ASA 8.4(4): Certain Identity NAT Configuration Disallowed

Contents

Introduction

Adaptive Security Appliances (ASAs) running 8.4(4) or higher may reject certain NAT configurations and display an error message similar to this:

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

This problem can also appear when you upgrade your ASA to 8.4(4) or higher from a prior release. You may notice that some NAT commands are no longer present in the running-config of the ASA. In these instances, you should look at the console messages printed out in order to see if there are messages present in the above format.

Another effect you may notice is that traffic for certain subnets behind the ASA may cease passing through Virtual Private Network (VPN) tunnel(s) terminating on the ASA. This document describes how to resolve these issues.

Before You Begin

Requirements

These conditions need to be met in order to encounter this problem:

- ASA running version 8.4(4) or higher, or upgraded to version 8.4(4) or higher from a prior release.
- ASA configured with a standby IP address on at least one of its interfaces.
- A NAT is configured with the above interface as the mapped interface.

Components Used

The information in this document is based on this hardware and software version:

- ASAs running 8.4(4) or higher

Conventions

For more information on document conventions, refer to Cisco Technical Tips Conventions.

Problem

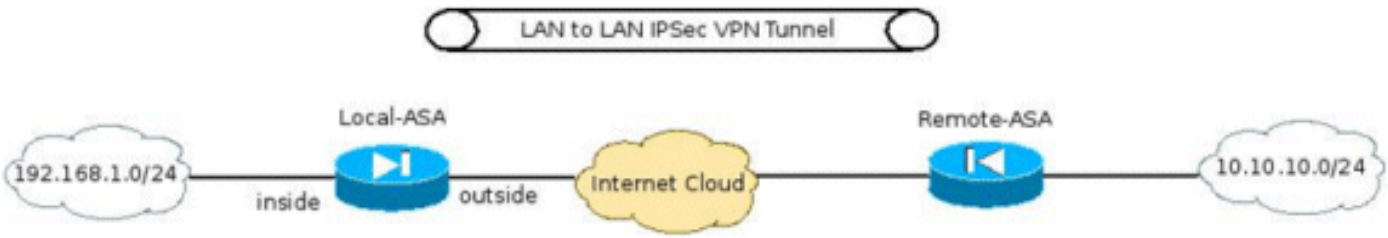
As the error message suggests, if the mapped address range in a static NAT statement includes the "standby" IP address assigned to the mapped interface, the NAT command is rejected. This behavior has always existed for Static port redirection, but it has been introduced for Static one-to-one NAT statements as well with version 8.4(4) as a fix for Cisco bug ID CSCtw82147 (registered customers only) .

This bug was filed because prior to 8.4(4) the ASA allowed users to configure the mapped address in a static NAT configuration to be the same as the standby IP address assigned to the mapped interface. For example, look at this snippet of configuration from an ASA:

```
ciscoasa(config)# show run int e0/0 ! interface Ethernet0/0 nameif vm security-level
0 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2 ciscoasa(config)# show run
nat ! object network obj-10.76.76.160 nat (tftp,vm) static 192.168.1.2
```

Even though the command is accepted, this NAT configuration will never work by design. As a result, beginning with 8.4(4), the ASA does not allow such a NAT rule to be configured in the first place.

This has resulted in another unforeseen problem. For example, consider the scenario where the user has a VPN tunnel terminating on the ASA and wants to allow the "inside" subnet to be able to talk to the remote VPN subnet.



Among other commands required for configuring the VPN tunnel, one of the more important configurations is to ensure that the traffic between the VPN subnets does not get NATed. This is implemented with 8.3 and above using a Manual/Twice NAT command of this format:

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
```

```
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

When this ASA is upgraded to 8.4(4) or higher, this NAT command will not be present in the ASA's running-config and this error will be printed on the ASA's console:

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

As a result, traffic between subnets 192.168.1.0/24 and 10.10.10.0/24 will no longer flow through the VPN tunnel.

Solution

There are two possible workarounds for this condition:

- Make the NAT command as specific as possible before upgrading to 8.4(4) so the mapped interface is not "any". For example, the above NAT command can be changed to the interface through which the Remote VPN subnet is reachable (named "outside" in the above scenario):`nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0`
- If the above workaround is not possible, complete these steps:When the ASA is running 8.4(4) or higher, remove the standby IP address assigned to the interface.Apply the NAT command.Re-apply the standby IP address on the interface.For example:`ciscoasa(config)# **interface Ethernet0/0** ciscoasa(config-if)# **ip address 192.168.1.1 255.255.255.0** ciscoasa(config-if)# **exit** ciscoasa(config)# **nat (inside,any) 1 source static obj-192.168.1.0 obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0** ciscoasa(config)# **interface Ethernet0/0** ciscoasa(config-if)# **ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2**`

Related Information

- **Technical Support & Documentation - Cisco Systems**