為雙內部網路配置ASA

目錄

簡介

本文檔介紹如何配置運行軟體版本9.x的思科自適應安全裝置(ASA)以使用兩個內部網路。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於運行軟體版本9.x的Cisco ASA。

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。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

當您在ASA防火牆後面新增第二個內部網路時，請考慮以下重要資訊：

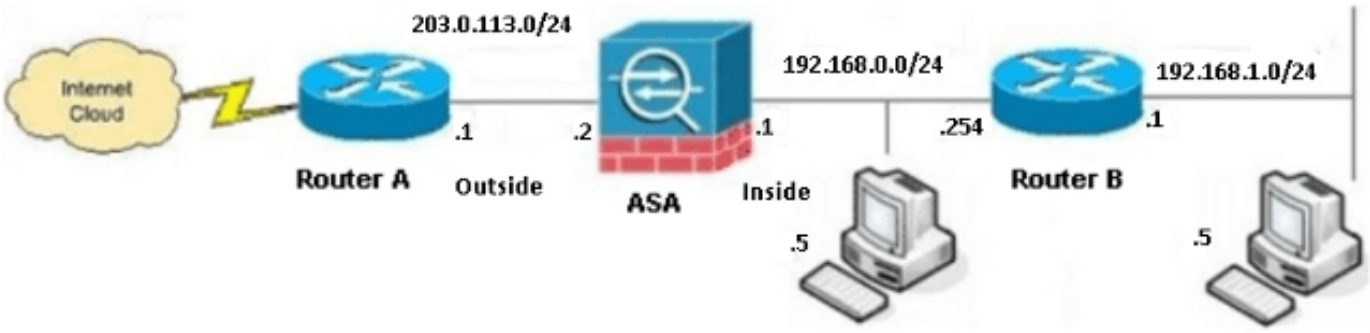
- ASA不支援輔助定址。
- 必須在ASA後面使用路由器，以在當前網路和新新增的網路之間實現路由。
- 所有主機的預設網關必須指向內部路由器。
- 必須在指向ASA的內部路由器上新增預設路由。
- 您必須清除內部路由器上的位址解析通訊協定(ARP)快取。

設定

使用本節中介紹的資訊配置ASA。

網路圖表

以下是本文檔中示例使用的拓撲：



附註：此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

ASA 9.x配置

如果您的Cisco裝置具有**write terminal**命令的輸出，可以使用Output Interpreter工具(僅供註冊客戶使用)以顯示潛在問題和修正程式。

以下是運行軟體版本9.x的ASA的配置：

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
```

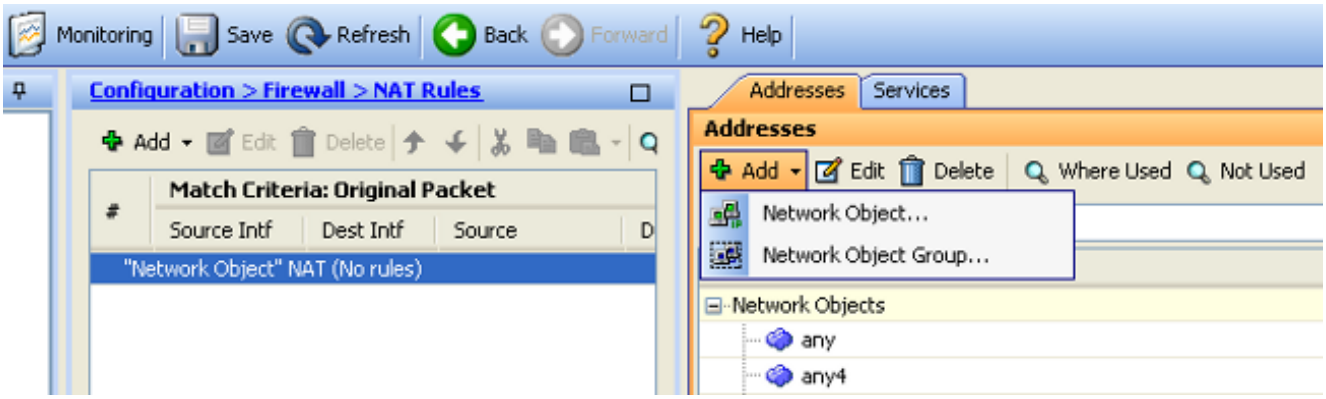
```
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

允許內部主機通過PAT訪問外部網路

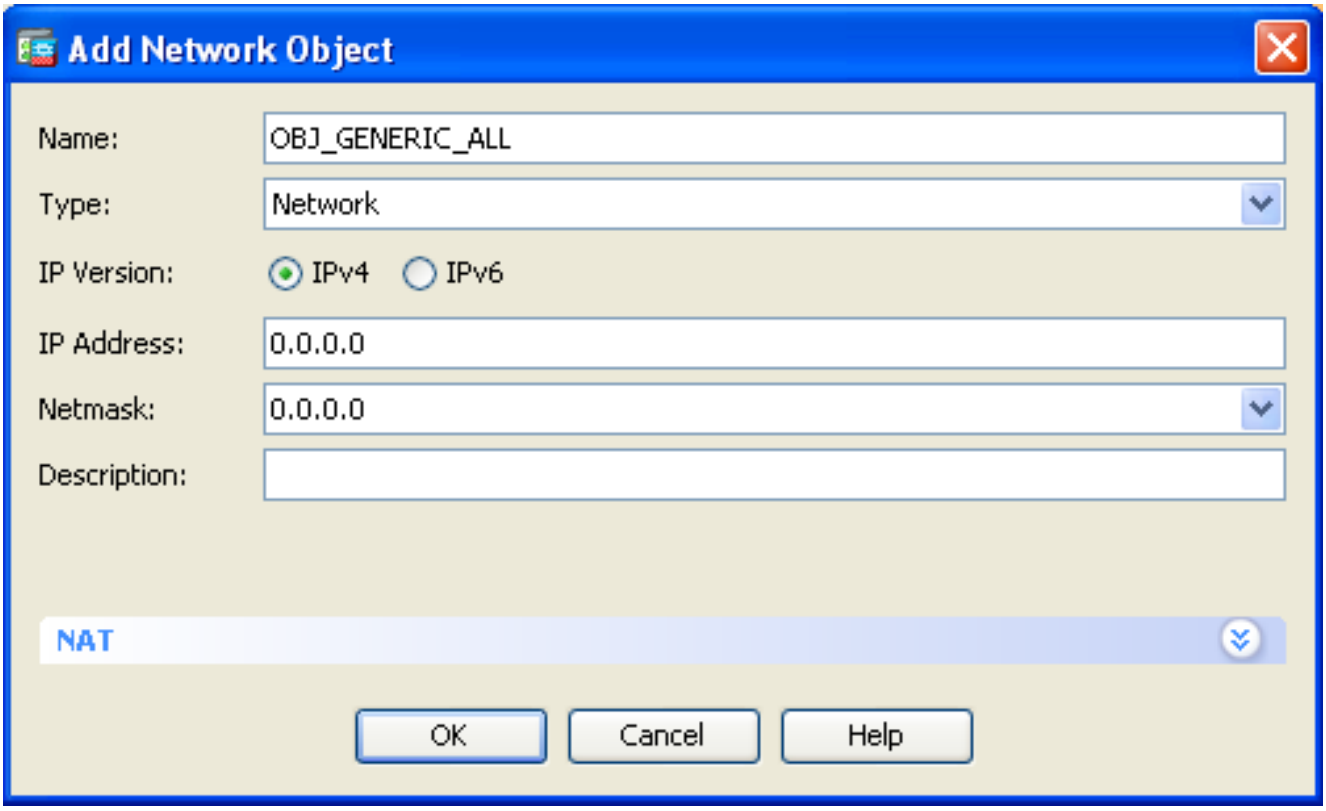
如果您希望讓內部主機共用一個公共地址進行轉換，請使用埠地址轉換(PAT)。 最簡單的PAT配置之一涉及所有內部主機的轉換，以使它們看起來像外部介面IP。當ISP提供的可路由IP地址數量限製為少數幾個或只有一個時，通常使用這種PAT配置。

完成以下步驟，允許內部主機使用PAT存取外部網路：

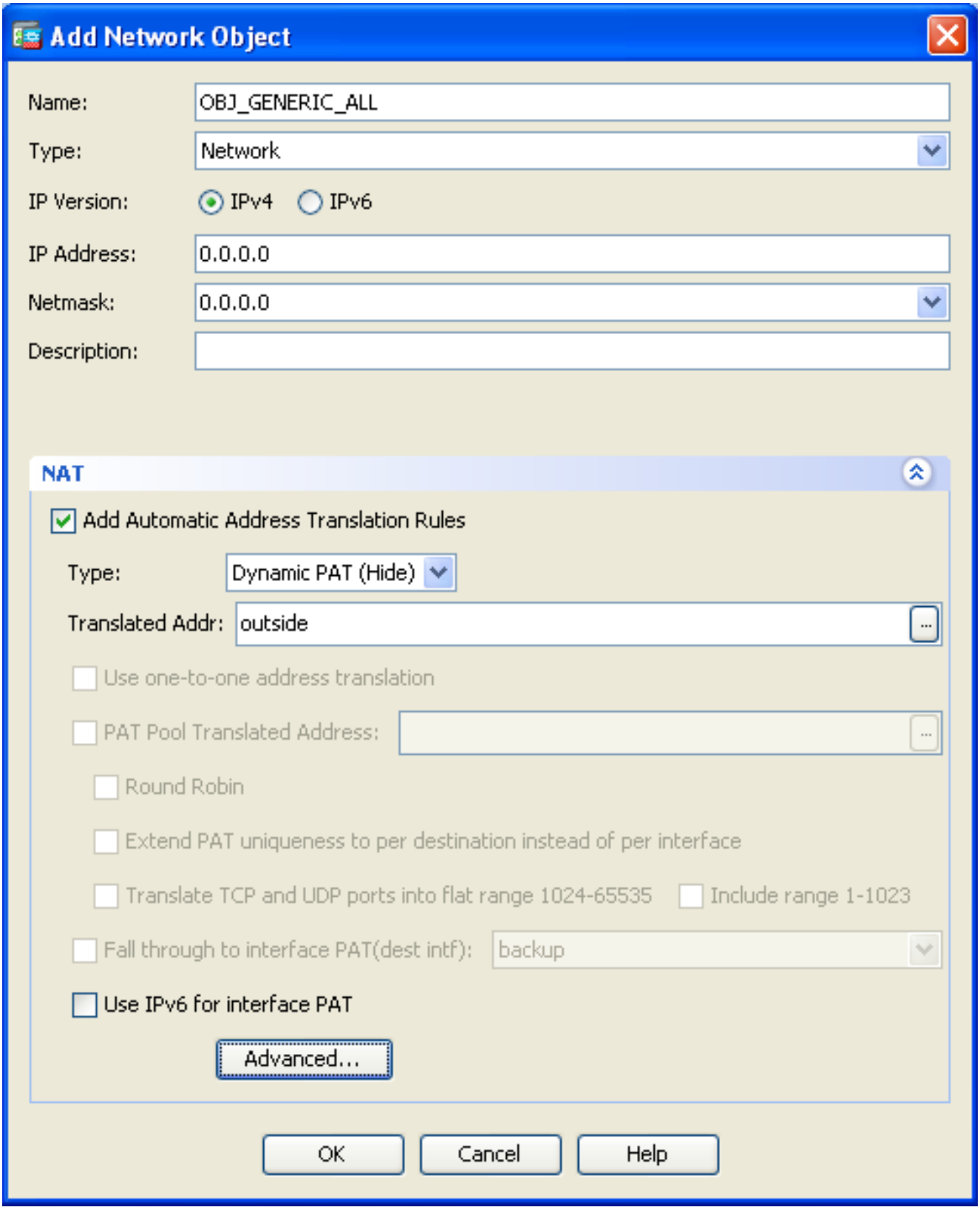
1. 導航到Configuration > **Firewall > NAT Rules**，按一下**Add**，然後選擇**Network Object**以配置動態NAT規則：



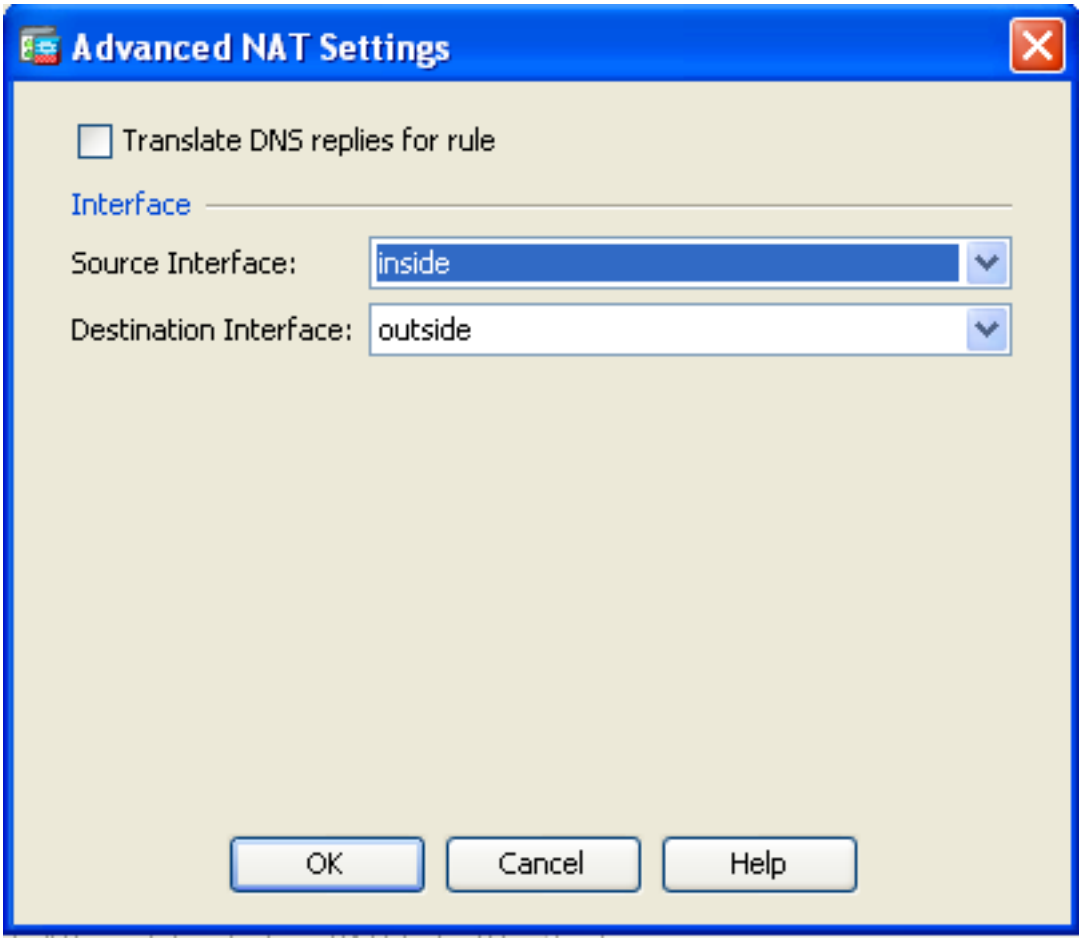
2. 配置需要動態PAT的網路/主機/範圍。在此示例中，已選擇所有內部子網。對於要以此方式轉換的特定子網，應重複此過程：



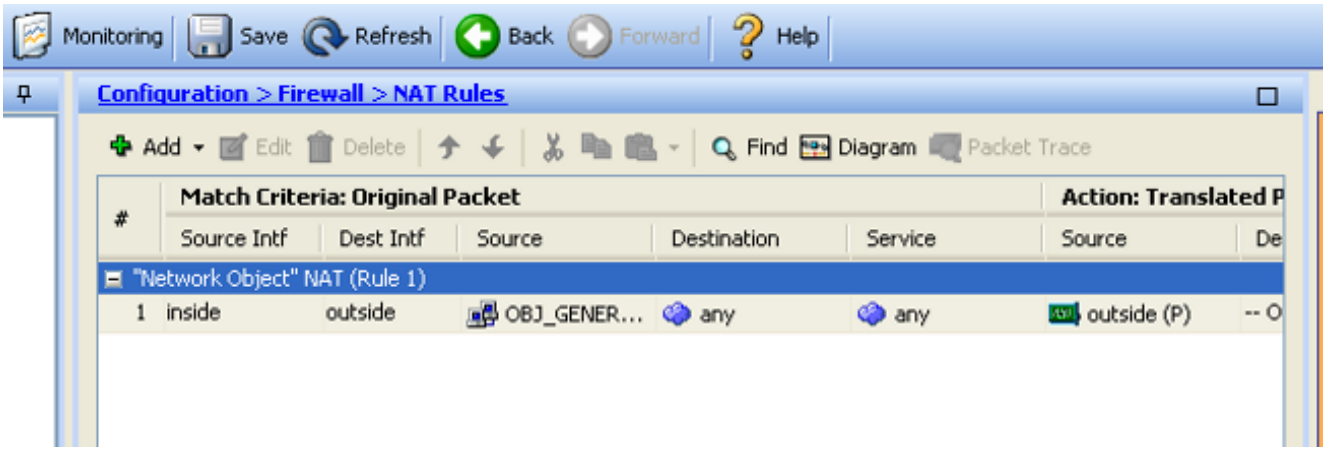
3. 按一下**NAT**，選中**Add Automatic Address Translation** Rule覈取方塊，輸入**Dynamic**，並設定**Translated Addr**選項，使其反映外部介面。如果按一下省略號按鈕，將幫助您選取預配置的對象，例如外部介面：



4. 按一下**Advanced**以選擇來源介面和目的地介面：



5. 按一下「OK」，然後按一下「Apply」以應用變更。完成後，自適應安全裝置管理器(ASDM)顯示NAT規則：



路由器B配置

以下是路由器B的組態：

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

驗證

透過Web瀏覽器透過HTTP存取網站，以驗證您的組態是否正常運作。

此示例使用託管於IP地址*198.51.100.100*的站點。如果連線成功，則在ASA CLI上可以看到以下部分中提供的輸出。

連線

輸入**show connection address** 命令以驗證連線：

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937,
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某個連線匹配。與先前存在的連線相匹配的流量允許通過防火牆，而無需被介面訪問控制清單(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。

附註：有關連線標誌的詳細資訊，請參閱ASA TCP連線標誌(連線建立和拆除)思科文檔。

疑難排解

使用本節所述的資訊來疑難排解組態問題。

系統日誌

輸入**show log**命令以檢視系統日誌：

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

Apr 27 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:192.168.1.5/58799 (203.0.113.2/58799)
```

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*看到的兩個系統日誌。

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的日誌消息；具體而言，就是動態TCP轉換(PAT)。 當流量從內部介面穿越到外部介面時，它指示源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，它會記錄拒絕連線的原因或有關禁止建立連線的因素的指示。

封包追蹤器

輸入以下命令以啟用Packet Tracer功能：

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80
```

```
--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

ASA上的Packet Tracer功能允許您指定*模擬*資料包，並檢視防火牆處理流量時完成的所有各種步驟、檢查和功能。使用此工具，識別您認為應該允許通過防火牆的流量示例*並使用*該5元組來模擬流量會非常有用。在上一個示例中，使用Packet Tracer模擬符合以下條件的連線嘗試：

- 模擬資料包到達內部介面。
- 使用的協定是TCP。
- 模擬客戶端IP地址為192.168.1.5。
- 使用者端會傳送源自連線埠1234的流量。
- 流量將發往IP地址為198.51.100.100的伺服器。
- 流量將傳至連線埠80。

請注意，命令中並未提及外部介面。這是由於Packet Tracer設計。該工具將告訴您防火牆如何處理該型別的連線嘗試，包括它將如何路由它以及從哪個介面發出。

> **提示：**有關Packet Tracer功能的詳細資訊，請參閱*使用CLI 8.4和8.6的Cisco ASA 5500系列配置指南*的使用Packet Tracer跟蹤資料包部分。

CAPTURE

輸入以下命令以應用捕獲：

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

3 packets captured

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768

ASA#show capture capout

3 packets captured
```

```
1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

ASA防火牆可以捕獲進入或離開其介面的流量。此捕獲功能非常棒，因為它可以明確證明流量是到達防火牆還是離開防火牆。上例顯示了分別在內外部介面上配置兩個名為**capin**和**capout**的捕獲。**capture**命令使用**match**關鍵字，允許您指定要捕獲的流量。

在 *capin*擷取範例中，表示您要與在*tcp主機192.168.1.5主機198.51.100.100*上看到的內部介面（輸入或輸出）上看到的流量相符。換句話說，您要擷取從主機*192.168.1.5*傳送到主機*198.51.100.100的任何TCP流量，或反之亦然*。使用**match**關鍵字允許防火牆雙向捕獲該流量。為外部介面定義的**capture**命令不引用內部客戶端IP地址，因為防火牆在該客戶端IP地址上執行PAT。因此，您無法與該客戶端IP地址匹配。相反，此範例使用**any**來表示所有可能的IP位址均與該條件相符。

配置捕獲後，您可以嘗試再次建立連線，並繼續使用**show capture<capture_name>**命令檢視捕獲。在此範例中，您可以看到使用者端能夠連線到伺服器，如擷取中看到的TCP 3次交握所示。

相關資訊

- **思科調適型資安裝置管理員**
- **Cisco ASA 5500-X系列下一代防火牆**
- **要求建議(RFC)**
- **Cisco ASA系列CLI配置指南，9.0配置ââ靜â和預設路由**
- **技術支援與檔案 ââ â Cisco Systems**