DHCP サーバとして設定された ASA ではホストが IP アドレスを取得できない

内容

概要

このドキュメントでは、ホストが DHCP を使用して Cisco 適応型セキュリティ アプライアンス（ASA）から IP アドレスを取得できなくなる可能性がある特定の設定の問題について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、ASA ソフトウェア バージョン 8.2.5 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

問題

DHCP サーバとして設定された ASA で、ホストが IP アドレスを取得できません。

ASA は、VLAN 6 (内部インターフェイス) および VLAN 10 (DMZ2 インターフェイス) の 2 つのインターフェイスで DHCP サーバとして設定されています。これらの VLAN 上の PC は、ASA から DHCP 経由で正常に IP アドレスを取得できません。

- DHCP 設定は適切です。
- ASA で、問題の原因を示す syslog は生成されていません。
- ASA で取得されたパケット キャプチャのみが、DHCP DISCOVER パケットの到着を示しています。ASA は、OFFER パケットで応答しません。

パケットは高速セキュリティパス(ASP)によってドロップされ、ASPに適用されたキャプチャは、DHCP DISCOVERパケットが「Slowpath security checks failed:

```
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
```

解決方法

設定には、そのサブネット上のすべての IP トラフィックを含む広範な静的ネットワーク アドレス変換 (NAT) ステートメントが含まれています。ブロードキャスト DHCP DISCOVER パケット (255.255.255.255 宛て) はこの NAT ステートメントに一致し、これによって障害が発生しています。

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

不適切に設定された NAT ステートメントを削除すると、問題が解決します。

追加情報

ASA でパケット トレーサ ユーティリティを使用して、DMZ2 インターフェイスを入力する DHCP DISCOVER パケットをシミュレートすると、問題の原因が NAT 設定であると特定できます。

```
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
```