Unexpected Behaviour of Dynamic NAT with Non-Pattable Traffic

Contents

[Introduction](#)
[Problem](#)
[Solution](#)

Introduction

This document describes the unexpected behaviour of dynamic Network Address Translation (NAT) with Non-Pattable traffic on IOS® devices.

Problem

Non-Pattable traffic creates half-entries in NAT translations table in case of dynamic NAT. These entries pose as a security risk since they work for outside-to-inside traffic.

NAT Configuration:

```
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            ---                   ---
```

Half entries are created in certain cases where there is a mapping of inside -> outside or when packet is initiated from inside -> outside.

When the router is configured for NAT overload (Port Addess Translation (PAT)) and non-pattable traffic hits the router, non-pattable bind entries get created for this traffic. It leads to this kind of entry in the NAT table:

```
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            ---                   ---
```

This bind entry consumes an entire address from the pool. In this example, 10.10.10.1 is an address from an overloaded pool.

That means an inside local IP Address gets bound to the outside global IP which is similar to static NAT. Because of this, until the current entry gets timed out, new inside local IP Addresses cannot use this global IP Address. All the translation created for this bind is 1-to-1 translations instead of overload.

Solution

In order to solve this issue, you can use route-maps with dynamic NAT. With route-maps, NAT won't create half-entries or use interface overload instead of pool overload. Non-pattable bindings are not created in case of interface overload.