ASA 9.(x)版使用網際網路連線三個內部網路的配置示例

目錄

簡介

本文提供有關如何設定思科自適應安全裝置(ASA)版本9.1(5)以與三個內部網路配合使用的資訊。為簡單起見，路由器上使用靜態路由。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據思科調適型安全裝置(ASA)版本9.1(5)。

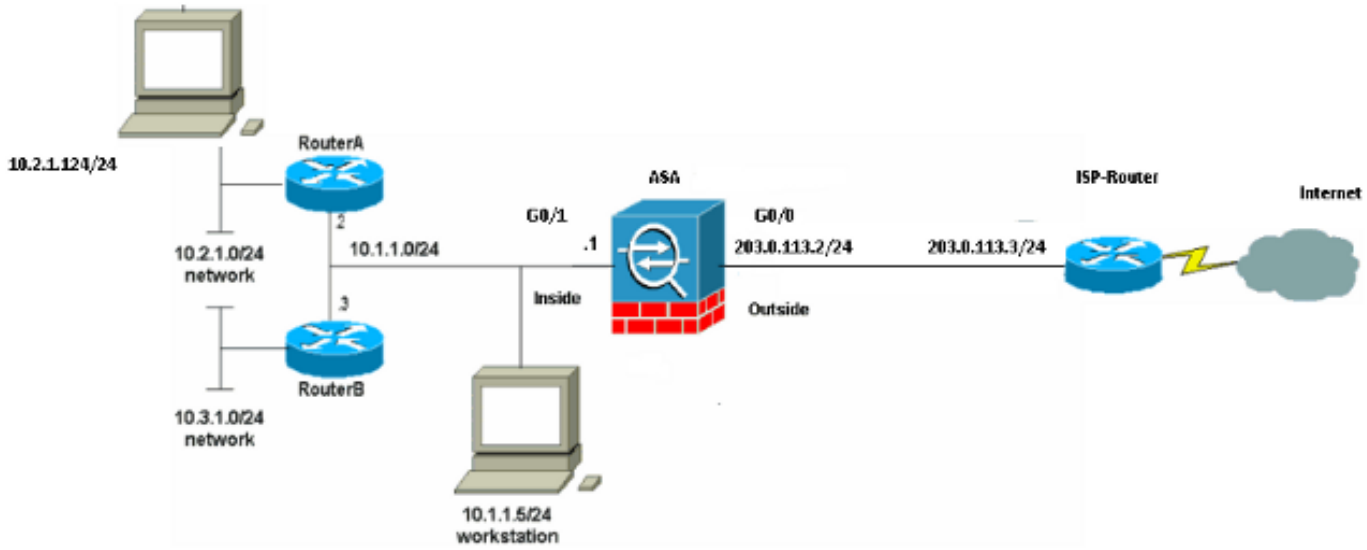
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

本節提供用於設定本文件中所述功能的資訊。

附註：使用命令查詢工具(僅供已註冊客戶使用)可獲取本節中使用的命令的更多資訊。

網路圖表



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RFC 1918 address，已在實驗室環境中使用。

ASA 9.1配置

本檔案會使用這些設定。如果您的Cisco裝置具有**write terminal**命令的輸出，可以使用Output Interpreter(僅限註冊客戶)顯示潛在問題和修正程式。

組態

- 路由器A配置
- 路由器B配置
- ASA版本9.1及更高版本配置

路由器A配置

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!
boot-start-marker
boot-end-marker
!
```

```
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
```

```
line vty 0 4
password ww
login
!
!
end

RouterA#
```

路由器B配置

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
```

```
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

ASA版本9.1及更高版本配置

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa915-k8.bin

ftp mode passive
```

```
!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get PAT to the outside interface IP
!--- on the ASA (or 10.165.200.226) for internet bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用輸出直譯器工具來檢視**show**命令輸出的分析。

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的站點。如果連線成功，則可在ASA CLI上看到此輸出。

連線

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
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 | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

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:10.2.1.124/18711 (203.0.113.2/18711)
```

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（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轉換

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 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:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 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NAT轉換(xlate)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。根據我們的配置，內部主機IP和埠被轉換為203.0.113.2地址。列出的標誌r i表示轉換是動態**的**並具有**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

本節提供的資訊可用於對組態進行疑難排解。

ASA提供多種工具用於排除連線故障。如果在驗證配置並檢查之前列出的輸出後，問題仍然存在，則這些工具和技巧可幫助確定連線失敗的原因。

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 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執行的所有各種步驟、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，並使用該五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**。
- 使用的協定是**TCP**。
- 模擬客戶端IP地址為**10.2.1.124**。
- 使用者端會傳送源自連線埠1234**的流量**。
- 流量將傳至IP位址為**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**outside**介面。這是通過Packet Tracer設計的。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。有關Packet Tracer的詳細資訊，請參閱使用Packet Tracer跟蹤資料包。

CAPTURE

```
ASA# capture capin interface inside match tcp host 10.2.1.124 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       10.2.1.124.18711 > 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 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 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 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 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。上一個範例顯示了在內部和外部介面上分別設定兩個擷取，分別為**capin**和**capout**。capture命令使用**match**關鍵字，允許您具體說明要捕獲的流量。

對於擷取capin，表示您想要比對在**tcp主機10.2.1.124主機198.51.100.100**的內部介面（輸入或輸出）上看到的流量。換句話說，您想要擷取從主機10.2.1.124傳送到**主機198.51.100.100**或**主機198.51.10000**的任何的TCPTCPTCP流量。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，不能將**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。

設定擷取後，您會嘗試再次建立連線，並繼續使用**show capture *<capture_name>指令檢視擷***取。在此範例中，您可以看到使用者端能夠連線到伺服器，從擷取中看到的TCP 3次交握可以清楚看到。