排除ASA网络地址转换(NAT)配置故障

目录

简介

本文档介绍如何对思科自适应安全设备(ASA)平台上的网络地址转换(NAT)配置进行故障排除。

先决条件

要求

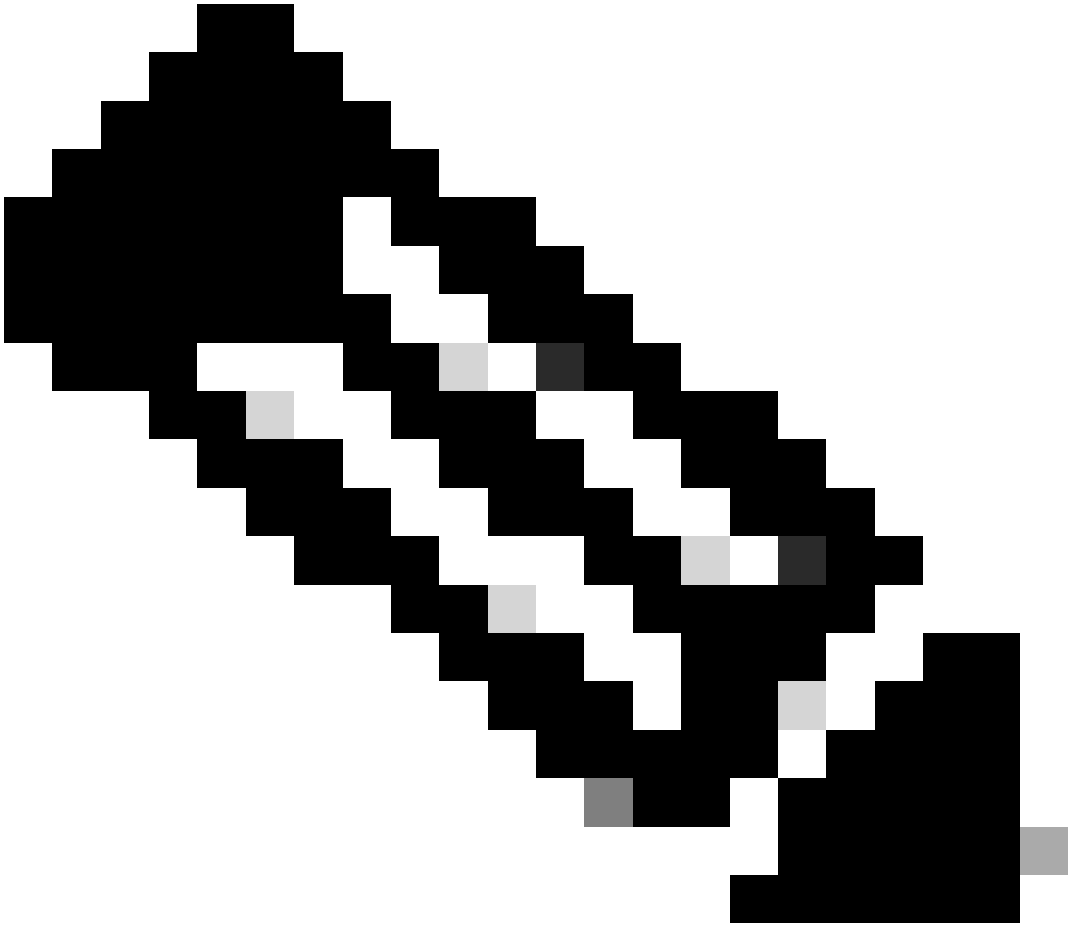
本文档没有任何特定的要求。

使用的组件

本文档中的信息基于ASA版本8.3及更高版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

排除ASA上的NAT配置故障



注意：有关NAT配置的一些基本示例（包括显示基本NAT配置的视频），请参阅本文档底部的相关信息部分。

当您排除NAT配置故障时，必须了解如何使用ASA上的NAT配置来构建NAT策略表。

这些配置错误是ASA管理员遇到的大多数NAT问题的原因：

- NAT配置规则顺序混乱。例如，手动NAT规则放置在NAT表的顶部，这样会导致放置在NAT表下方的更具体的规则永远不会被命中。
- NAT配置中使用的网络对象过于宽泛，导致流量无意间与这些NAT规则相匹配，并且缺少更具体的NAT规则。

Packet tracer实用程序可用于诊断ASA上大多数与NAT相关的问题。请参阅下一部分，了解有关如何使用NAT配置来构建NAT策略表，以及如何排除和解决特定NAT问题的详细信息。

此外，还可以使用show nat detail命令来了解新连接影响哪些NAT规则。

如何使用ASA配置构建NAT策略表

根据NAT表评估ASA处理的所有数据包。此评估从顶部（第1部分）开始，向下进行，直到匹配NAT规则。

通常，一旦NAT规则匹配，该NAT规则将应用于连接，并且不再针对数据包检查更多NAT策略，但有一些警告将在后面说明。

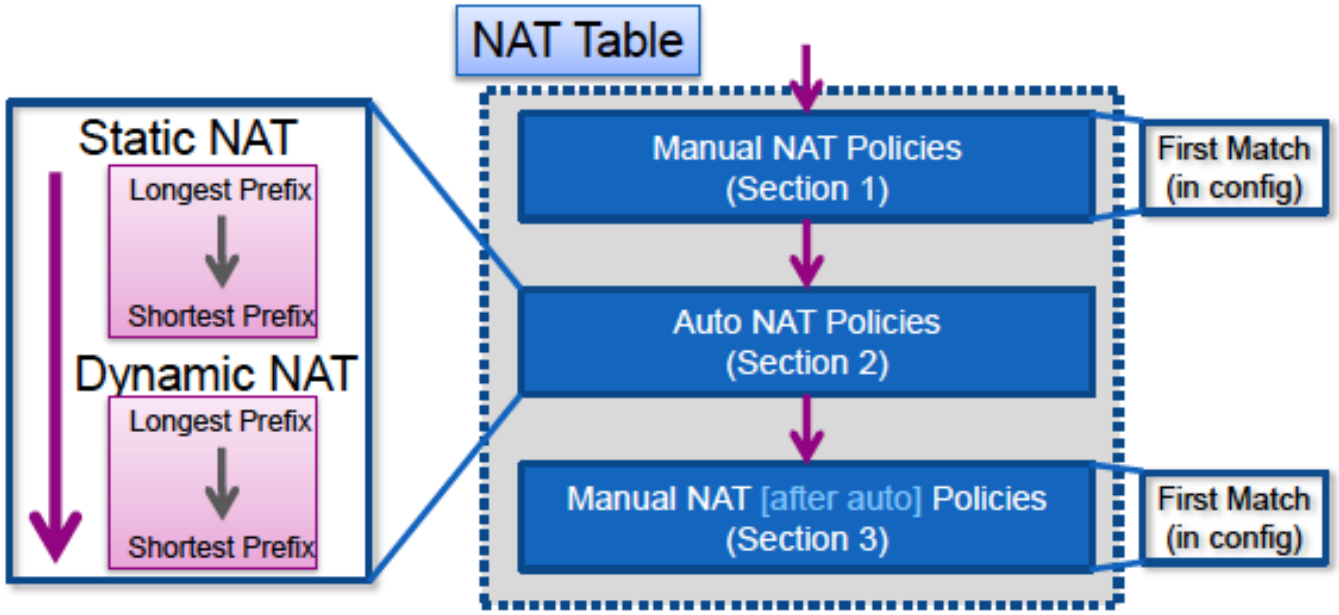
NAT策略表

ASA上的NAT策略根据NAT配置构建。

ASA NAT表的三个部分是：

第 1 部分	手动NAT策略 它们按照它们在配置中出现的顺序进行处理。
第 2 部分	自动NAT策略 根据对象中的NAT类型（静态或动态）和前缀（子网掩码）长度处理这些值。
第 3 部分	自动后手动NAT策略 它们按照它们在配置中出现的顺序进行处理。

下图显示了不同的NAT部分及其排序方式：



NAT规则匹配

第 1 部分

- 首先根据以第一条规则开头的NAT表第1部分评估流量。
  - 如果数据包的源IP和目标IP与手动NAT规则的参数匹配，则应用转换并停止进程，不评估任何部分中的其他NAT规则。
  - 如果未匹配NAT规则，则根据NAT表的第2部分评估流量。

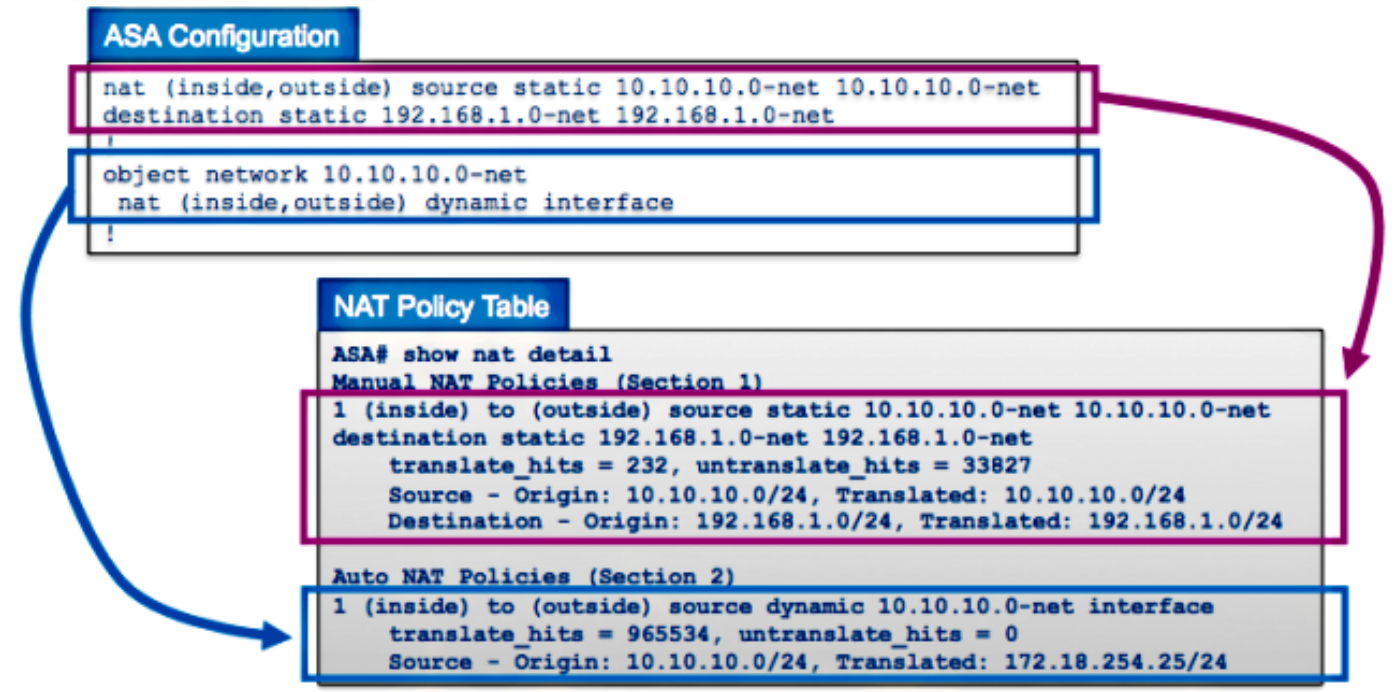
第 2 部分

- 系统会根据第二部分NAT规则按之前指定的顺序评估流量，首先评估静态NAT规则，然后评估动态NAT规则。
  - 如果转换规则与流的源IP或目标IP匹配，则可以应用转换，并继续评估其余规则，以查看它们是否与流中的其他IP匹配。例如，一个自动NAT规则可以转换源IP，另一个自动NAT规则可以转换目标。
  - 如果流与自动NAT规则匹配，则当到达第2部分的末尾时，NAT查找停止，且不评估第3部分的规则。
  - 如果第2部分的NAT规则与流不匹配，查找将进入第3部分

第 3 部分

- 第3部分中的过程与第1部分中的过程基本相同。 如果数据包的源IP和目标IP与手动NAT规则的参数匹配，则应用转换并停止进程，不评估任何部分中的其他NAT规则。

本示例展示了如何使用两条规则（一条手动NAT语句和一个自动NAT配置）在NAT表中表示ASA NAT配置：



如何排除NAT故障

使用Packet Tracer实用程序

要对NAT配置问题进行故障排除，请使用Packet Tracer实用程序验证数据包是否符合NAT策略。Packet tracer允许您指定进入ASA的数据包示例，ASA指示什么配置适用于该数据包以及是否允许该配置。

在下一个示例中，给出了一个进入内部接口并发往Internet上的主机的示例TCP数据包。Packet Tracer实用程序显示，数据包与动态NAT规则匹配，并被转换为外部IP地址172.16.123.4：

<#root>

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

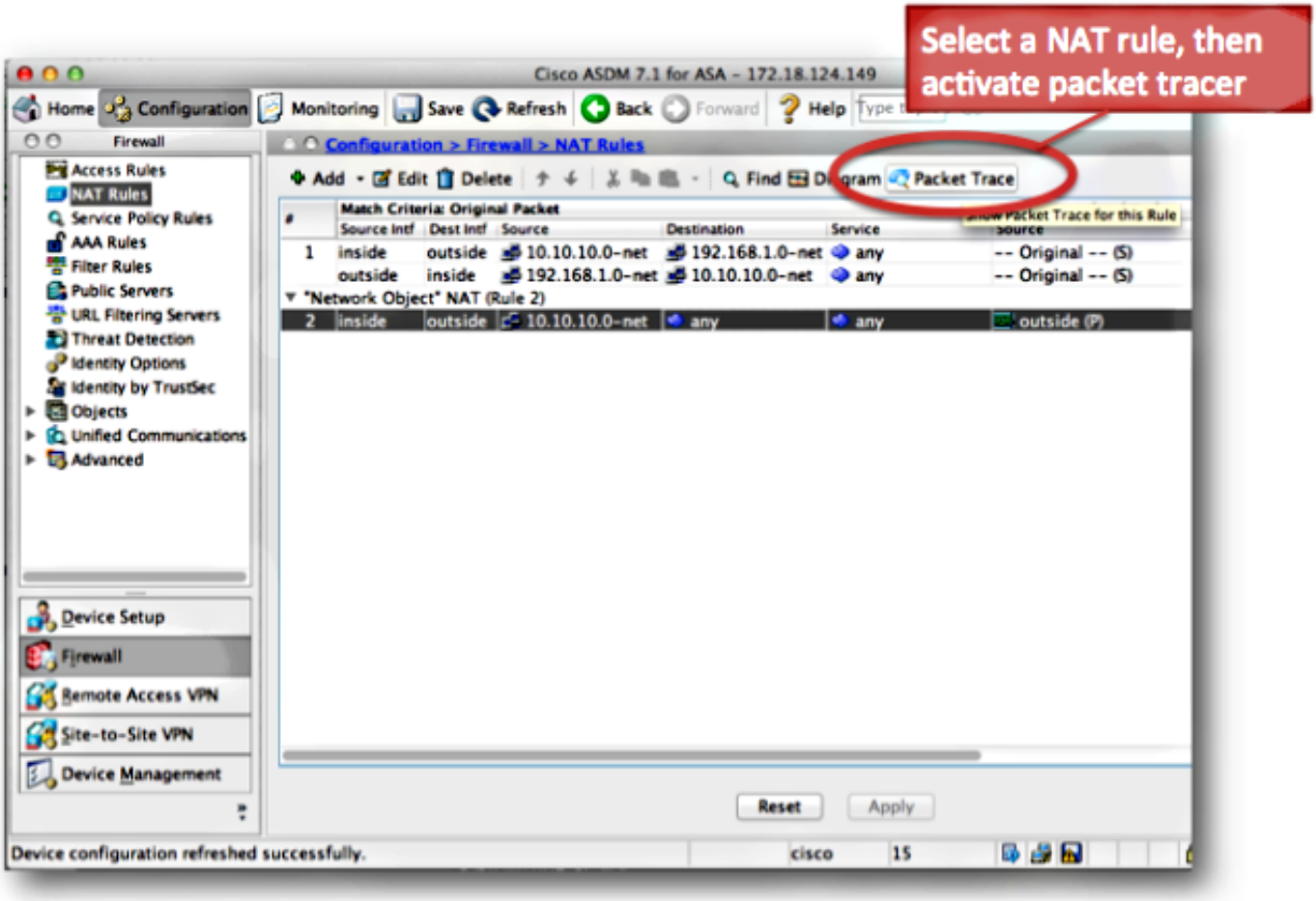
...(output omitted)...

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

Action: allow

ASA#

选择NAT规则并单击Packet Trace以从思科自适应安全设备管理器(ASDM)中激活Packet Tracer。这使用NAT规则中指定的IP地址作为Packet Tracer工具的输入：

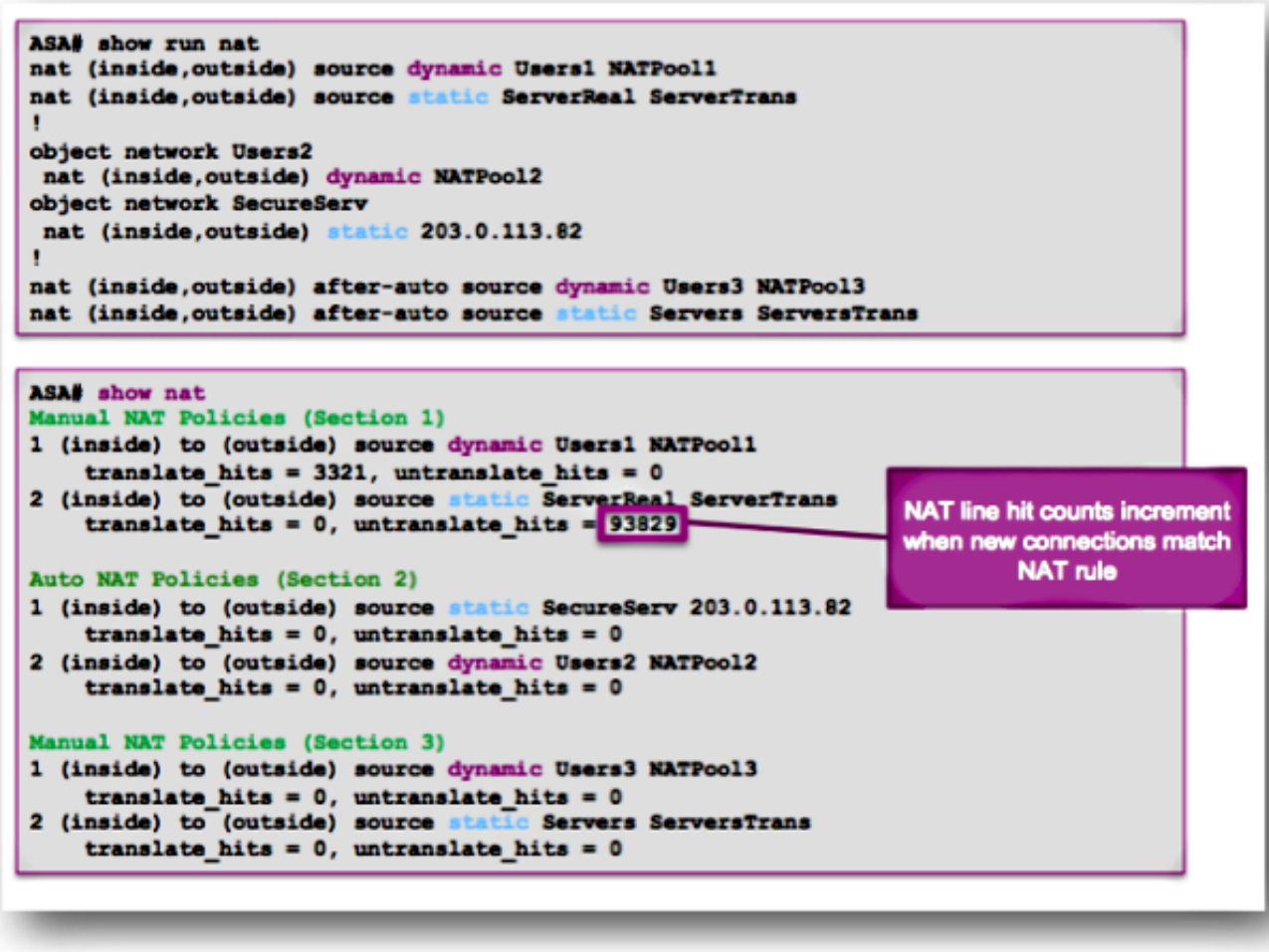


查看Show Nat命令的输出

show nat detail命令的输出可用于查看NAT策略表。具体而言，可以使用translate_hits和untranslate_hits计数器确定ASA上使用哪些NAT条目。

如果您看到新的NAT规则没有translate_hits或untranslate_hits，则意味着流量未到达ASA，或者可能另一个在NAT表中优先级较高的规则与流量匹配。

下面是来自其他ASA配置的NAT配置和NAT策略表：



在上一个示例中，此ASA上配置了六个NAT规则。show nat输出显示如何使用这些规则构建NAT策略表，以及每个规则的translate_hits和untranslate_hits数量。

这些命中计数器每次连接仅增加一次。在通过ASA建立连接后，匹配该当前连接的后续数据包不会增加NAT线路（很像访问列表命中计数在ASA上的工作方式）。

Translate_hits：在转发方向上与NAT规则匹配的新连接数。

“转发方向”表示连接是通过ASA在NAT规则中指定的接口方向建立的。

如果NAT规则指定将内部服务器转换为外部接口，则NAT规则中接口的顺序为“nat (inside，outside)……”；如果该服务器发起到外部主机的新连接，则translate_hit计数器将会增加。

Untranslate_hits：在相反方向与NAT规则匹配的新连接数。

如果NAT规则指定将内部服务器转换为外部接口，则NAT规则中接口的顺序为“nat (inside，outside)……”；如果ASA外部的客户端发起到内部服务器的新连接，则untranslate_hit计数器将会增加。

同样，如果您看到新的NAT规则没有translate_hits或untranslate_hits，则意味着流量未到达ASA，或者可能另一个在NAT表中优先级较高的规则与流量匹配。

NAT问题故障排除方法

使用Packet Tracer以确认示例数据包是否与ASA上的正确NAT配置规则匹配。使用show nat detail命令可以了解匹配的NAT策略规则。如果连接匹配的NAT配置与预期的不同，请通过以下问题排除故障：

- 是否有不同的NAT规则优先于您希望流量命中的NAT规则？
- 是否存在另一个NAT规则，其对象定义过于宽泛（子网掩码太短，例如255.0.0.0），从而导致此流量与错误的规则匹配？
- 手动NAT策略是否顺序混乱，从而导致数据包匹配错误的规则？
- 您的NAT规则配置是否不正确，从而导致规则与您的流量不匹配？

有关示例问题和解决方案，请参见下一节。

NAT配置的常见问题

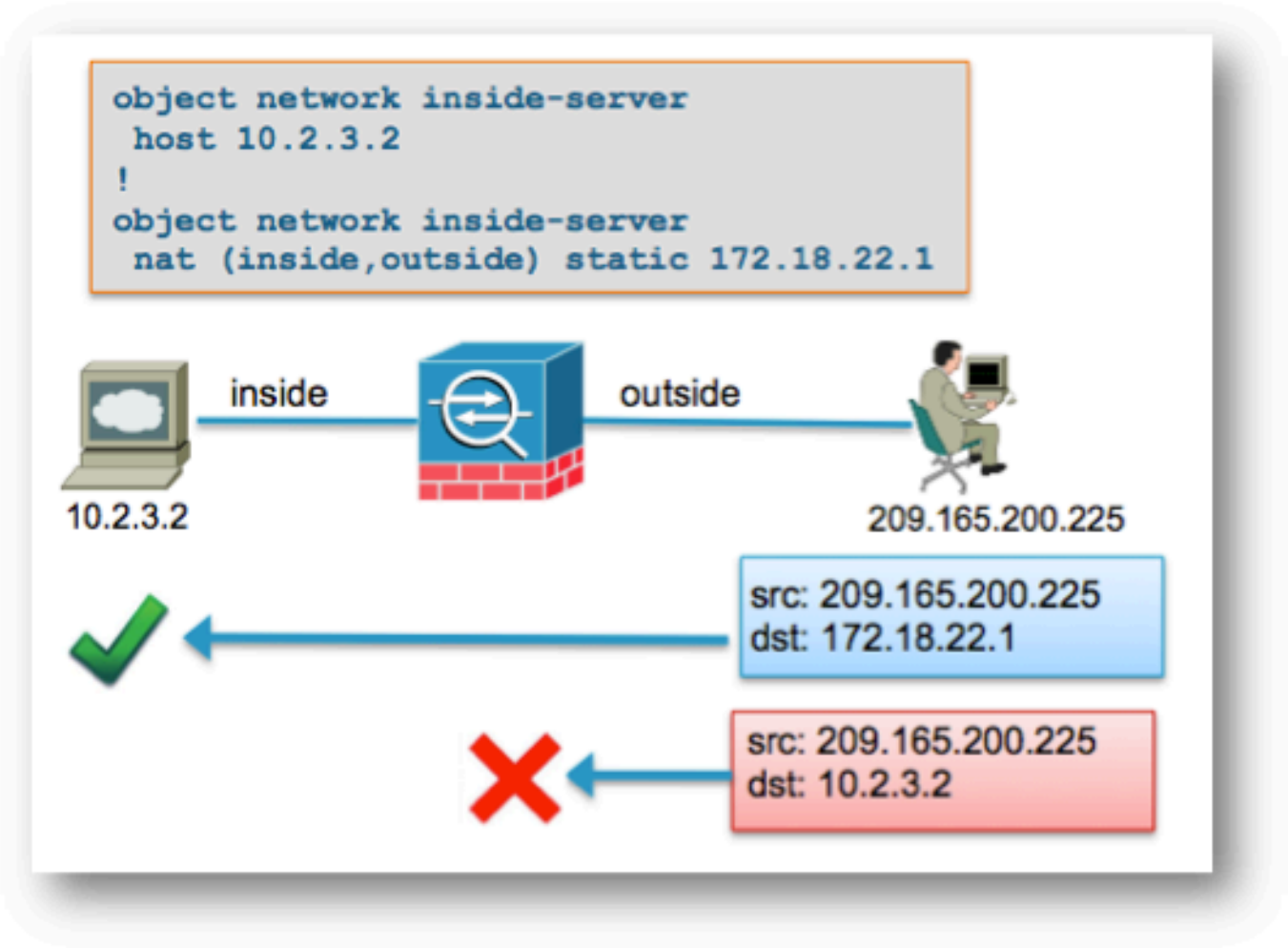
以下是在ASA上配置NAT时遇到的常见问题。

问题：流量因NAT反向路径故障(RPF)而失败。错误：为转发和反向流匹配的非对称NAT规则

NAT RPF检查可确保ASA在转发方向转换的连接（例如TCP同步[SYN]）在相反方向被同一NAT规则转换，例如TCP SYN/确认(ACK)。

通常，此问题是由发往NAT语句中的本地（未转换）地址的入站连接引起的。在基本级别，NAT RPF验证从服务器到客户端的反向连接是否与同一NAT规则匹配；如果不匹配，则NAT RPF检查失败。

示例：209.165.200.225



当位于192.168.200.225的外部主机将直接发往本地（未转换）IP地址10.2.3.2的数据包时，ASA将丢弃该数据包并记录下此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
```

解决方案：

首先，确保主机将数据发送到正确的全局NAT地址。如果主机发送的数据包目的地址正确，请检查连接匹配的NAT规则。

验证NAT规则定义正确，NAT规则中引用的对象正确。还要验证NAT规则的顺序是否合适。

使用Packet Tracer实用程序指定被拒绝的数据包的详细信息。Packet tracer必须显示由于RPF检查失败而丢弃的数据包。

接下来，查看Packet Tracer的输出，以便查看NAT阶段和NAT-RPF阶段中匹配的NAT规则。

如果数据包在NAT RPF检查阶段匹配NAT规则（表明反向流会命中NAT转换），但在NAT阶段不匹

配规则（表明转发流不会命中NAT规则），则丢弃数据包。

此输出与上图所示的场景相匹配，其中外部主机错误地将流量发送到服务器的本地IP地址，而不是全局（转换后的）IP地址：

```
<#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)#
```

当数据包的目的地址正确映射IP地址172.18.22.1时，数据包在转发方向的非NAT阶段与正确的NAT规则匹配，在NAT RPF检查阶段与相同的规则匹配：

```
<#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

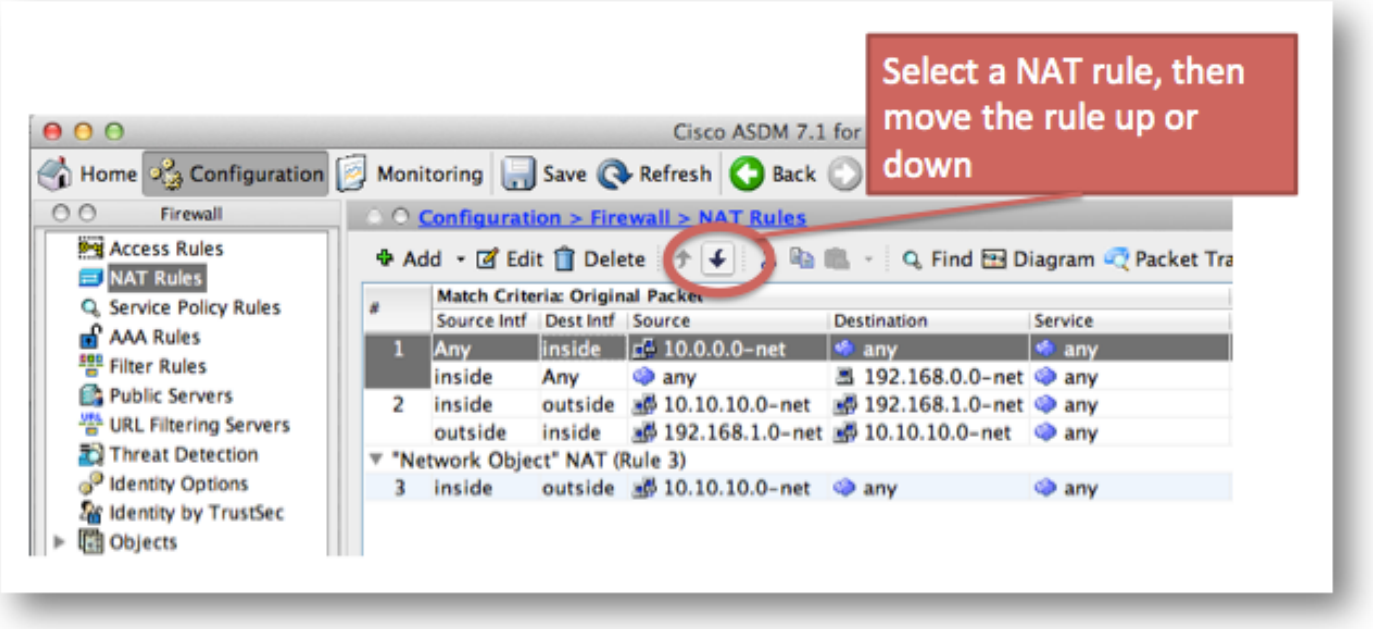
```
Config:
object network inside-server
 nat (inside,outside) static 172.18.22.1
Additional Information:
...

ASA(config)#
```

问题：手动NAT规则顺序混乱，导致不正确的数据包匹配

手动NAT规则根据它们在配置中的外观进行处理。如果配置中首先列出一个非常广泛的NAT规则，则它可以覆盖NAT表中更靠下的另一个更具体规则。使用Packet Tracer验证您的流量到达哪个NAT规则；可能需要将手动NAT条目重新排列到不同的顺序。

解决方案：

使用ASDM对NAT规则重新排序。



解决方案：

如果删除规则并在特定行号重新插入，则可以使用CLI对NAT规则进行重新排序。要在特定行插入新规则，请在指定接口后输入行号。

示例：

```
<#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
```

问题

NAT规则过于宽泛，无意中与某些流量匹配。 有时会创建使用过宽对象的NAT规则。如果这些规则放置在NAT表的顶部（例如，位于第1部分的顶部），则它们可能匹配比预期更多的流量，导致更靠下表的NAT规则永远不会被命中。

解决方案

使用Packet Tracer确定流量是否与对象定义过于宽泛的规则匹配。如果出现这种情况，您必须缩小这些对象的范围，或者在NAT表中将规则进一步向下移动，或者移动到NAT表的after-auto部分（第3部分）。

问题

NAT规则将流量转移到不正确的接口。 当确定数据包从ASA传出的接口时，NAT规则可以优先于路由表。如果入站数据包与NAT语句中的转换IP地址匹配，则会使用NAT规则来确定出口接口。

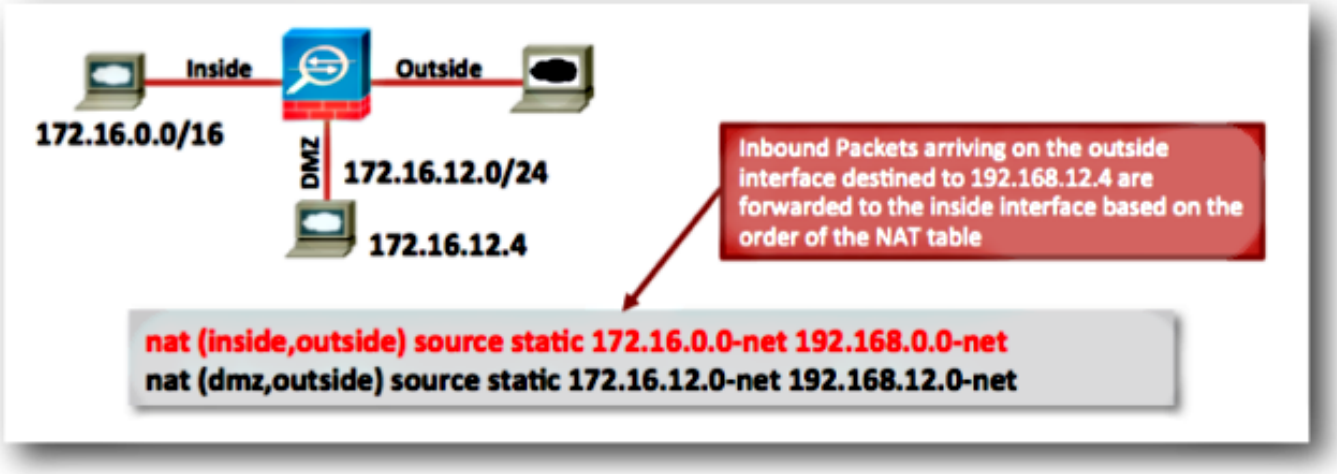
NAT转移检查（可以覆盖路由表的内容）检查是否存在任何NAT规则，为到达接口的入站数据包指定目标地址转换。

如果没有明确指定如何转换该数据包目标IP地址的规则，则会查询全局路由表以确定出口接口。

如果有规则明确指定如何转换数据包目标IP地址，则NAT规则会将数据包提取到转换中的另一个接口，并有效绕过全局路由表。

此问题通常出现在入站流量中，这些流量到达外部接口，并且通常是由将流量转移到非预期接口的无序NAT规则引起的。

示例：



解决方案：

可通过以下任一操作解决此问题：

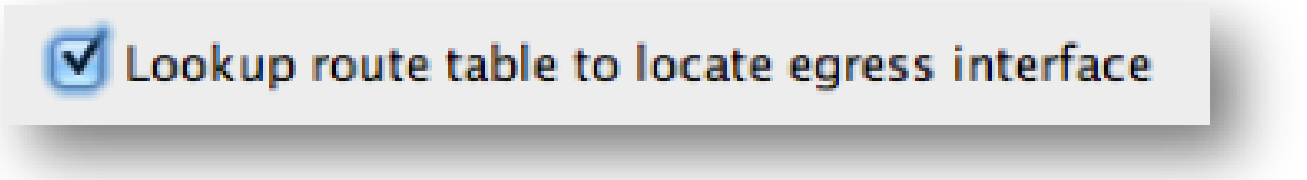
- 对NAT表重新排序，以便首先列出更具体的条目。
- 为NAT语句使用非重叠全局IP地址范围。

请注意，如果NAT规则是身份规则（这意味着规则不会更改IP地址），则可以使用route-lookup关键字（此关键字不适用于上一个示例，因为NAT规则不是身份规则）。

route-lookup关键字会使ASA在匹配NAT规则时执行额外检查。它会检查ASA的路由表是否将数据包转发到此NAT配置将数据包转移到的同一出口接口。

如果路由表出口接口与NAT转移接口不匹配，则不会匹配NAT规则（跳过该规则），数据包会继续向下通过NAT表进行处理，以由以后的NAT规则进行处理。

route-lookup选项仅在NAT规则是身份NAT规则时才可用，这意味着规则不会更改IP地址。如果将route-lookup添加到NAT行的末尾，或者在ASDM的NAT规则配置中选中Lookup route table to locate egress interface复选框，则可以对NAT规则启用route-lookup选项：



问题：NAT规则导致ASA为映射接口上的流量代理地址解析协议(ARP)

ASA代理ARP用于全局接口上NAT语句中的全局IP地址范围。如果将no-proxy-arp关键字添加到NAT语句，则可以基于每个NAT规则禁用此代理ARP功能。

如果无意中将全局地址子网创建得比预期的大得多，也会出现此问题。

解决方案

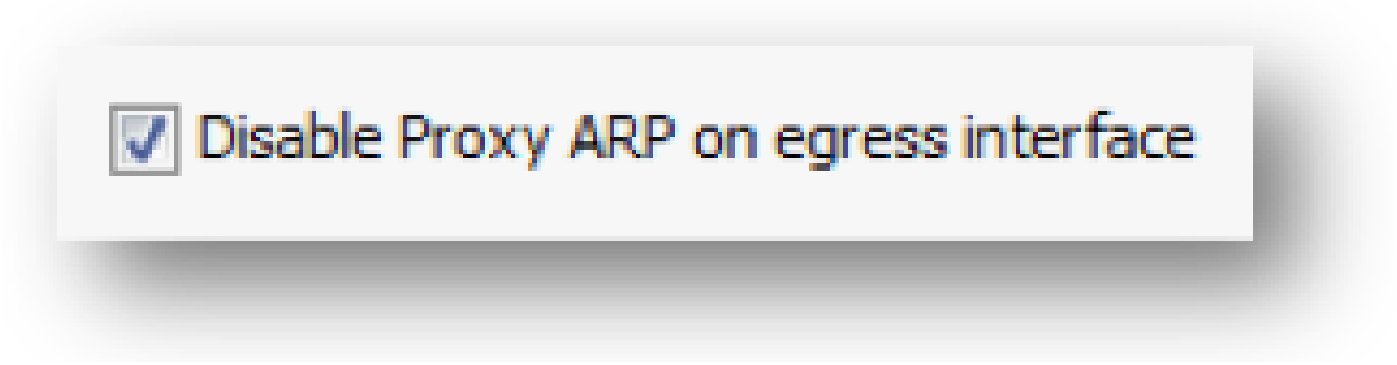
如有可能，向NAT行添加no-proxy-arp关键字。

示例：

```
<#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#
```

这也可以通过ASDM完成。在NAT规则中，选中Disable Proxy ARP on egress interface复选框。



.

相关信息

- 视频：DMZ服务器访问的ASA端口转发（版本8.3和8.4）
- 基本ASA NAT配置：ASA版本8.3及更高版本中DMZ中的Web服务器
- 第2册：思科ASA系列防火墙CLI配置指南，9.1
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。