ASA网络地址转换配置故障排除

目录

简介

本文描述如何排除故障在思科可适应安全工具(ASA)平台的网络地址转换(NAT)配置。 本文为ASA版本8.3和以上是有效。

> **Note**:对于NAT一些基本示例配置，包括视频显示一基本NAT配置，在本文的底部参见部分相关信息。

排除故障在ASA的NAT配置

当您排除故障NAT配置时，知道是重要的在ASA的NAT配置如何用于构件NAT策略表。

这些配置错误占ASA管理员遇到的NAT问题的多数：

- NAT配置规则有故障。例如，一个手工的NAT规则被放置在NAT表顶部，导致更加特定的规则放置更更的下来从未点击的NAT表。
- 用于NAT配置的网络对象是太清楚的，造成流量疏忽地匹配这些NAT规则，并且未命中更加特定的NAT规则。

数据包跟踪程序工具可以用于诊断在ASA的最Nat相关的问题。请参阅下一部分关于NAT配置如何用于构件NAT策略表和如何排除故障和解决特定NAT问题的更多信息。

另外， **detail命令的show nat**可以用于为了了解哪些NAT规则由新连接点击。

ASA配置如何用于建立NAT策略表

ASA处理的所有信息包被评估NAT表。此评估在顶部(下来部分1)和工作开始，直到NAT规则匹配。一旦NAT规则匹配，该NAT规则应用对连接，并且没有其他NAT策略没有根据数据包核对。

在ASA的NAT策略从NAT配置被建立。

ASA NAT表的三个部分是：

第 1 部分	**手工的NAT策略** 这些按他们在配置里出现的顺序处理。
第 2 部分	**自动NAT策略** 这些处理根据NAT类型(静态或动态)和在对象的前缀(子网掩码)长度。
第 3 部分	**在以后自动手工的NAT策略** 这些按他们在配置里出现的顺序处理。

此图表显示不同的NAT部分，并且他们如何被定购：

此示例显示与两个规则(一个指南NAT语句和一自动NAT配置)的ASA的NAT配置如何在NAT表里代表：

如何排除故障NAT问题

请使用数据包跟踪程序工具

为了排除故障与NAT配置的问题，请使用**数据包跟踪程序**工具为了验证数据包押NAT策略。数据包跟踪程序允许您指定输入ASA的示例数据包，并且ASA指示什么配置适用于数据包，并且，如果允许。

在下面的示例中进入内部接口和被注定到在互联网的一台主机的，示例TCP数据包给。数据包跟踪程序工具显示数据包匹配一个动态NAT规则和翻译对**172.16.123.4**外部IP地址：

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 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**并且点击**数据包踪迹**为了激活从Cisco Adaptive Security Device Manager (ASDM)的数据包跟踪程序。这在NAT规则使用作为输入指定的IP地址数据包跟踪程序工具：

查看输出show nat命令

detail命令的show nat的输出可以用于为了查看NAT策略表。特别地， **translate_hits**和**untranslate_hits**计数器可以用于为了确定哪些NAT条目在ASA使用。如果看到您新的NAT规则没有**translate_hits**或**untranslate_hits**，该意味着或者流量不到达在ASA，或许或者有一更加高优先级在NAT表里的一个不同的规则匹配流量。

这是NAT配置和NAT策略表从一不同的ASA配置：

在前一个示例中，有在此ASA配置的六个NAT规则。**show nat**输出显示这些规则如何用于构件NAT策略表，以及**translate_hits**和**untranslate_hits**数量每个规则的。这些命中计数器一次只每连接增加。在连接通过ASA后被建立，匹配该当前连接的后续信息包不增加NAT线路(很象方法访问列表命中数计数请工作在ASA)。

Translate_hits ：匹配在转发方向的NAT规则新连接的数量。

“转发方向”意味着连接通过ASA被建立了朝指定的接口的方向在NAT规则。如果NAT规则指定内部的服务器翻译对外部接口，接口的定货在NAT规则的“nat (里面，从外部)…”;如果该服务器首次对一台主机的一个新连接在外部， **translate_hit**计数器增加。

Untranslate_hits ：匹配在反向的NAT规则新连接的数量。

如果NAT规则指定内部的服务器翻译对外部接口，接口的定货在NAT规则的“nat (里面，从外部)…”;如果ASA的外部的一个客户端首次对服务器的一个新连接在里面， **untranslate_hit**计数器增加。

再次，如果看到您新的NAT规则没有**translate_hits**或**untranslate_hits**，该意味着或者流量不到达在ASA，或许或者有一更加高优先级在NAT表里的一个不同的规则匹配流量。

NAT问题故障排除方法

请使用数据包跟踪程序为了确认示例数据包匹配在ASA的适当的NAT配置规则。请使用**detail命令的show nat**为了了解哪些NAT策略规则点击。如果连接比预计匹配一不同的NAT配置，请排除故障与这些问题：

- 有没有优先于NAT规则您打算流量点击的一个不同的NAT规则？
- 有没有与是太清楚的对象定义的一个不同的NAT规则(子网掩码是否是太短的，例如255.0.0.0)造成此流量匹配错误的规则？

- 手工的NAT是否是故障中的策略，造成数据包匹配错误的规则？
- 您的不正确地配置的NAT规则是否是，导致不是规则匹配您的流量？

请参阅下一部分关于问题示例和解决方案。

与NAT配置的常见问题

这是遇到的一些常见问题，当您配置在ASA时的NAT。

问题：流量发生故障由于NAT反向路径失败(RPF) Error:为转发和反向流匹配的不对称NAT规则

NAT RPF检查保证由在转发方向的ASA翻译的一连接，例如TCP同步(SYN)，由在反向的同一个NAT规则翻译，例如TCP SYN/acknowledge (ACK)。

通常，此问题由被注定的Inbound连接引起对本地(未翻译的)地址的NAT语句。在一个基本级别，NAT RPF验证从服务器的反向连接到客户端匹配同一个NAT规则;如果它不， NAT RPF检查发生故障。

示例：

当在**209.165.200.225的**外部主机发送被注定的数据包直接地对**10.2.3.2的**本地(未翻译的)时IP地址，ASA丢弃数据包并且记录此Syslog ：

```
ASA# packet-tracer input inside tcp 10.10.10.123 12345 209.165.200.123 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#
```

解决方案：

首先，请保证主机发送数据对正确全局NAT地址。如果主机发送被注定的数据包对正确地址，请检

查由连接点击的NAT规则。验证NAT规则正确地定义，并且NAT规则参考的对象正确。并且请验证NAT规则的命令是适当的。

请使用数据包跟踪程序工具为了指定被拒绝的数据包的详细信息。数据包跟踪程序应该显示丢弃的数据包由于RPF检查失败。其次，看看数据包跟踪程序输出为了看到哪些NAT规则在NAT相位和NAT-RPF相位点击。

如果数据包匹配在NAT RPF检查相位的一个NAT规则，表明反向流将点击NAT转换，但是不匹配在NAT相位的一个规则，表明向前流不会点击NAT规则，数据包丢弃。

此输出匹配在上一个图表中显示的方案，外部主机不正确地发送流量对服务器而不是全局(翻译的)IP地址的本地IP地址：

```
ASA# packet-tracer input outside tcp 209.165.200.225 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)#
```

当数据包被注定对172.18.22.1时的正确被映射的IP地址，数据包匹配在UN-NAT相位的正确NAT规则在转发方向和在NAT RPF检查相位的同一个规则：

```
ASA(config)# packet-tracer input outside tcp 209.165.200.225 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：手工的NAT规则有故障，导致不正确的信息包匹配

手工的NAT规则在配置里处理根据他们的外观。如果一个非常清楚的NAT规则首先在配置里列出，在NAT表里也许改写别的，更多特定规则下来。请使用数据包跟踪程序为了验证哪个NAT规则您的流量点击;重新整理手工的NAT条目到不同命令也许是必要的。

解决方案：

重拨与ASDM的NAT规则。

解决方案：

如果删除规则并且再插入它在特定编号， NAT规则可以重拨与CLI。在接口指定之后，为了插入新规则在特定，请输入线路号。

示例：

```
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规则是太清楚的并且疏忽地匹配若干流量

有时使用对象是太清楚的NAT规则创建。如果这些规则在NAT表的顶部附近被放置(例如在部分1顶部)，他们比打算不也许匹配更多流量和导致NAT规则在表下点击。

解决方案：

请使用数据包跟踪程序为了确定您的流量是否匹配与是太清楚的对象定义的一个规则。如果这是实际情形，您应该减少范围那些对象，或者请移动规则在NAT表下，或者对在以后自动部分(NAT表的部分3)。

问题：NAT规则将流量转变为不正确的接口

NAT规则能优先于路由表，当他们确定时哪个接口数据包出口ASA。如果入站数据包匹配在NAT语句的一转换后的IP地址， NAT规则用于为了确定出口接口。

看到NAT (是的转移检查什么能改写路由表)的检查是否有指定入站数据包的目的地址地址转换在接口到达的任何NAT规则。如果没有明确地指定如何翻译该数据包目的IP地址，则全球路由表的规则参见确定出口接口。如果有明确地指定如何翻译数据包目的IP地址，则NAT规则“的规则在转换和全球路由表里拉”数据包对另一个接口有效绕过。

此问题为入站数据流比较常见，在外部接口到达，并且通常归结于故障中NAT裁决转移流量对不愿意的接口。

示例：

解决方案：

此问题可以用这些操作之一解决：

- 重拨NAT表，以便特定条目首先列出越多。
- 请使用非重复全局IP地址范围NAT语句。

注意，如果NAT规则是标识规则， (意味着IP地址没有由规则更改)可以然后使用路由**查找**关键字(此关键字不是可适用的对以上示例，因为NAT规则不是标识规则)。当匹配NAT规则时，路由**查找**关键字造成ASA执行一额外的检查。它检查ASA的路由表转发数据包对此NAT配置将数据包转变的同一出口接口。如果路由表出口接口不匹配NAT转移接口， NAT规则没有匹配(规则被跳过)，并且数据包继续在一个最新NAT规则将处理的NAT表下。

路由查找选项只是可用的，如果NAT规则是'标识' NAT规则，因此意味着IP地址没有由规则更改。 **路由查找**选项可以每个NAT规则启用是否添加路由**查找**到NAT线路的末端，或者是否在NAT规则配置里检查**查找路由表找出出口接口**复选框在ASDM ：

问题：NAT规则导致ASA代理地址解析协议(ARP)在被映射的接口的流量的

全局IP地址的ASA代理ARP在全局接口的一个NAT语句排列。如果添加NO-代理**ARP**关键字到NAT语句，此代理ARP功能可以禁用根据一个每NAT规则基本类型。

此问题也被看到，当全局地址子网大于它打算疏忽地创建时。

解决方案：

若可能添加NO-代理**ARP**关键字到NAT线路。

示例：

```
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#
```

这可以用ASDM也完成。在NAT规则内，请检查**在出口接口**复选框的**禁用代理ARP**。

相关信息

- 视频：ASA DMZ服务器访问的(版本8.3和8.4)端口转发
- 基本ASA NAT配置：在DMZ的网络服务器在ASA版本8.3和以上
- 书2 ：思科ASA系列防火墙CLI配置指南， 9.1
- 技术支持和文档 - Cisco Systems