ASA 8.4(x)將單個內部網路連線到網際網路的配置示例

目錄

簡介

本文檔介紹如何設定版本8.4(1)的思科自適應安全裝置(ASA)以在單個內部網路中使用。

請參閱PIX/ASA:使用Internet連線單個內部網路配置示例，適用於使用版本8.2及更低版本的ASA上的相同配置。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本文檔中的資訊基於8.4(1)版的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。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

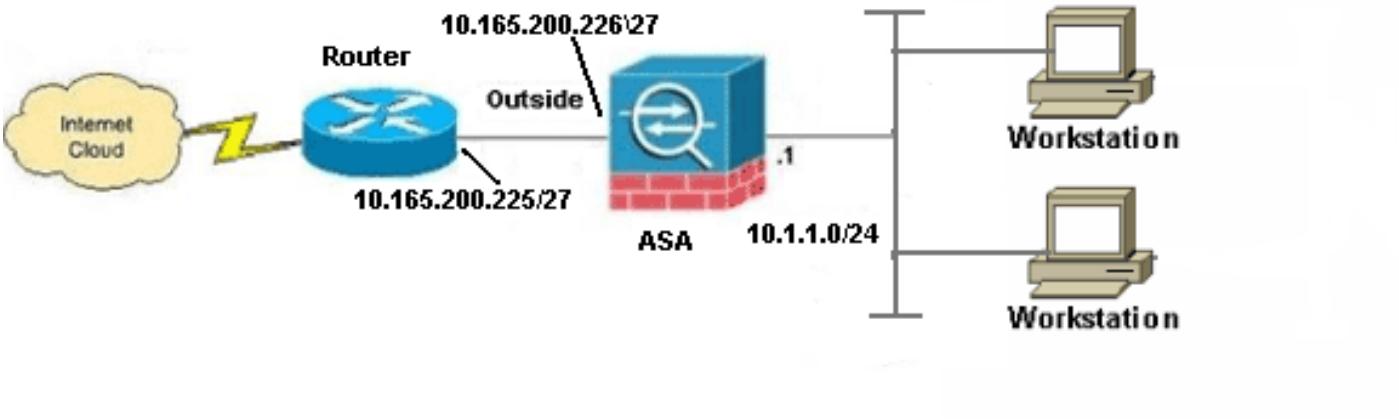
設定

本節提供用於設定本文件中所述功能的資訊。

> **附註**：若要尋找有關本檔案中所用命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



> **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位址，已在實驗室環境中使用。

ASA 8.4配置

本檔案會使用以下設定：

- 路由器配置
- ASA 8.4及更高版本配置

路由器配置

```
Building configuration...

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

```
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
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
```

ASA 8.4及更高版本配置

```
ASA#show run
: Saved
:
ASA Version 8.4(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
nameif inside
```

```
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (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
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
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
```

附註：有關ASA 8.4版上網路地址轉換(NAT)和埠地址轉換(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的站點。如果連線成功，可以在ASA CLI上看到以下輸出：

連線

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, 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***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 10.1.1.154
```

```
Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

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:10.1.1.154/58799 (10.165.200.226/58799)
```

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 10.1.1.154
3 in use, 80 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:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 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。根據我們的配置，內部主機IP和埠被轉換為10.165.200.226地址。列出的標誌r i表示轉換是動態**的**並是**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

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 10.1.1.154 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**。
- 使用的協定是**TCP**。
- 模擬客戶端IP地址為**10.1.1.154**。
- 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 10.1.1.154 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       10.1.1.154.58799 > 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 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 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，您表示想要比對在與**tcp主機10.1.1.154主機198.51.100.100**相符的內部介面（輸入或輸出）上看到的流量。換句話說，您要擷取從主機10.1.154傳送到**主機198.51.100.100**或**198.51.1000**的任何TCP流量**的的上的**上的上TCPTCP。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。

配置捕獲後，您會再次嘗試建立連線，並使用**show capture *<capture_name>*命令繼續檢視捕**獲。在此範例中，您可以看到使用者端能夠連線到伺服器，從擷取中看到的TCP 3次交握可以清楚看到。

相關資訊

- **思科調適型資安裝置管理員**
- **Cisco ASA 5500系列調適型安全裝置**
- **要求建議 (RFC)**
- **技術支援與文件 - Cisco Systems**