

Troubleshoot ASA Network Address Translation (NAT) Configuration

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Troubleshoot NAT Configuration on the ASA](#)

[How the ASA Configuration is Used to Build the NAT Policy Table](#)

[How to Troubleshoot NAT Problems](#)

[Use the Packet Tracer Utility](#)

[View the Output of the Show Nat Command](#)

[NAT Problem Troubleshooting Methodology](#)

[Common Problems with NAT Configurations](#)

[Problem: Traffic fails due to NAT Reverse Path Failure \(RPF\) Error: Asymmetric NAT rules matched for forward and reverse flows](#)

[Problem: Manual NAT Rules are out-of-order, which causes incorrect packet matches](#)

[Problem](#)

[Problem](#)

[Problem: A NAT Rule Causes the ASA to Proxy Address Resolution Protocol \(ARP\) for Traffic on the Mapped Interface](#)

Introduction

This document describes how to troubleshoot Network Address Translation (NAT) configuration on the Cisco Adaptive Security Appliance (ASA) platform.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on ASA Version 8.3 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Troubleshoot NAT Configuration on the ASA



Note: For some basic examples of NAT configurations, which include a video that shows a basic NAT configuration, see the section **Related Information** at the bottom of this document.

When you troubleshoot NAT configurations, it is important to understand how the NAT configuration on the ASA is used to build the NAT policy table.

These configuration mistakes account for the majority of the NAT problems encountered by ASA administrators:

- The NAT configuration rules are out of order. For example, a manual NAT rule is placed at the top of the NAT table, which causes more specific rules placed farther down the NAT table to never be hit.
- The network objects used in the NAT configuration are too broad, which causes traffic to inadvertently match these NAT rules, and miss more specific NAT rules.

The **packet tracer** utility can be used to diagnose most NAT-related issues on the ASA. See the next section for more information about how the NAT configuration is used to build the NAT policy table, and how to troubleshoot and resolve specific NAT problems.

Additionally, the **show nat detail** command can be used in order to understand which NAT rules are hit by new connections.

How the ASA Configuration is Used to Build the NAT Policy Table

All packets processed by the ASA are evaluated against the NAT table. This evaluation starts at the top (Section 1) and works down until a NAT rule is matched.

In general, once a NAT rule is matched, that NAT rule is applied to the connection and no more NAT policies are checked against the packet but there are some caveats explained next.

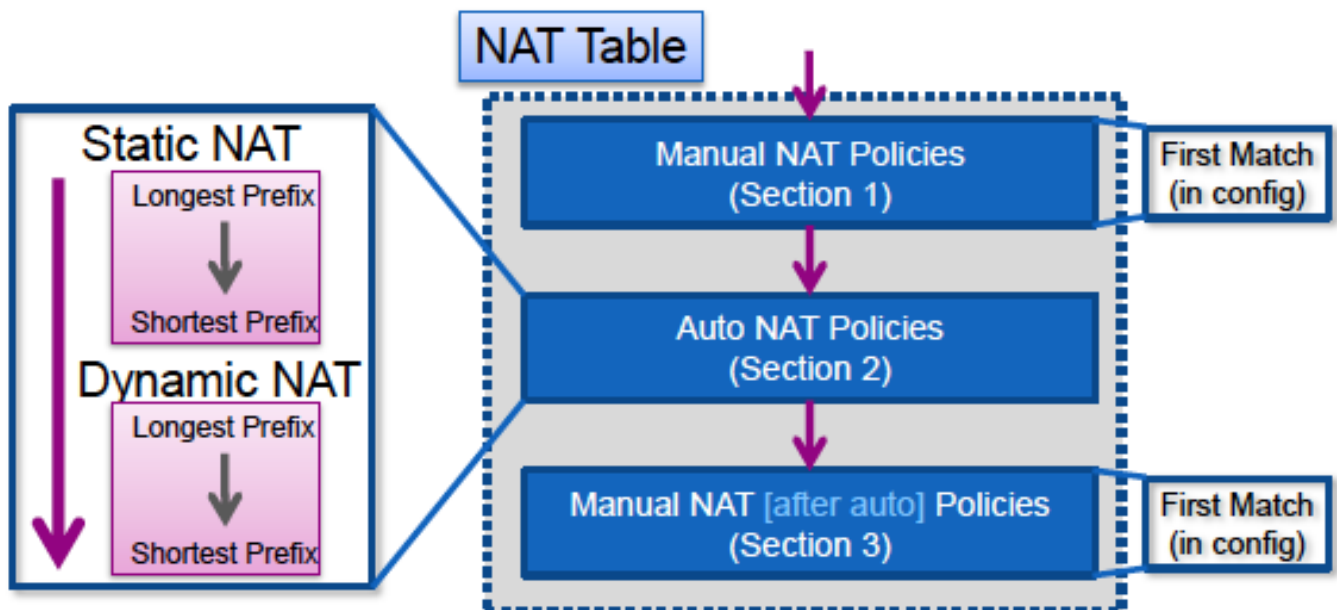
The NAT Policy Table

The NAT policy on the ASA is built from the NAT configuration.

The three sections of the ASA NAT table are:

Section 1	Manual NAT policies These are processed in the order in which they appear in the configuration.
Section 2	Auto NAT policies These are processed based on the NAT type (static or dynamic) and the prefix (subnet mask) length in the object.
Section 3	After-auto manual NAT policies These are processed in the order in which they appear in the configuration.

This diagram shows the different NAT sections and how they are ordered:



NAT Rule Match

Section 1

- A flow is first evaluated against section 1 of the NAT table that starts with the first rule.
 - If the source and destination IP of the packet match the parameters of the manual NAT rule the translation is applied and the process stops and no further NAT rules in any section are evaluated.
 - If no NAT rule is matched, the flow is then evaluated against section 2 of the NAT table.

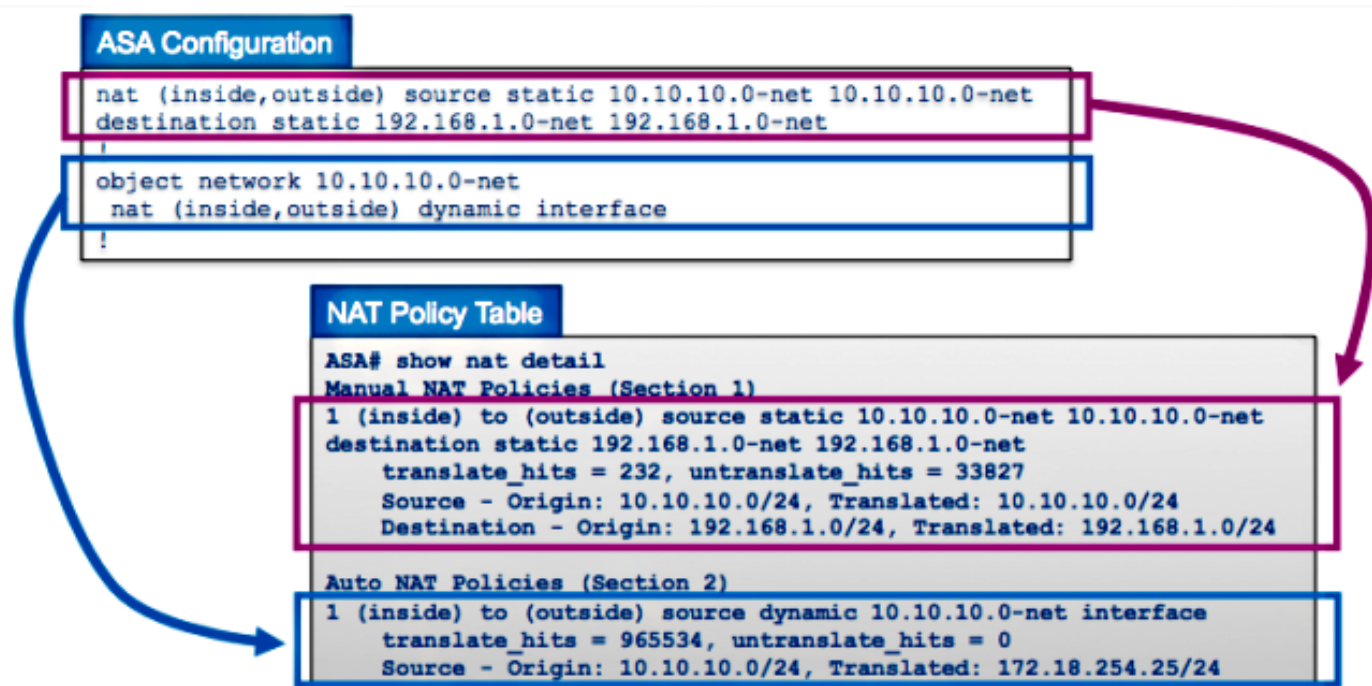
Section 2

- A flow is evaluated against the section 2 NAT rules in the order specified previously, first the static NAT rules, then the dynamic NAT rules.
 - If a translation rule matches either the source or destination IP of the flow, the translation can be applied and the rest of the rules can continue to be evaluated to see if they match the other IP in the flow. For example, one auto-NAT rule could translate the source IP and another auto-NAT rule could translate the destination.
 - If the flow matches an auto-NAT rule, when the end of section 2 is reached the NAT lookup stops, and the rules in section 3 are not evaluated.
 - If no NAT rule from section 2 is matched against the flow, the lookup proceeds to section 3

Section 3

- The process in section 3 is essentially the same as in section 1. If the source and destination IP of the packet match the parameters of the manual NAT rule the translation is applied and the process stops and no further NAT rules in any section are evaluated.

This example shows how the ASA NAT configuration with two rules (one Manual NAT statement and one Auto NAT configuration) are represented in the NAT table:



How to Troubleshoot NAT Problems

Use the Packet Tracer Utility

In order to troubleshoot problems with NAT configurations, use the **packet tracer** utility in order to verify that a packet hits the NAT policy. Packet tracer allows you to specify a sample packet that enters the ASA, and the ASA indicates what configuration applies to the packet and if it is permitted or not.

In the next example, a sample TCP packet that enters the inside interface and is destined to a host on the Internet is given. The packet tracer utility shows that the packet matches a dynamic NAT rule and is translated to the outside IP address of **172.16.123.4**:

ASA#

```
packet-tracer input inside tcp 10.10.10.123 12345 192.168.200.123 80
```

...(output omitted)...

```
Phase: 2  
Type: NAT  
Subtype:  
Result: ALLOW  
Config:
```

```
object network 10.10.10.0-net  
  nat (inside,outside) dynamic interface
```

```
Additional Information:  
Dynamic translate 10.10.10.123/12345 to 172.16.123.4/12345
```

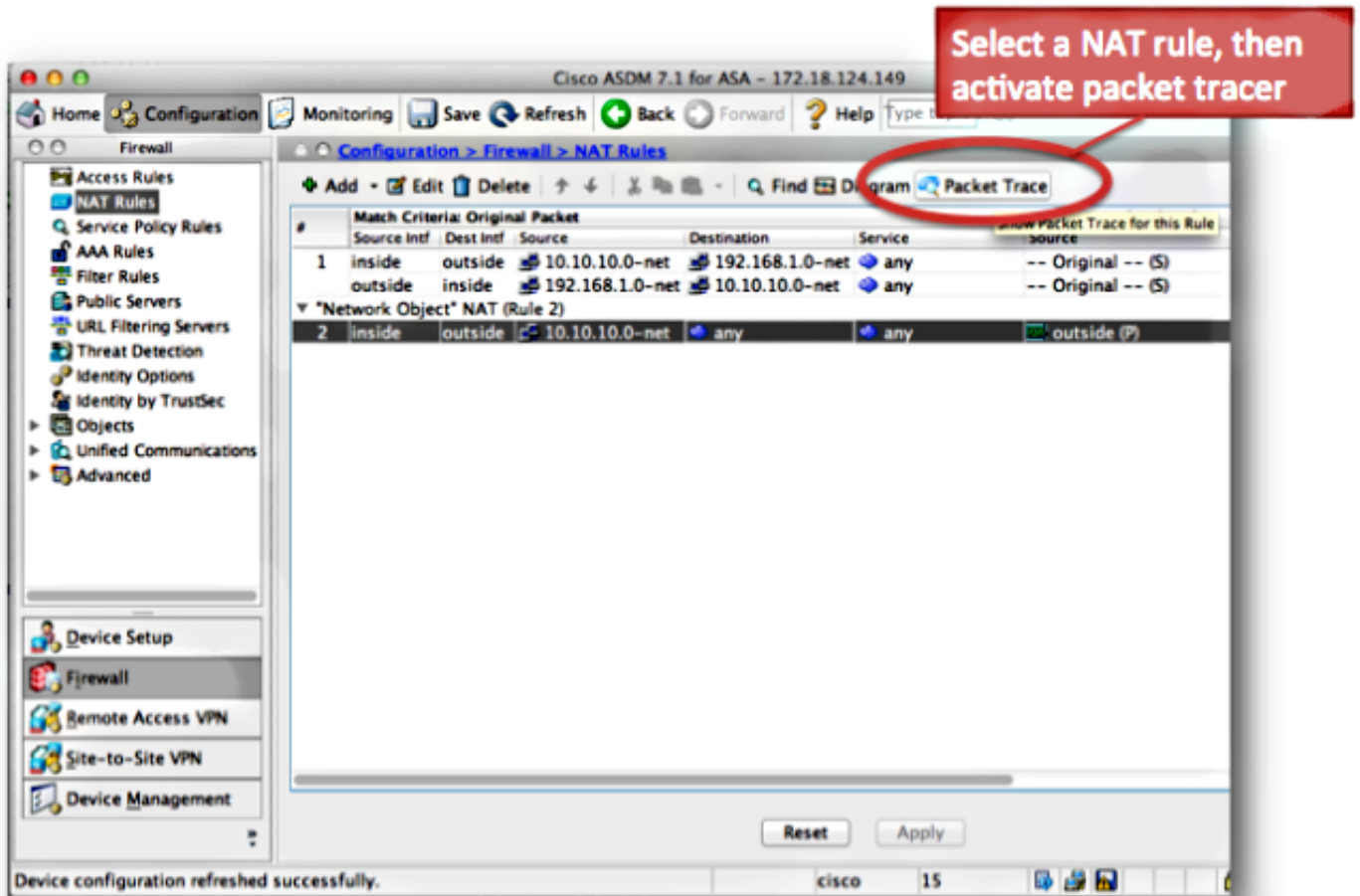
...(output omitted)...

```
Result:  
input-interface: inside  
input-status: up  
input-line-status: up  
output-interface: outside  
output-status: up  
output-line-status: up
```

```
Action: allow
```

ASA#

Choose the **NAT rule** and click **Packet Trace** in order to activate the packet tracer from the Cisco Adaptive Security Device Manager (ASDM). This uses the IP addresses specified in the NAT rule as the inputs for the packet tracer tool:



View the Output of the Show Nat Command

The output of the **show nat detail** command can be used in order to view the NAT policy table. Specifically, the **translate_hits** and **untranslate_hits** counters can be used in order to determine which NAT entries are used on the ASA.

If you see that your new NAT rule has no **translate_hits** or **untranslate_hits**, that means that either the traffic does not arrive at the ASA, or perhaps a different rule that has a higher priority in the NAT table matches the traffic.

Here is the NAT configuration and the NAT policy table from a different ASA configuration:

```

ASA# show run nat
nat (inside,outside) source dynamic Users1 NATPool1
nat (inside,outside) source static ServerReal ServerTrans
!
object network Users2
 nat (inside,outside) dynamic NATPool2
object network SecureServ
 nat (inside,outside) static 203.0.113.82
!
nat (inside,outside) after-auto source dynamic Users3 NATPool3
nat (inside,outside) after-auto source static Servers ServersTrans

```

```

ASA# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic Users1 NATPool1
  translate_hits = 3321, untranslate_hits = 0
2 (inside) to (outside) source static ServerReal ServerTrans
  translate_hits = 0, untranslate_hits = 93829

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static SecureServ 203.0.113.82
  translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic Users2 NATPool2
  translate_hits = 0, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic Users3 NATPool3
  translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source static Servers ServersTrans
  translate_hits = 0, untranslate_hits = 0

```

NAT line hit counts increment when new connections match NAT rule

In the previous example, there are six NAT rules configured on this ASA. The **show nat** output shows how these rules are used to build the NAT policy table, as well as the number of **translate_hits** and **untranslate_hits** for each rule.

These hit counters increment only once per connection. After the connection is built through the ASA, subsequent packets that match that current connection do not increment the NAT lines (much like the way access-list hit counts work on the ASA).

Translate_hits: The number of new connections that match the NAT rule in the forward direction.

"Forward direction" means that the connection was built through the ASA in the direction of the interfaces specified in the NAT rule.

If a NAT rule specified that the inside server is translated to the outside interface, the order of the interfaces in the NAT rule is "nat (inside,outside)..."; if that server initiates a new connection to a host on the outside, the **translate_hit** counter increments.

Untranslate_hits: The number of new connections that match the NAT rule in the reverse direction.

If a NAT rule specifies that the inside server is translated to the outside interface, the order of the interfaces in the NAT rule is "nat (inside,outside)..."; if a client on the outside of the ASA initiates a new connection to the server on the inside, the **untranslate_hit** counter increments.

Again, if you see that your new NAT rule has no **translate_hits** or **untranslate_hits**, that means that either the traffic does not arrive at the ASA, or perhaps a different rule that has a higher priority in the NAT table matches the traffic.

NAT Problem Troubleshooting Methodology

Use packet tracer in order to confirm that a sample packet matches the proper NAT configuration rule on the ASA. Use the **show nat detail** command in order to understand which NAT policy rules are hit. If a connection matches a different NAT configuration than expected, troubleshoot with these questions:

- Is there a different NAT rule that takes precedence over the NAT rule you intended the traffic to hit?
- Is there a different NAT rule with object definitions that are too broad (the subnet mask is too short, such as 255.0.0.0) which causes this traffic to match the wrong rule?
- Are the manual NAT policies out-of-order, which causes the packet to match the wrong rule?
- Is your NAT rule incorrectly configured, which causes the rule to not match your traffic?

See the next section for sample problems and solutions.

Common Problems with NAT Configurations

Here are some common problems experienced when you configure NAT on the ASA.

Problem: Traffic fails due to NAT Reverse Path Failure (RPF) Error: Asymmetric NAT rules matched for forward and reverse flows

The NAT RPF check ensures that a connection that is translated by the ASA in the forward direction, such as the TCP synchronize (SYN), is translated by the same NAT rule in the reverse direction, such as the TCP SYN/acknowledge (ACK).

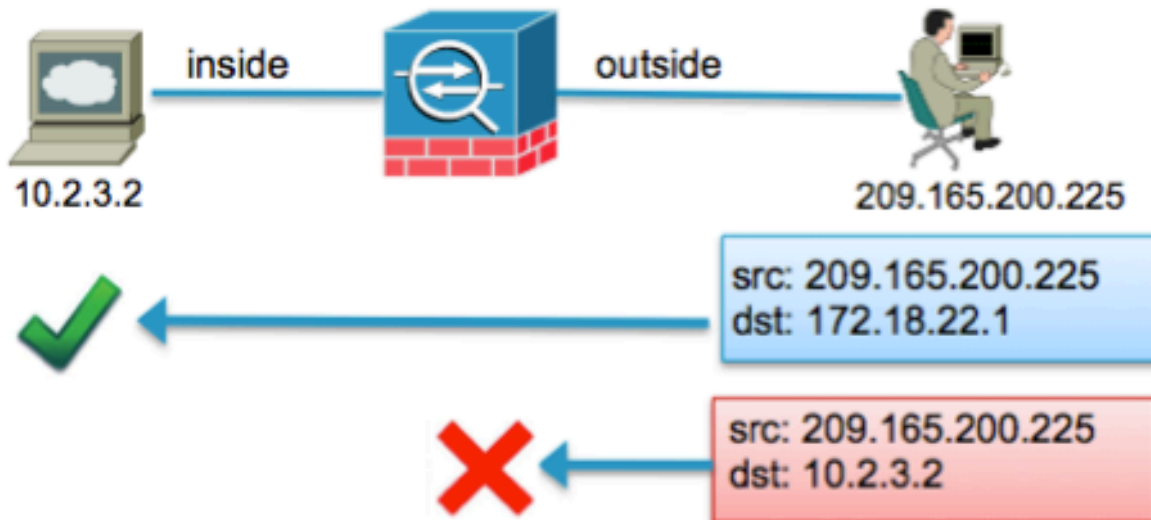
Most commonly, this problem is caused by inbound connections destined to the local (untranslated) address in a NAT statement. At a basic level, the NAT RPF verifies that the reverse connection from the server to the client matches the same NAT rule; if it does not, the NAT RPF check fails.

Example: 209.165.200.225


```

object network inside-server
 host 10.2.3.2
!
object network inside-server
 nat (inside,outside) static 172.18.22.1

```



When the outside host at **192.168.200.225** sends a packet destined directly to the local (untranslated) IP address of **10.2.3.2**, the ASA drops the packet and logs this syslog:

```

%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse flows;
Connection for icmp src outside:192.168.200.225 dst inside:10.2.3.2 (type 8, code 0)
denied due to NAT reverse path failure

```

Solution:

First, ensure that the host sends data to the correct global NAT address. If the host sends packets destined to the correct address, check the NAT rules that are hit by the connection.

Verify that the NAT rules are correctly defined, and that the objects referenced in the NAT rules are correct. Also verify that the order of the NAT rules is appropriate.

Use the packet tracer utility in order to specify the details of the denied packet. Packet tracer must show the dropped packet due to the RPF check failure.

Next, look at the output of packet tracer in order to see which NAT rules are hit in the NAT phase and the NAT-RPF phase.

If a packet matches a NAT rule in the NAT RPF-check phase, which indicates that the reverse flow would hit a NAT translation, but does not match a rule in the NAT phase, which indicates that the forward flow

would NOT hit a NAT rule, the packet is dropped.

This output matches the scenario shown in the previous diagram, where the outside host incorrectly sends traffic to the local IP address of the server and not the global (translated) IP address:

```
<#root>
ASA#
packet-tracer input outside tcp 192.168.200.225 1234 10.2.3.2 80

.....

Phase: 8
Type: NAT
Subtype: rpf-check
Result:

DROP

Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...
ASA(config)#
```

When the packet is destined to the correct mapped IP address of **172.18.22.1**, the packet matches the correct NAT rule in the UN-NAT phase in the forward direction, and the same rule in the NAT RPF-check phase:

```
<#root>
ASA(config)#
packet-tracer input outside tcp 192.168.200.225 1234 172.18.22.1 80

...
Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
NAT divert to egress interface inside
Untranslate 172.18.22.1/80 to 10.2.3.2/80
...
Phase: 8
Type: NAT
Subtype: rpf-check
Result:

ALLOW
```

```

Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#

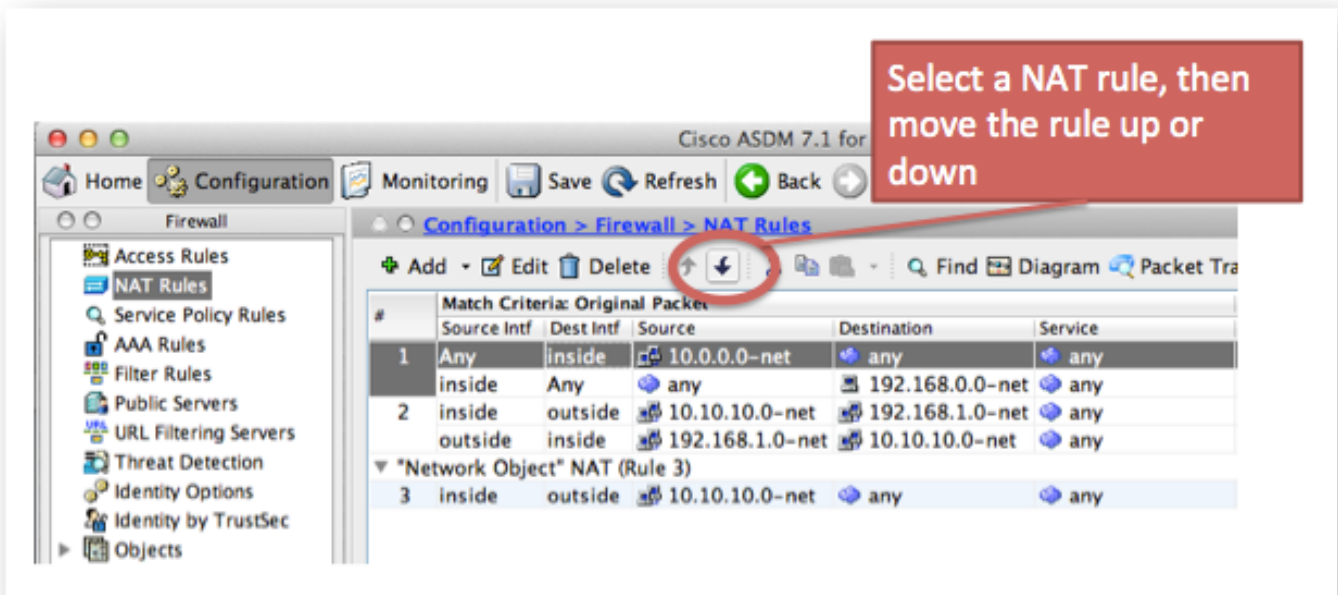
```

Problem: Manual NAT Rules are out-of-order, which causes incorrect packet matches

The manual NAT rules are processed based on their appearance in the configuration. If a very broad NAT rule is listed first in the configuration, it can override another, more specific rule farther down in the NAT table. Use packet tracer in order to verify which NAT rule your traffic hits; it can be necessary to rearrange the manual NAT entries to a different order.

Solution:

Reorder NAT rules with ASDM.



Solution:

NAT rules can be reordered with the CLI if you remove the rule and reinsert it at a specific line number. In order to insert a new rule at a specific line, enter the line number just after the interfaces are specified.

Example:

```

<#root>
ASA(config)#
nat (inside,outside) 1 source static 10.10.10.0-net
10.10.10.0-net destination static 192.168.1.0-net 192.168.1.0-net

```

Problem

A NAT rule is too broad and matches some traffic inadvertently. Sometimes NAT rules are created that use objects that are too broad. If these rules are placed near the top of the NAT table (at the top of Section 1, for example), they can match more traffic than intended and cause NAT rules farther down the table to never be hit.

Solution

Use packet tracer in order to determine if your traffic matches a rule with object definitions that are too broad. If this is the case, you must reduce the scope of those objects, or move the rules farther down the NAT table, or to the after-auto section (Section 3) of the NAT table.

Problem

A NAT rule diverts traffic to an incorrect interface. NAT rules can take precedence over the routing table when they determine which interface a packet egresses the ASA. If an inbound packet matches a translated IP address in a NAT statement, the NAT rule is used in order to determine the egress interface.

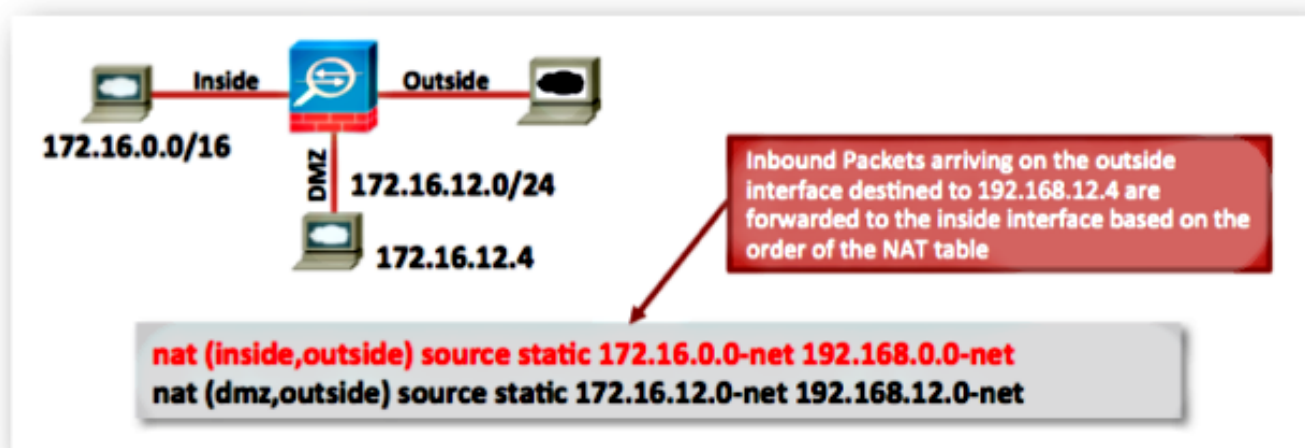
The NAT divert check (which is what can override the routing table) checks to see if there is any NAT rule that specifies destination address translation for an inbound packet that arrives on an interface.

If there is no rule that explicitly specifies how to translate that packet destination IP address, then the global routing table is consulted to determine the egress interface.

If there is a rule that explicitly specifies how to translate the packet destination IP address, then the NAT rule pulls the packet to the other interface in the translation and the global routing table is effectively bypassed.

This problem is most often seen for inbound traffic, which arrives on the outside interface, and is usually due to out-of-order NAT rules that divert traffic to unintended interfaces.

Example:



Solutions:

This problem can be resolved with either of these actions:

- Reorder the NAT table so that the more specific entry is listed first.


- Use non-overlapping global IP address ranges for the NAT statements.

Note that if the NAT rule is an identity rule, (which means that the IP addresses are not changed by the rule) then the **route-lookup** keyword can be used (this keyword is not applicable to the previous example since the NAT rule is not an identity rule).

The **route-lookup** keyword causes the ASA to perform an extra check when it matches a NAT rule. It checks that the routing table of the ASA forwards the packet to the same egress interface to which this NAT configuration diverts the packet.

If the routing table egress interface does not match the NAT divert interface, the NAT rule is not matched (the rule is skipped) and the packet continues down the NAT table to be processed by a later NAT rule.

The **route-lookup** option is only available if the NAT rule is an identity NAT rule, which means that the IP addresses are not changed by the rule. The **route-lookup** option can be enabled per NAT rule if you add route-lookup to the end of the NAT line, or if you check the Lookup route table to locate egress interface check box in the NAT rule configuration in ASDM:

 **Lookup route table to locate egress interface**

Problem: A NAT Rule Causes the ASA to Proxy Address Resolution Protocol (ARP) for Traffic on the Mapped Interface

The ASA Proxy ARPs for the global IP address range in a NAT statement on the global interface. This Proxy ARP functionality can be disabled on a per-NAT rule basis if you add the **no-proxy-arp** keyword to the NAT statement.

This problem is also seen when the global address subnet is inadvertently created to be much larger than it was intended to be.

Solution

Add the **no-proxy-arp** keyword to the NAT line if possible.

Example:

```
<#root>
ASA(config)#
object network inside-server

ASA(config-network-object)#
nat (inside,outside) static 172.18.22.1 no-proxy-arp

ASA(config-network-object)#
```

end

ASA#

ASA#

```
show run nat
```

```
object network inside-server
```

```
  nat (inside,outside) static 172.18.22.1
```

```
no-proxy-arp
```

ASA#

This can also be accomplished with ASDM. Within the NAT rule, check the **Disable Proxy ARP on egress interface** check box.

A screenshot of a configuration window in ASDM. On the left, there is a small square checkbox with a blue checkmark inside. To the right of the checkbox, the text "Disable Proxy ARP on egress interface" is displayed in a blue, sans-serif font.

Related Information

- [VIDEO: ASA port forwarding for DMZ server access \(versions 8.3 and 8.4\)](#)
- [Basic ASA NAT Configuration: Webserver in the DMZ in ASA Version 8.3 and later](#)
- [Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.1](#)
- [Cisco Technical Support & Downloads](#)