非パッタブルトラフィックのダイナミックNATの予期しない動作

内容

概要

このドキュメントでは、IOS®デバイス上の非パッタブルトラフィックに対するダイナミックネットワークアドレス変換(NAT)の予期しない動作について説明します。

問題

Pattable以外のトラフィックは、ダイナミックNATの場合、NAT変換テーブルにハーフエントリを作成します。これらのエントリは外部から内部へのトラフィックに対して機能するため、セキュリティリスクとなります。

NAT の設定

```
ip nat pool ATT_FIBER 10.10.10.1 10.10.10.6 netmask  255.255.255.248
ip nat inside source list GUEST_SUBNET pool ATT_FIBER overload
ip nat inside source list OFFICE_SUBNETS pool ATT_FIBER overload

ip access-list extended OFFICE_SUBNETS
 deny   ip 172.16.26.0 0.0.0.127 any
 permit ip 172.16.8.0 0.0.1.255 any

ip access-list extended GUEST_SUBNET
 permit ip 172.16.26.0 0.0.0.127 any
```

```
udp 10.10.10.1:49370    172.16.9.9:49370      192.168.1.1:53      192.168.1.1:53
udp 10.10.10.1:49535    172.16.9.9:49535      192.168.2.2:53    192.168.2.2:53
tcp 10.10.10.1:53133    172.16.9.9:53133      192.168.3.3:80     192.168.3.3:80
tcp 10.10.10.1:56311    172.16.9.9:56311      192.168.4.4:5816    192.168.4.4:5816
--- 10.10.10.1         172.16.9.9            ---                  ---
```

ハーフエントリは、inside -> outsideのマッピングがある場合、またはパケットがinside -> outsideから開始された場合に作成されます。

ルータがNATオーバーロード(ポートアドレス変換(PAT))に設定され、パッタブルトラフィックがルータに到達すると、このトラフィックに対してパッタブルバインドエントリが作成されます。NATテーブルのエントリは次のようになります。

```
--- 10.10.10.1        172.16.9.9           ---                  ---
```

このバインドエントリは、プールからアドレス全体を消費します。この例では、10.10.10.1はオーバーロードされたプールのアドレスです。

つまり、内部ローカルIPアドレスは、スタティックNATに似た外部グローバルIPにバインドされます。このため、現在のエントリがタイムアウトになるまで、新しい内部ローカルIPアドレスはこのグローバルIPアドレスを使用できません。このバインドに対して作成される変換はすべて、オーバーロードではなく1対1変換です。

解決方法

この問題を解決するには、ダイナミックNATでルートマップを使用できます。 ルートマップでは、NATはハーフエントリを作成せず、プールオーバーロードの代わりにインターフェイスオーバーロードを使用しません。インターフェイスのオーバーロードの場合、パッタブルでないバインディングは作成されません。