FWSM ：排除故障流量失败由于错误的Xlate

目录

简介

由于处理防火墙服务模块的(FWSM)的数据包的设计，路由信息包建立的xlate能通过防火墙不正确地导致连接的流量失败。为了选择入站数据包的一出口接口， FWSM首先检查发现入站数据包的目的地IP是否在其xlate表里匹配在一个NAT转换(xlate)的任何现有全局IP/Network该接口的。如果找到匹配，根据在xlate条目的本地接口完全选定的出口接口，并且防火墙不参见路由表做出出口接口决策。

FWSM的默认行为是建立在其接口之一接收所有允许的数据包的来源IP的xlate条目。如果数据包通过网络不正确地路由(任何数量的原因)并且到达入站在FWSM的错误接口， xlate被建立反射此。当这发生时，条目在xlate表里在路由表里能改写条目和导致受影响的目的地的流量失败。

本文描述症状和触发此问题的，如何诊断它，并且为防止它提供解决方案发生。

先决条件

要求

思科建议您有FWSMs知识。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

症状

逻辑拓扑

相关配置

```
interface Vlan1
 nameif outside
 security-level 0
 ip address 192.168.100.50 255.255.255.0
!
interface Vlan10
 nameif inside
 security-level 100
 ip address 10.10.1.50 255.255.255.0
!
interface Vlan20
 nameif dmz
 security-level 50
 ip address 10.20.1.50 255.255.255.0
!
same-security-traffic permit intra-interface
access-list outside_in extended permit tcp any host 10.30.1.1 eq www
access-list inside_in extended permit ip any any
access-group inside_in in interface inside
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.100.254
route dmz 10.30.1.0 255.255.255.0 10.20.1.254
```

观察行为

从客户端PC的连接在172.16.1.10对Web服务器在10.30.1.1发生故障。

外部接口的一数据包捕获显示从客户端PC的TCP SYN到达在FWSM的接口的。

```
FWSM# show capture outside
3 packets seen, 3 packets captured
   1: 13:58:09.280752960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   2: 13:58:12.280755950 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   3: 13:58:18.280761960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
3 packets shown
```

dmz接口的一数据包捕获不显示该数据包留下防火墙的。

```
FWSM# show capture dmz
0 packet seen, 0 packet captured
0 packet shown
```

条目在FWSM的连接表里没有被建立，并且Syslog不显示中的任一相关的信息对客户端或服务器IP地址。

触发

在一个基本的级别，此问题是由条目导致的在一个路由信息包不正确地构件的FWSM的xlate表里。由于FWSM的数据包处理设计的方式，防火墙检查xlate表，在检查路由表确定出口接口前。结果，如果数据包匹配现有xlate出口接口根据该条目将选择，即使条目与什么相冲突在路由表里列出。换句话说， xlate表优先于路由表。

为了诊断此问题，请检查**debug命令的show xlate的**输出：

```
FWSM# show xlate debug
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
3 in use, 3 most used
NAT from inside:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:00 timeout 3:00:00 connections
0
NAT from inside:10.30.1.1 to inside:10.30.1.1 flags Ii idle 0:00:07 timeout 3:00:00 connections
0

NAT from dmz:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:10 timeout 3:00:00 connections 0
```

注意： 在show xlate的调试关键字是关键的。没有它， xlate条目不会包括接口名称条目关联与。

xlate表显示有为Web服务器建立的3 xlate。第一xlate被建立在**内部接口**和**外部接口之间**。第二xlate被建立作为使用发夹的或u启用的xlate在**内部接口**。第三xlate被建立在**dmz**和**外部接口之间**。i标志位表明这是标识xlate，并且IP实际上没有翻译。

在条目列出的第一个接口是IP应该实际上存在的“实时”或“本地”接口。第二个接口列出是IP翻译的“被映射的”或“全局”接口。两xlate显示不正确。这是因为Web服务器(10.30.1.1)在**dmz**接口后实际上存在。第三xlate为此网络设计是正确。

连接失败发生由于在表里列出的第一xlate。当客户端的TCP Syn信息包在外部接口到达被注定对10.30.1.1时， FWSM检查xlate表并且匹配首先进入。此条目表明数据包应该在**内部接口的**出口，不正确和数据包是黑洞。

默认情况下， FWSM将自动地建立不匹配一个明确地配置的NAT规则的所有流量的标识xlate。因此，即使数据包在不正确的接口不正确到达， xlate将被建立。特别地对于此案件，从10.30.1.1发出的数据包到达入站在**内部接口**而不是到达在**dmz**接口象预计。

第一xlate (**里面>从外部**)被建立了，当Web服务器设法ping一个不存在的IP地址(10.199.199.1)。ECHO请求离开Web服务器被注定对其默认网关(DMZ路由器)。DMZ路由器转发数据包往内部路由器，每其静态路由：

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

由于10.199.199.0/24网络任何地方实际上不存在，内部路由器跟随其默认路由并且发送数据包对FWSM的**内部接口**：

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

同样， FWSM也没有目的地网络的一个路由。所以，它选择外部接口作为出口接口并且建立标识xlate从里边**>外部**：

```
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.100.254, outside
```

第二xlate (**里面>里面**)被建立了，当Web服务器设法访问DNS服务器，当内部路由器的

10.40.1.254接口临时地是在于下链路抖动时。DNS请求离开Web服务器被注定对其默认网关(DMZ路由器)。DMZ路由器转发数据包往内部路由器，每其静态路由：

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

然而，内部路由器的接口连接对10.40.1.0/24网络临时地是下来，并且其此网络的已连接路由直接地未命中。所以，唯一的匹配的路由在路由表里是默认路由上一步往FWSM ：

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

数据包路由对FWSM的**内部接口**。FWSM的路由表表明目的地网络10.40.1.0/24在同一个**内部接口后**存在：

```
S    10.40.1.0 255.255.255.0 [1/0] via 10.10.1.254, inside
```

由于**intra-interface命令same-security-traffic的permit**启用， FWSM将允许u启用的xlate将被构件。

要汇总，第一xlate触发：

- 在DMZ路由器配置的一个清楚的10.0.0.0/8路由
- 在FWSM的内部接口配置的**permit ip any any ACL**

第二xlate触发：

- 在内部路由器的一个振荡的接口
- **same-security-traffic**在FWSM配置的**permit接口内**

解决方案

有许多不同的可能的解决方案对此问题。首要，删除从表的xlate应该允许流量开始再工作，直到xlate重建。这可以实行同**clear xlate命令**。例如：

```
FWSM# clear xlate interface inside local 10.30.1.1 global 10.30.1.1
```

注意： 使用删除的xlate的所有连接也将被切断。

一旦那完成，重点应该在防止xlate返回。通常时期，多数首选的方法执行此将修复在环境的路由配置防止流量到达在错误的FWSM接口。FWSM也提供几个配置选项解决这些问题。

解决不正确路由配置

此解决方案采取仔细规划和对网络环境的深刻的理解。在第一以上示例中，因为整个/8网络不在其10.50.1.253接口之外，存在DMZ路由器的10.0.0.0/8路由是技术上的错误。反而，存在的某些选项是：

- 一起排除10.50.1.0/24网络全部和通过FWSM路由所有流量。这也提供更加好的分段和安全在内部和DMZ网络之间。
- 只配置在DMZ的静态路由10.40.1.0/24的并且删除10.0.0.0/8路由。
- 请使用在内部和DMZ路由器之间的一个动态路由协议正确地通告实际上存在仅的网络。

经常有调节路由配置的许多可能性，但是结尾目标是保证从一台给的主机的流量能仅到达在单个FWSM接口。

禁用same-security-traffic permit接口内

intra-interface命令same-security-traffic的permit允许FWSM对U字型转向或在接口的发夹流量。这

意味着数据包能进入离开在同一个接口的防火墙。默认情况下此功能禁用并且有很少使用在多数FWSM设计。由于FWSM使用VLAN接口，不应该由FWSM处理在同样VLAN内的逗留的流量。

在第二以上示例中， **intra-interface命令same-security-traffic的permit**允许数据包对回车并且离开**内部接口**。在xlate被建立了前，禁用的**same-security-traffic permit接口内将**防止此行为并且丢弃数据包：

```
FWSM(config)# no same-security-traffic permit intra-interface
```

丢弃在不正确的接口到达的数据包(ACL或uRPF)

在两以上示例中，当从Web服务器的一数据包在**内部接口，**不正确地到达xlate被建立了。为了一起防止问题全部， FWSM可以配置丢弃在错误接口到达的数据包。

FWSM要求所有流量由ACL允许，在能通过前。所以，此功能可以通过只允许从适当的源网络的流量达到在每个接口。在以上示例中，**内部接口**允许所有IP数据流：

```
access-list inside_in extended permit ip any any
```

反而，应该更改这只允许从10.10.1.0/24和10.40.1.0/24子网的流量：

```
access-list inside_in extended permit ip 10.10.1.0 255.255.255.0 any

access-list inside_in extended permit ip 10.40.1.0 255.255.255.0 any
```

在一些环境，这不是可行选项由于通过通过FWSM的不同的网络的大小和缩放。然而，此功能可以达到使用功能呼叫单播逆向路径转发(URPF)。

当uRPF功能启用， FWSM对其路由表将比较第一数据包的源IP地址每连接。如果找到的路由不配合与接口数据包到达，该数据包丢弃的归结于RPF故障。

在以上示例中， FWSM有使用**dmz**接口到达10.30.1.0/24网络的静态路由。所以，如果uRPF在**内部接口**启用，在**内部接口**到达将不正确地丢弃的数据包从Web服务器(10.30.1.1)来源。

为了启用uRPF，请应用**ip验证reverse-path**命令对有问题的每个的接口。例如：

```
FWSM(config)# ip verify reverse-path interface inside
```

Enable (event) xlate旁路

在两个以上示例， xlate用ii标志创建。这些标志表明xlate是在高安全性(i)接口产生的标识转换(i)。默认情况下， FWSM将建立不匹配一个明确NAT/PAT规则的所有流量的这些xlate。为了禁用此行为， xlate**旁路**命令在FWSM 3.2(1)可以启用及以后：

```
FWSM(config)# xlate-bypass
```

此功能将防止FWSM建立标识xlate首先。因此，在以上示例的流量不会重定向对不正确的接口由于xlate条目。然而，流量将穿过FWSM取消转译。

摘要

为了确定数据包的出口接口， FWSM在查看其路由表前永远将参见其xlate表。如果该数据包匹配现有xlate，出口接口根据xlate的关联接口选择。这发生不管在路由表里也许被找到的所有矛盾。这样， xlate表优先于路由表。

默认情况下由于FWSM永远将建立所有新连接的xlate条目，这能导致流量失败，在路由信息包不正确地造成FWSM建立xlate处。如上所述，有这能发生的许多可能的情况，但是所有关连回到在不正

确的接口接收的数据包。本文包括这些可能的问题：

- 清楚的路由设置发送在一个不正确方向的数据包
- FWSM配置允许从不正确源网络的流量
- FWSM配置对发夹/U字型转向流量

为了迅速恢复发生故障由于错误的xlate的连接的连接，请删除条目用**clear xlate命令**。本文也包括防止的这些xlate多种解决方案在将来返回，包括：

- 使用更加特定的路由，解决不正确路由配置
- 禁用same-security-traffic permit接口内
- 丢弃使用ACL或uRPF，在不正确的接口到达的数据包
- 启用xlate旁路

相关信息

- **命令参考：ip验证reverse-path**
- **命令参考：xlate旁路**
- **技术支持和文档 - Cisco Systems**