配置為DHCP伺服器的ASA不允許主機獲取IP地址

目錄

簡介

本文描述可能導致主機無法從帶DHCP的思科自適應安全裝置(ASA)獲取IP地址的特定配置問題。

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ASA軟體版本8.2.5。

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。

問題

將ASA配置為DHCP伺服器後，主機無法獲取IP地址。

ASA在兩個介面上配置為DHCP伺服器：VLAN 6（內部介面）和VLAN 10（DMZ2介面）。這些VLAN上的PC無法通過DHCP從ASA成功獲取IP地址。

- DHCP配置正確。
- ASA不會生成指示問題原因的系統日誌。

- ASA上捕獲的資料包僅顯示DHCP DISCOVER資料包的到達。ASA不使用OFFER資料包回覆。

資料包被加速安全路徑(ASP)丟棄，並且應用於ASP的捕獲表示由於「Slowpath安全檢查失敗：」而丟棄了DHCP DISCOVER資料包。

```
ASA# capture asp type asp-drop all
ASA# show capture asp

3 packets captured
1: 14:57:05.627241 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
2: 14:57:08.627286 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
3: 14:57:16.626966 802.1Q VLAN#10 P0 0.0.0.0.68 > 255.255.255.255.67:
udp 300 Drop-reason: (sp-security-failed) Slowpath security checks failed
```

解決方案

配置包含廣泛的靜態網路地址轉換(NAT)語句，該語句包含該子網上的所有IP流量。廣播DHCP DISCOVER資料包（目的地為255.255.255.255）與導致故障的此NAT語句匹配：

```
static (DMZ1,DMZ2) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
```

如果刪除配置不正確的NAT語句，則會解決此問題。

其他資訊

如果您在ASA上使用Packet Tracer實用程式來模擬進入DMZ2介面的DHCP DISCOVER資料包，則問題可以確定是由於NAT配置引起的：

```
tutera-firewall#packet-tracer input DMZ2 udp 0.0.0.0 68 255.255.255.255 67 detail
.....
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Configuration:
static (DMZ1,DMZ2) 0.0.0.0 0.0.0.0 netmask 0.0.0.0
match ip DMZ1 any DMZ2 any
static translation to 0.0.0.0
translate_hits = 0, untranslate_hits = 641
Additional Information:
NAT divert to egress interface DMZ1
Untranslate 0.0.0.0/0 to 0.0.0.0/0 using netmask 0.0.0.0
Result:
input-interface: DMZ2
input-status: up
input-line-status: up
output-interface: DMZ1
output-status: up
output-line-status: up
Action: drop
Drop-reason: (sp-security-failed) Slowpath security checks failed
```