配置NAT NVI时排除基于IOS区域的策略防火墙检查问题

目录

简介

本文档介绍在Cisco IOS路由器中配置IOS基于区域的防火墙(ZBF)和网络地址转换虚拟接口(NAT NVI)时发生的检查问题。

本文的主要目的是解释此问题的原因，并为您提供在此类实施中允许所需流量通过路由器所需的解决方案。

先决条件

要求

Cisco 建议您了解以下主题：

- IOS路由器中的Cisco ZBF配置。
- IOS路由器中的Cisco NAT NVI配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 集成多业务路由器(ISR G1)
- IOS 15M&T

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。

背景信息

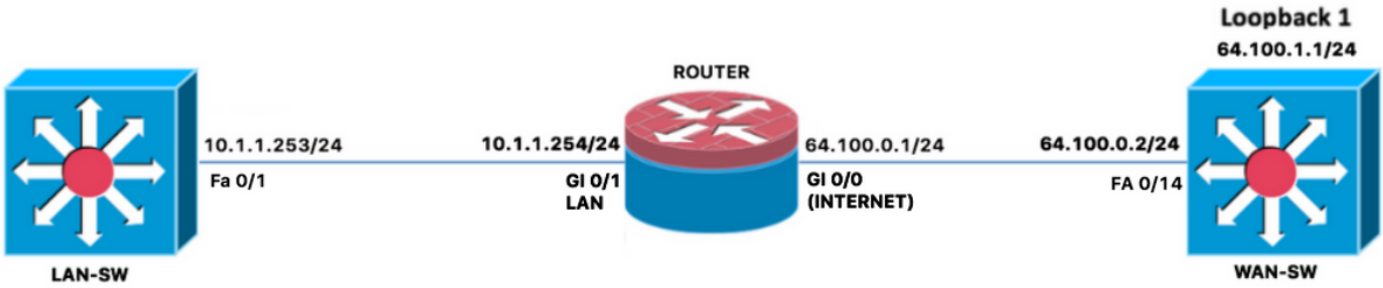
下面进一步详细介绍什么是NAT NVI以及如何在思科路由器上配置NAT NVI:

网络地址转换虚拟接口(NAT NVI)功能消除了将接口配置为NAT内部或NAT外部的要求。接口可以配置为使用NAT或不使用NAT。NVI允许同一提供商边缘(PE)路由器中重叠的VPN路由/转发(VRF)之间的流量，以及重叠网络之间从内部到内部的流量。

NAT虚拟接口

问题：配置NAT NVI时的IOS基于区域的策略防火墙检查问题

ZBF在配置NAT NVI时有检查ICMP和TCP流量的问题，如图所示，它确认ZBF与路由器ROUTER中的NAT NVI一起配置时，TCP和ICMP流量未从内部区域检查到外部区域。



已检查应用于路由器ROUTER的实际ZBF配置，并确认了以下内容：

```
ROUTER#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         64.100.0.1      YES NVRAM  up                    up
GigabitEthernet0/1         10.1.1.254      YES NVRAM  up                    up
GigabitEthernet0/2         unassigned      YES NVRAM  administratively down down
NVI0                       10.0.0.1        YES unset  up                    up
Tunnel1                    10.0.0.1        YES NVRAM  up                    up
ROUTER#show zone security zone self Description: System Defined Zone zone INSIDE Member
Interfaces: Tunnel1 GigabitEthernet0/1 zone OUTSIDE Member Interfaces: GigabitEthernet0/0

Extended IP access list ACL_LAN_INSIDE_TO_OUTSIDE
 10 permit ip 10.0.0.0 0.255.255.255 any (70 matches)

ROUTER#show run | b class-map
class-map type inspect match-any CMAP_FW_PASS_OUTSIDE_TO_SELF
  match access-group name ACL_DHCP_IN
  match access-group name ACL_ESP_IN
  match access-group name ACL_GRE_IN
class-map type inspect match-any CMAP_FW_PASS_SELF_TO_OUTSIDE
  match access-group name ACL_ESP_OUT
  match access-group name ACL_DHCP_OUT
class-map type inspect match-any CMAP_FW_INSPECT_INSIDE_TO_OUTSIDE
  match access-group name ACL_LAN_INSIDE_TO_OUTSIDE
class-map type inspect match-any CMAP_FW_INSPECT_OUTSIDE_TO_SELF
  match access-group name ACL_SSH_IN
  match access-group name ACL_ICMP_IN
  match access-group name ACL_ISAKMP_IN
class-map type inspect match-any CMAP_FW_INSPECT_SELF_TO_OUTSIDE
  match access-group name ACL_ISAKMP_OUT
  match access-group name ACL_NTP_OUT
  match access-group name ACL_ICMP_OUT
  match access-group name ACL_HTTP_OUT
  match access-group name ACL_DNS_OUT

policy-map type inspect PMAP_FW_INSIDE_TO_OUTSIDE
class type inspect CMAP_FW_INSPECT_INSIDE_TO_OUTSIDE
```

```
  inspect
 class class-default
  drop log
policy-map type inspect PMAP_FW_SELF_TO_OUTSIDE
class type inspect CMAP_FW_INSPECT_SELF_TO_OUTSIDE
  inspect
 class type inspect CMAP_FW_PASS_SELF_TO_OUTSIDE
  pass
class class-default
  drop log
policy-map type inspect PMAP_FW_OUTSIDE_TO_SELF
class type inspect CMAP_FW_INSPECT_OUTSIDE_TO_SELF
  inspect
 class type inspect CMAP_FW_PASS_OUTSIDE_TO_SELF
  pass
class class-default
  drop log

zone security INSIDE
zone security OUTSIDE
zone-pair security ZPAIR_FW_INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE service-policy
type inspect PMAP_FW_INSIDE_TO_OUTSIDE zone-pair security ZPAIR_FW_SELF_TO_OUTSIDE source self
destination OUTSIDE
  service-policy type inspect PMAP_FW_SELF_TO_OUTSIDE
zone-pair security ZPAIR_FW_OUTSIDE_TO_SELF source OUTSIDE destination self
  service-policy type inspect PMAP_FW_OUTSIDE_TO_SELF

interface GigabitEthernet0/1
 description LAN
 ip address 10.1.1.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 zone-member security INSIDE
 duplex auto
 speed auto
 end

interface GigabitEthernet0/0
 description INTERNET
 ip vrf forwarding PUBLIC
 ip address 64.100.0.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 zone-member security OUTSIDE
 duplex auto
 speed auto
 end

ip nat inside source route-map RMAP_NAT_POLICY interface GigabitEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 64.100.0.2 name DEFAULT ip route vrf INET_PUBLIC
0.0.0.0 0.0.0.0 GigabitEthernet0/0 64.100.0.2 name DEFAULT route-map RMAP_NAT_POLICY permit 10
description ROUTE-MAP FOR NAT match ip address ACL_NAT

ROUTER#show access-list ACL_NAT
Extended IP access list ACL_NAT
10 permit ip 10.0.0.0 0.255.255.255 any (72 matches)
```

当流量通过路由器ROUTER发送时，请确认下一个结果：

当NAT配置应用了ip为路由器接口分配的nat inside和ipnat outside，以及ipnat inside 用于动态NAT的nat语句，ping未从 LAN-SW 10.1.1.253 IP地址到64.100.1.1 WAN-SW交换机。

即使从路由器接口删除ZBF区域后，流量也未通过路由器，在 NAT规则已更改如下：

```
ip nat source route-map RMAP_NAT_POLICY interface GigabitEthernet0/0 overload

interface GigabitEthernet0/1
description LAN
ip address 10.1.1.254 255.255.255.0
ip nat enable
ip virtual-reassembly in
duplex auto
speed auto
end

interface GigabitEthernet0/0
description INTERNET
ip vrf forwarding PUBLIC
ip address 64.100.0.1 255.255.255.0
ip nat enable
ip virtual-reassembly in
duplex auto
speed auto
```

之后，在路由器接口中重新应用ZBF区域。

```
ip nat source route-map RMAP_NAT_POLICY interface GigabitEthernet0/0 overload

interface GigabitEthernet0/1
description LAN
ip address 10.1.1.254 255.255.255.0
ip nat enable
ip virtual-reassembly in
zone-member security INSIDE
duplex auto
speed auto
end

interface GigabitEthernet0/0
description INTERNET
ip vrf forwarding PUBLIC
ip address 64.100.0.1 255.255.255.0
ip nat enable
ip virtual-reassembly in
zone-member security OUTSIDE
duplex auto
speed auto
```

一旦ZBF区域在路由器接口中重新应用，确认ZBF开始显示从OUTSIDE区域到自区域的回复的丢弃系统日志消息：

```
Jun 28 18:32:13.843: %FW-6-SESS_AUDIT_TRAIL_START: (target:class)-
(ZPAIR_FW_INSIDE_TO_OUTSIDE:CMAP_FW_INSPECT_INSIDE_TO_OUTSIDE):Start tcp session: initiator
(10.1.1.253:59393) -- responder (64.100.1.1:23)

Jun 28 18:32:13.843: %FW-6-DROP_PKT: Dropping tcp session 64.100.1.1:23 64.100.0.1:59393 on
zone-pair ZPAIR_FW_OUTSIDE_TO_SELF class class-default due to  DROP action found in policy-map
with ip ident 62332
```

> **注意：**从日志消息中，您可以在第一个AUDIT_TRAIL日志中确认TCP Telnet会话首次从INSIDE发起到OUTSIDE区域，但是返回的流量由于NAT NVI和ZBF在位时处理流量的方式而错误地从OUTSIDE返回到自区域。

它已确认，强制返回流量通过ZBF的唯一方法是应用通过操作规则以允许从外部区域到自区域的返回流量，此规则应用于icmp和TCP流量作为测试目的，并且对于这两者，确认其工作正常且允许根据需要返回流量。

> **注意：**要在OUTSIDE区域和自区域之间的区域对中应用通过操作规则，不建议解决此问题，这是因为ZBF强烈要求检查返回流量并自动允许其通过。

解决方案

ZBF不支持NAT NVI，此问题的唯一解决方案是应用CSCsh12490区域防火墙和NVI NAT不互操作错误中提到的任何解决方法，详细信息如下：

1.删除ZBF并应用传统防火墙(CBAC)，这当然不是最佳选项，这是因为CBAC是IOS路由器的已经寿命终止的防火墙解决方案，IOS-XE路由器不支持它。

或者

2.从IOS路由器删除NAT NVI配置，并改为应用正常的内部/外部NAT配置。

> **提示：**另一种可能的解决方法是在路由器中保留NAT NVI配置并删除ZBF配置，然后在具有安全功能的任何其他安全设备中应用所需的安全策略。

相关 Bug

CSCsh12490区域防火墙和NVI NAT不能互操作

CSCek35625 NVI和FW互操作性增强

CSCvf17266 DOC:ZBF配置指南缺少与NAT NVI相关的限制

相关信息

- NAT虚拟接口
- 安全配置指南：基于区域的策略防火墙，Cisco IOS版本15M&T
- Cisco IOS 防火墙传统和基于区域的虚拟防火墙应用程序配置示例