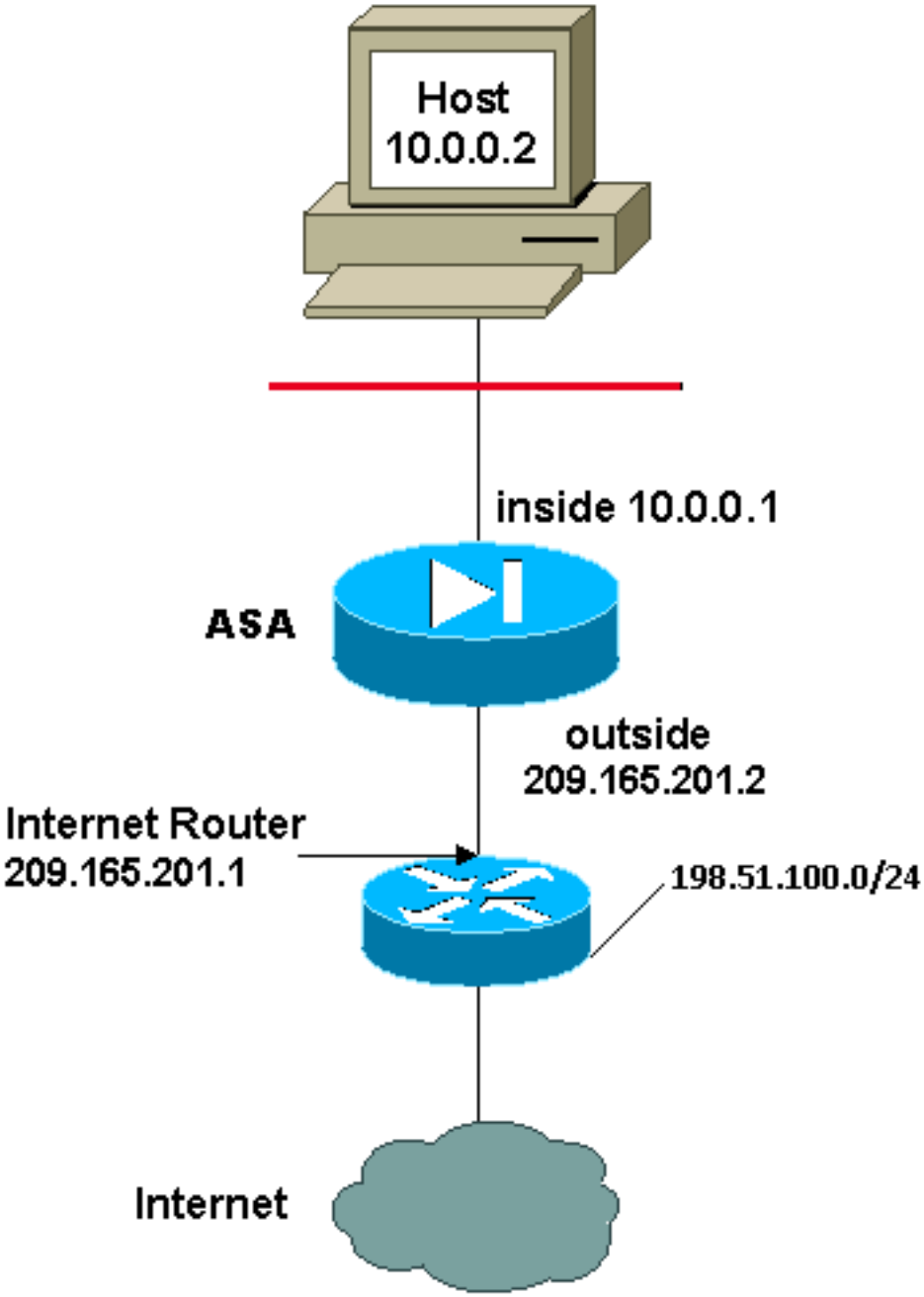
Using the Auto Nat statements:

```
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語句

網路圖表



在本例中，ISP為網路管理員提供從209.165.201.1到209.165.201.30的地址範圍以供公司使用。網路管理員決定將209.165.201.1用於Internet路由器上的內部介面，將209.165.201.2用於ASA上的外部介面。然後，您將使用209.165.201.3到209.165.201.30來用於NAT池。但是，網路經理知道，在任何時候，嘗試退出ASA的人員都可能超過28人。網路管理員決定採用209.165.201.30並將其作為PAT地址，以便多個使用者可以同時共用一個地址。

這些命令指示ASA將源地址轉換為209.165.201.3到209.165.201.29，以便前27個內部使用者通過ASA。在這些地址耗盡後，ASA會將所有後續源地址轉換為209.165.201.30，直到NAT池中的某個地址變為可用地址。

> **附註**：NAT語句中使用了萬用字元定址方案。此語句通知ASA在內部源地址傳出Internet時對其進行轉換。如果需要，此命令中的地址可以更具體一些。

ASA 8.3及更高版本

以下是組態。

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
```

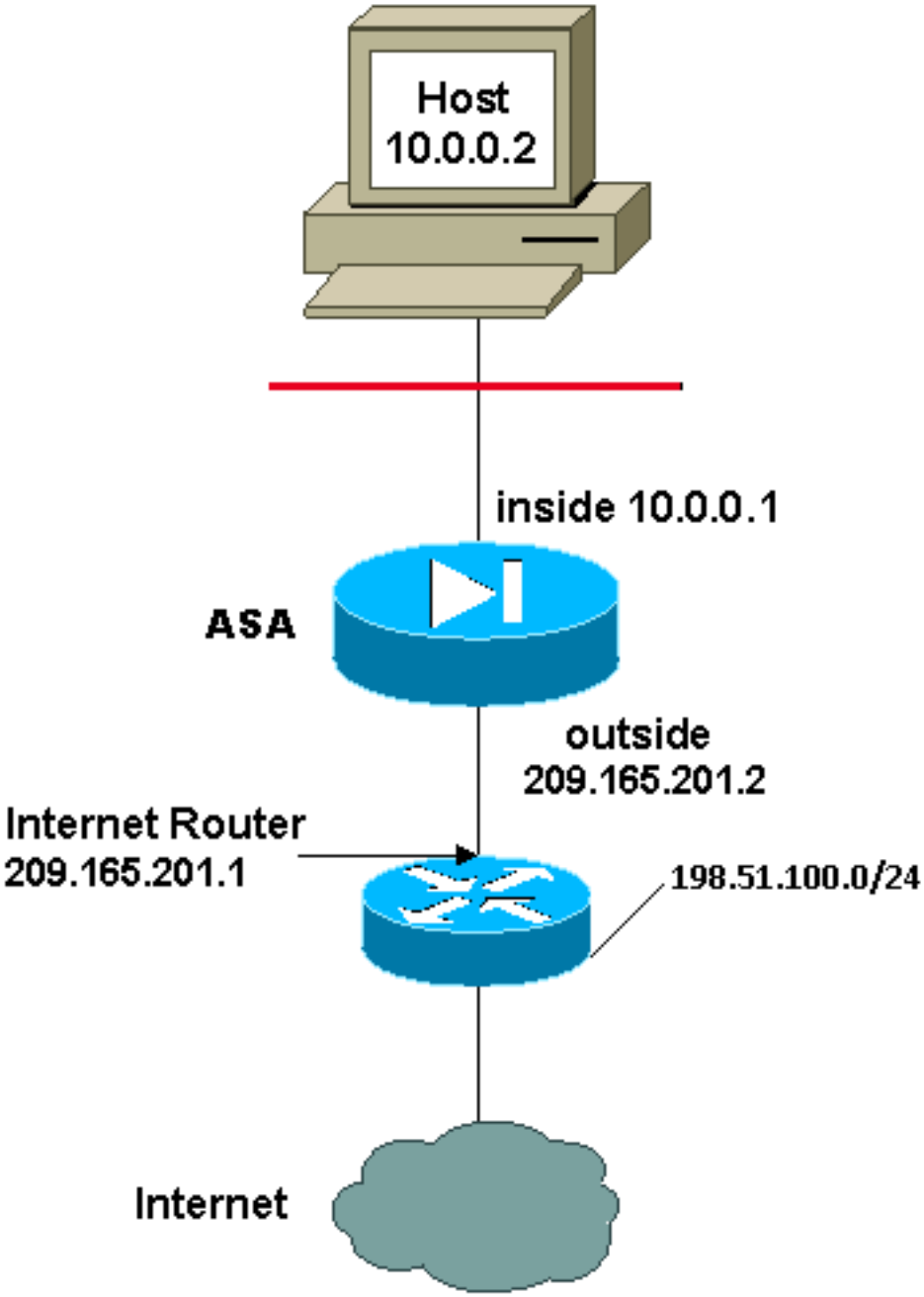
Using the Auto Nat statements:

```
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 — 使用手動語句的多條NAT語句

網路圖表



在本例中，ISP再次為網路管理員提供從209.165.201.1到209.165.201.30的地址範圍。網路管理員決定將209.165.201.1分配給Internet路由器上的內部介面，將209.165.201.2分配給ASA的外部介面。

但是在此案例中，另一個私有LAN網段是從Internet路由器放置的。當這兩個網路中的主機相互通訊時，網路管理員不希望浪費全域性池中的地址。當網路管理器輸出到網際網路時，仍然需要轉換所有內部使用者的源地址(10.0.0.0/8)。

此組態不會將來源位址為10.0.0.0/8、目的地位址為198.51.100.0/24的位址轉譯。它會將來源位址從從10.0.0.0/8網路中起始且目的地為198.51.100.0/24以外的任何流量的來源位址轉譯成從209.165.201.3到209.165.201.30範圍內的位址。

如果您的Cisco裝置具有**write terminal**指令的輸出，可以使用輸出直譯器工具(僅限註冊客戶)。

ASA 8.3及更高版本

以下是組態。

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
```

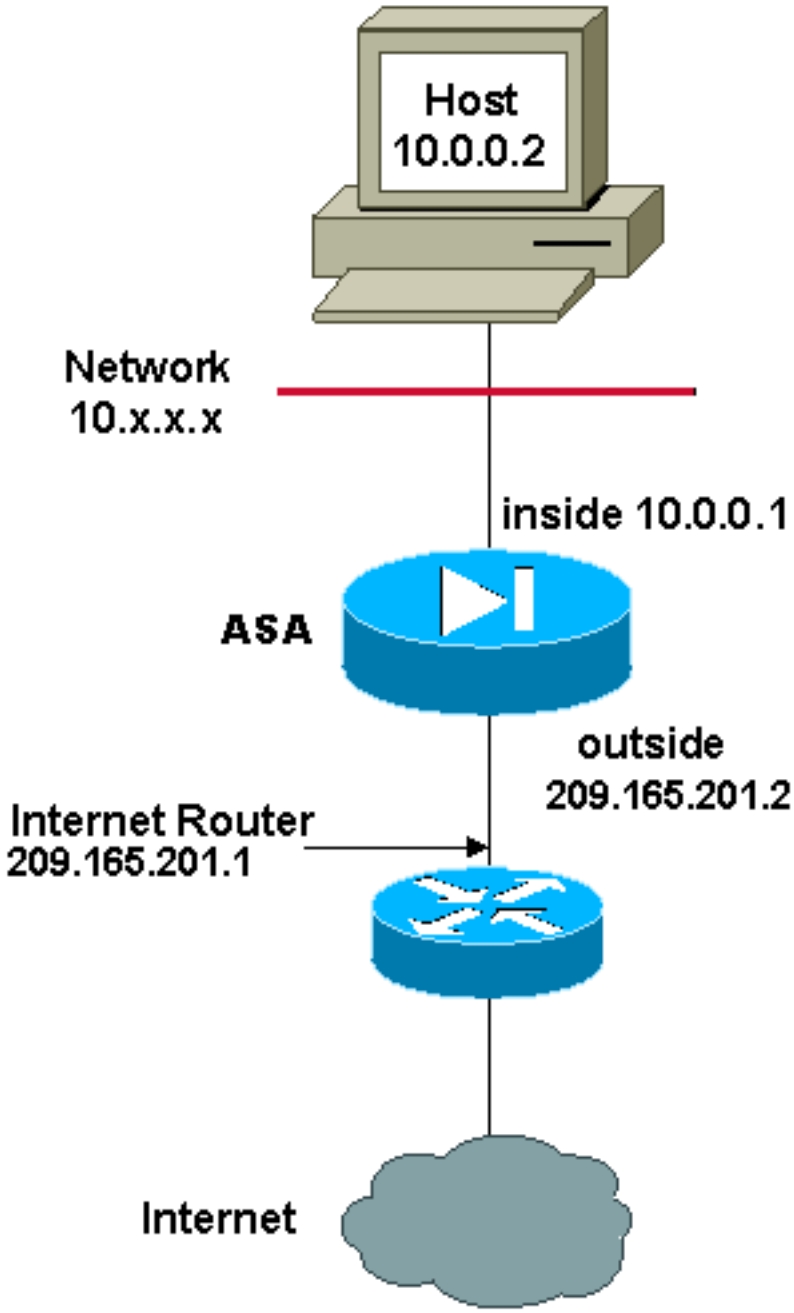
Using the Auto Nat statements:

```
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

網路圖表



將訪問清單與**nat**命令一起用於除0以外的任何NAT ID時，將啟用策略NAT。

策略NAT允許您根據訪問清單中源和目標地址（或埠）的規範來標識本地流量以進行地址轉換。常規NAT僅使用源地址/埠。策略NAT同時使用源地址和目標地址/埠。

> **附註**：除NAT免除（nat 0訪問清單）外，所有型別的NAT都支援策略NAT。NAT豁免使用訪問控制清單(ACL)來識別本地地址，但不同於策略NAT，因為未考慮埠。

使用策略NAT，可以建立多個NAT或靜態語句，只要源/埠和目標/埠組合對於每條語句是唯一的，這些語句就標識同一個本地地址。然後，您可以將不同的全域性地址與每個源/埠和目標/埠對匹配。

在本例中，網路管理員必須為埠80(Web)和埠23(Telnet)提供目標IP地址172.30.1.11的訪問許可權，但必須使用兩個不同的IP地址作為源地址。209.165.201.3用作Web的源地址，209.165.201.4用作Telnet，必須轉換10.0.0.0/8範圍內的所有內部地址。網路管理員可以執行以下操作：

```
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 8.3及更高版本

以下是組態。

```
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
```

附註：有關ASA 8.4版上的NAT和PAT配置的詳細資訊，請參閱有關NAT的資訊。

有關ASA 8.4版中訪問清單配置的詳細資訊，請參閱關於訪問清單的資訊。

驗證

嘗試使用Web瀏覽器通過HTTP訪問網站。此示例使用託管在198.51.100.100上的站點。如果連線成功，則在ASA CLI上可以看到下一部分中的輸出。

連線

```
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是一個有狀態防火牆，來自Web伺服器的返回流量允許通過防火牆，因為它與防火牆連線表中的***連線***匹配。與預先存在的連線匹配的流量允許通過防火牆，不會被介面ACL阻止。

在前面的輸出中，內部介面上的客戶端已經從外部介面建立了到198.51.100.100主機的連線。此連線是使用TCP協定建立並且已空閒六秒。連線標誌指示此連線的當前狀態。有關連線標誌的詳細資訊，請參閱ASA TCP連線標誌。

系統日誌

```
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防火牆在正常運行期間生成系統日誌。系統日誌的範圍取決於日誌記錄配置。輸出顯示在級別6或「資訊」級別上看**到的兩個**syslog。

在此示例中，生成了兩個系統日誌。第一個是指示防火牆已建立**轉換**（尤其是動態TCP轉換[PAT]）的日誌消息。 它表示流量從內部到外部介面傳輸時的源IP地址和埠以及轉換後的IP地址和埠。

第二個系統日誌表示防火牆在其連線表中為客戶端和伺服器之間的此特定流量建立了一個**連線**。如果防火牆配置為阻止此連線嘗試，或者某個其他因素阻止了此連線的建立（資源限制或可能的配置錯誤），則防火牆不會生成指示已建立連線的日誌。相反，它將記錄拒絕連線的原因，或有關禁止建立連線的因素的指示。

NAT轉譯(Xlate)

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

作為此配置的一部分，配置PAT以將內部主機IP地址轉換為可在網際網路上路由的地址。為了確認已建立這些轉換，您可以檢查xlate（轉換）表。**show xlate**命令與**local**關鍵字和內部主機的IP地址結合使用時，會顯示該主機的轉換表中存在的所有條目。上一個輸出顯示，當前已為此主機在內部和外部介面之間構建轉換。根據配置，內部主機IP和埠將轉換為10.165.200.226地址。

列出的標誌**r i**表示轉換是動態**的**，並為**portmap**。有關不同NAT配置的詳細資訊，請參閱有關NAT的資訊。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。