ASA 8.3:通過思科安全裝置建立連線並排除連線故障

目錄

簡介

最初配置思科自適應安全裝置(ASA)時，它有一個預設安全策略，內部的所有人都可以離開，外部的任何人都無法進入。如果您的站點需要不同的安全策略，您可以允許外部使用者通過ASA連線到Web伺服器。

通過Cisco ASA建立基本連線後，可以對防火牆進行配置更改。確保您對ASA所做的任何配置更改符合您的站點安全策略。

請參閱PIX/ASA:對於版本8.2及更低版本的Cisco ASA上的相同配置，通過思科安全裝置建立連線並排除連線故障。

必要條件

需求

本文檔假定在Cisco ASA上已經完成一些基本配置。有關初始ASA配置的示例，請參閱以下文檔：

- ASA 8.3(x):將單個內部網路連線到Internet
- 在思科自適應安全裝置(ASA)上配置PPPoE客戶端

採用元件

本檔案中的資訊是根據執行8.3版及更新版本的思科調適型安全裝置(ASA)。

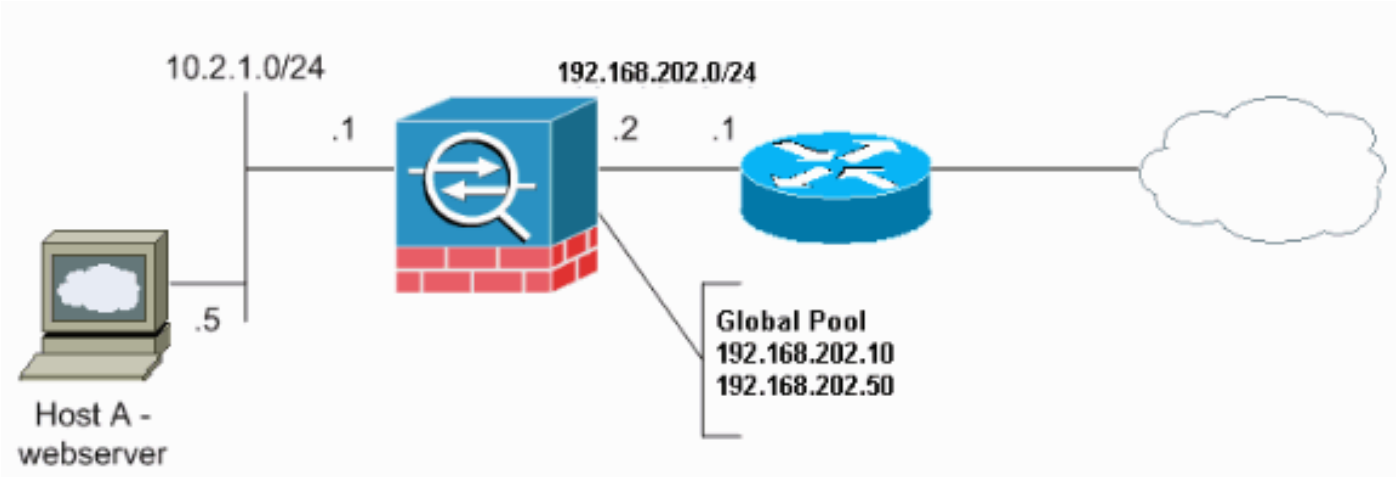
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

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。

通過ASA的連線的工作原理

在此網路中，主機A是內部地址為10.2.1.5的Web伺服器。為Web伺服器分配的外部（已轉換）地址為192.168.202.5。Internet使用者必須指向192.168.202.5才能訪問Web伺服器。Web伺服器的DNS條目必須是該地址。不允許從Internet進行其他連線。



注意：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 ，已在實驗室環境中使用。

通過Cisco ASA配置連線

完成以下步驟，以便通過ASA配置連線：

1. 建立一個網路對象，用於定義IP池範圍的內部子網和另一個網路對象。使用以下網路對象配置NAT:

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. 為Internet使用者有權訪問的內部主機分配靜態轉換地址。

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. 使用**access-list**命令允許外部使用者通過Cisco ASA。請始終在**access-list**命令中使用轉換的地址。

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

允許ARP廣播流量

安全裝置在其內部和外部介面上連線同一網路。由於防火牆不是路由躍點，因此您可以輕鬆地在現有網路中引入透明防火牆。無需重新定址IP。允許IPv4流量從較高安全介面自動通過透明防火牆到達較低安全介面，而無需訪問清單。允許位址解析通訊協定(ARP)在兩個方向上透過透明防火牆，且沒有存取清單。ARP流量可通過ARP檢查進行控制。對於從低安全性介面傳輸到高安全性介面的第3層流量，需要擴展訪問清單。

注意：透明模式安全裝置不會傳遞 Cisco Discovery Protocol(CDP)資料包或IPv6資料包，或者沒有大於或等於0x600的有效EtherType的任何資料包。例如，您無法傳遞IS-IS資料包。網橋協定資料單元(BPDU)例外，它們受支援。

允許的MAC地址

允許這些目標MAC地址通過透明防火牆。此清單中未列出的MAC地址將被丟棄：

- 真正的廣播目標MAC地址等於FFFF.FFFF.FFFF
- 從0100.5E00.0000到0100.5EFE.FFFF的IPv4組播MAC地址
- IPv6組播MAC地址從333.0000.0000到333.FFFF.FFFF
- BPDU組播地址等於0100.0CCC.CCD
- 從0900.0700.0000到0900.07FF.FFFF的Appletalk組播MAC地址

在路由器模式下不允許通過的流量

在路由器模式下，即使您在訪問清單中允許某些型別的流量，也不能通過安全裝置。但是，透明防火牆可以使用擴展訪問清單（用於IP流量）或EtherType訪問清單（用於非IP流量）允許幾乎所有流量通過。

例如，您可以通過透明防火牆建立路由協定鄰接關係。您可以根據擴充存取清單，允許開放最短路徑優先(OSPF)、路由資訊通訊協定(RIP)、增強型內部閘道路由通訊協定(EIGRP)或邊界閘道通訊協定(BGP)流量通過。同樣，熱待命路由器通訊協定(HSRP)或虛擬路由器備援通訊協定(VRRP)等通訊協定也可以通過安全裝置。

非IP流量（例如AppleTalk、IPX、BPDU和MPLS）可以配置為使用EtherType訪問清單通過。

對於透明防火牆不直接支援的功能，您可以允許流量通過，以便上游和下游路由器可以支援該功能。例如，通過使用擴展訪問清單，您可以允許動態主機配置協定(DHCP)流量（而不是不受支援的DHCP中繼功能）或組播流量（例如IP/TV建立的流量）。

排除連線故障

如果Internet使用者無法訪問您的網站，請完成以下步驟：

1. 確保已正確輸入配置地址：有效的外部地址正確內部地址外部DNS已轉換地址
2. 檢查外部介面是否存在錯誤。思科安全裝置已預配置為自動檢測介面上的速度和雙工設定。但是，存在多種可能導致自動交涉流程失敗的情況。這會導致速度或雙工不匹配（和效能問題）。 對於任務關鍵型網路基礎設施，思科會手動對每個介面的速度和雙工進行硬體編碼，因此不會出錯。這些裝置通常不會移動。因此，如果正確設定，就不需要變更它們。**範例：**

```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex full
asa(config-if)#speed 100
asa(config-if)#exit
```

   在某些情況下，對速度和雙工設定進行硬編碼會導致產生錯誤。因此，您需要將介面設定為自動偵測模式的預設設定，如以下範例所示：**範例：**

```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex auto
asa(config-if)#speed auto
asa(config-if)#exit
```

3. 如果流量不通過ASA或頭端路由器的介面傳送或接收，請嘗試清除ARP統計資訊。

```
asa#clear arp
```

4. 使用show run object和show run static命令以確保啟用靜態轉換。**範例：**

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

   在此方案中，外部IP地址用作Web伺服器的對映IP地址。

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. 檢查Web伺服器上的預設路由是否指向ASA的內部介面。
6. 使用show xlate命令檢查轉換表，以確定是否建立了轉換。
7. 使用logging buffered命令檢查日誌檔案以檢視是否發生拒絕。（查詢轉換後的地址，然後檢視是否有拒絕資訊。）
8. 使用capture命令：

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

   注意：此命令生成大量輸出。它可能導致路由器在繁重的流量負載下掛起或重新載入。
9. 如果資料包到達ASA，請確保從ASA到Web伺服器的路由正確。(檢查ASA配置中的route命令。)
10. 檢查代理ARP是否已禁用。在ASA 8.3中發出show running-config sysopt命令。這裡的sysopt noproxyarp outside指令會停用代理ARP:

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
```

```
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

若要重新啟用代理ARP，請在全域組態模式下輸入以下命令：

```
ciscoasa(config)#no sysopt noproxyarp outside
```

當主機向同一乙太網絡上的另一台裝置傳送IP流量時，該主機需要知道該裝置的MAC地址。ARP是將IP地址解析為MAC地址的第2層協定。主機傳送ARP請求並詢問「此IP地址是誰？」。 擁有IP地址的裝置會回覆，「我擁有該IP地址；這是我的MAC地址。」代理ARP允許安全裝置代表其背後的主機回覆ARP請求。它通過響應這些主機的靜態對映地址的ARP請求來完成此操作。安全裝置使用自己的MAC地址響應請求，然後將IP資料包轉發到相應的內部主機。例如，在本文檔的圖中，當對Web伺服器的全域性IP地址192.168.202.5發出ARP請求時，安全裝置會使用自己的MAC地址進行響應。如果在這種情況下未啟用代理ARP，則安全裝置外部網路中的主機無法通過發出地址192.168.202.5的ARP請求來訪問Web伺服器。有關 sysopt 命令的詳細資訊，請參閱命令參考。

11. 如果一切正常，且使用者仍無法訪問Web伺服器，請通過Cisco技術支援開啟案例。

錯誤消息 — %ASA-4-407001:

少數主機無法連線到Internet， – `%ASA-4-407001:Deny traffic for local-host interface_name:inside_address license limit of number exceeded`錯誤消息在系統日誌中接收。如何解決此錯誤？

當使用者數超過使用的許可證的使用者限制時，會收到此錯誤消息。要解決此錯誤，請將許可證升級到更多使用者。根據需要，可以是50、100或無限制使用者許可證。

相關資訊

- Cisco ASA 5500系列調適型安全裝置
- 安全產品現場通知(包括思科自適應安全裝置(ASA))
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems