ASA 8.2.X TCP狀態旁路功能配置示例

目錄

簡介

本文說明如何設定TCP狀態略過功能。此功能允許通過單獨的Cisco ASA 5500系列自適應安全裝置的出站和入站流量。

必要條件

許可證要求

Cisco ASA 5500系列自適應安全裝置應至少具有基本許可證。

採用元件

本檔案中的資訊是根據版本8.2(1)和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有關檔案慣例的資訊。

TCP狀態略過

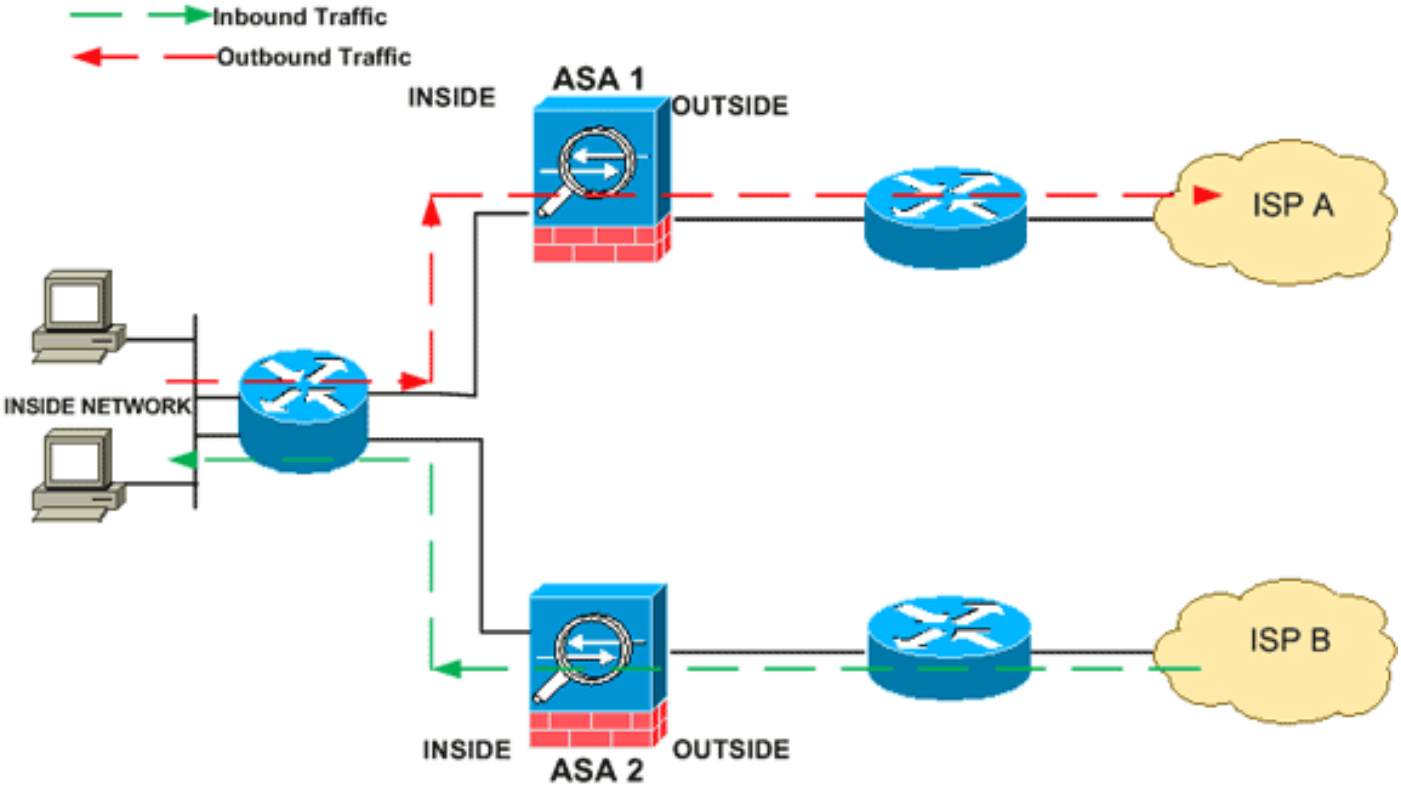
預設情況下，會使用自適應安全演算法檢查通過思科自適應安全裝置(ASA)的所有流量，並根據安全策略允許通過或丟棄這些流量。為了最大限度地提高防火牆效能，ASA會檢查每個資料包的狀態（例如，這是新連線還是已建立的連線？），並將其分配給會話管理路徑（新的連線SYN資料包）、快速路徑（已建立的連線）或控制平面路徑（高級檢查）。

與快速路徑中的現有連線匹配的TCP資料包可以通過自適應安全裝置，而無需重新檢查安全策略的各個方面。此功能可最大限度地提高效能。但是，在快速路徑中建立作業階段的方法（使用SYN封包）和在快速路徑中進行的檢查（例如TCP序號）可能會妨礙非對稱路由解決方案的方式：連線的出站和入站流都必須通過同一個ASA。

例如，新連線進入*ASA 1*。SYN資料包通過會話管理路徑，並且連線條目新增到快速路徑表中。如果此連線的後續資料包通過*ASA 1*，則這些資料包將與快速路徑中的條目匹配，並且被通過。如果後續資料包進入*ASA 2*，其中沒有經過會話管理路徑的SYN資料包，則快速路徑中沒有用於連線的條目，資料包將被丟棄。

如果在上游路由器上配置了非對稱路由，且流量在兩個ASA之間交替，則可以為特定流量配置TCP狀態旁路。TCP狀態略過會變更在快速路徑中建立作業階段的方式，並停用快速路徑檢查。此功能處理TCP流量的方式與處理UDP連線的方式相同：當與指定網路匹配的非SYN資料包進入ASA且沒有快速路徑條目時，該資料包將通過會話管理路徑在快速路徑中建立連線。進入快速路徑後，流量會繞過快速路徑檢查。

此圖提供非對稱路由的示例，其中出站流量通過與入站流量不同的ASA:



注意：Cisco ASA 5500系列自適應安全裝置上預設禁用TCP狀態旁路功能。

支援資訊

本節提供TCP狀態略過功能的支援資訊。

- Context Mode — 在單情景和多情景模式下受支援。
- 防火牆模式 — 在路由和透明模式下受支援。

- 故障轉移 — 支援故障轉移。

使用TCP狀態略過時，不支援以下功能：

- 應用檢測 — 應用檢測要求入站和出站流量通過同一個ASA，因此TCP狀態旁路不支援應用檢測。
- AAA authenticated sessions — 當使用者使用一個ASA進行身份驗證時，通過另一個ASA返回的流量將遭到拒絕，因為使用者未使用該ASA進行身份驗證。
- TCP攔截、最大初始連線限制、TCP序列號隨機化 — ASA不跟蹤連線的狀態，因此不應用這些功能。
- TCP規範化 — TCP規範器被禁用。
- SSM和SSC功能 — 不能使用TCP狀態旁路和在SSM或SSC上運行的任何應用程式，如IPS或CSC。

NAT准則:由於轉換會話是單獨為每個ASA建立的，因此請確保在兩個ASA上為TCP狀態繞過流量配置靜態NAT;如果您使用動態NAT，為*ASA 1*上的會話選擇的地址將與*ASA 2上的會話選擇的地址不*同。

設定

本節介紹如何在Cisco ASA 5500系列自適應安全裝置(ASA)上配置TCP狀態旁路功能。

TCP狀態略過功能組態

完成以下步驟，以便在Cisco ASA 5500系列自適應安全裝置上配置TCP狀態旁路功能：

1. 使用class-map class_map_name 命令建立類*對映*。類對映用於標識要為其禁用狀態防火牆檢測的流量。本示例中使用的類對映是*tcp_bypass*。
   ```
   ASA(config)#class-map tcp_bypass
   ```

2. 使用match parameter命令在類對映中指定相關流量。使用模組化策略框架時，請在類對映配置模式下使用**match access-list**命令，以便使用訪問清單來標識要應用操作的流量。以下是此組態的範例：
   ```
   ASA(config)#class-map tcp_bypass
   ASA(config-cmap)#match access-list tcp_bypass
   ```

   *tcp_bypass*是本示例中使用的訪問清單的名稱。如需指定相關流量的詳細資訊，請參閱識別流量（第3/4層類別映像）。
3. 使用policy-map name命令可新增策略對映或編輯策略對映（已經存在），策略對映設定要對已指定的類對映流量執行的操作。使用模組化策略框架時，請在全域性配置模式下使用**policy-map**命令（不帶type關鍵字），以便將操作分配給使用第3/4層類對映（class-map或class-map type management命令）標識的流量。 在本示例中，策略對映為*tcp_bypass_policy*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ```

4. 在策略對映配置模式下使用class命令，以將已建立的類對映(*tcp_bypass*)分配給策略對映(*tcp_bypass_policy*)，在該策略對映中，可以向類對映流量分配操作。在本示例中，類對映為*tcp_bypass*:
   ```
   ASA(config-cmap)#policy-map tcp_bypass_policy
   ASA(config-pmap)#class tcp_bypass
   ```

5. 在類配置模式下使用set connection advanced-options tcp-state-bypass 命令以啟用TCP狀態

略過功能。此命令在8.2(1)版中引入。 可通過策略對映配置模式訪問類配置模式，如以下示例所示：

```
ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
```

6. 使用service-policy policymap_name [global | interface *intf*] 命令在全域性配置模式下，以便在所有介面或目標介面上全域性啟用策略對映。若要停用服務原則，請使用此命令的**no**形式。使用**service-policy**命令在介面上啟用一組策略。**global**將策略對映應用於所有介面，**interface**將策略應用於一個介面。只允許一個全域性策略。可以通過將服務策略應用到介面來覆蓋該介面上的全域性策略。您只能對每個介面應用一個策略對映。

```
ASA(config-pmap-c)#service-policy tcp_bypass_policy outside
```

以下是TCP狀態略過的一個組態範例：

```
!--- Configure the access list to specify the TCP traffic !--- that needs to by-pass inspection
to improve the performance. ASA(config)#access-list tcp_bypass extended permit tcp 10.1.1.0
255.255.255.224 any

!--- Configure the class map and specify the match parameter for the !--- class map to match the
interesting traffic. ASA(config)#class-map tcp_bypass
ASA(config-cmap)#description "TCP traffic that bypasses stateful firewall"
ASA(config-cmap)#match access-list tcp_bypass

!--- Configure the policy map and specify the class map !--- inside this policy map for the
class map. ASA(config-cmap)#policy-map tcp_bypass_policy
ASA(config-pmap)#class tcp_bypass
!--- Use the set connection advanced-options tcp-state-bypass !--- command in order to enable
TCP state bypass feature.

ASA(config-pmap-c)#set connection advanced-options tcp-state-bypass
!--- Use the service-policy policymap_name [ global | interface intf ] !--- command in global
configuration mode in order to activate a policy map !--- globally on all interfaces or on a
targeted interface.

ASA(config-pmap-c)#service-policy tcp_bypass_policy outside

ASA(config-pmap-c)#static (inside,outside) 192.168.1.224 10.1.1.0 netmask
255.255.255.224
```

驗證

show conn命令顯示活動TCP和UDP連線的數量，並提供有關各種連線型別的資訊。要顯示指定連線型別的連線狀態，請在特權EXEC模式下使用show conn命令。此命令支援IPv4和IPv6地址。使用TCP狀態旁路的連線**的輸出顯**示包括標誌**b**。

疑難排解

錯誤消息

即使啟用TCP狀態旁路功能，ASA也會顯示此錯誤消息。

```
%PIX|ASA-4-313004:Denied ICMP type=icmp_type, from source_address oninterface
interface_name to dest_address:no matching session
```

由於有狀態ICMP功能新增了安全檢查，安全裝置丟棄了ICMP資料包。有狀態ICMP功能通常是未通過安全裝置的有效回應請求的ICMP回應應答，或者是與安全裝置中已建立的任何TCP、UDP或ICMP會話無關的ICMP錯誤消息。

即使由於無法禁用此功能（即檢查連線表中型別3的ICMP返回條目）而啟用了TCP狀態旁路，ASA也會顯示此日誌。但TCP狀態略過功能可以正常工作。

使用以下命令可防止出現以下訊息：

```
hostname(config)#no logging message 313004
```

相關資訊

- 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