当配置时，排除IOS区域基本策略防火墙检查问题故障NAT NVI

Contents

Introduction

本文描述发生的检查问题，当IOS基于区域的防火墙(ZBF)时与网络地址转换虚拟接口(NAT NVI)一起被配置在Cisco IOS路由器。

本文的主要目的将解释此问题为什么发生并且提供您要求的解决方案允许必需的数据流穿过在这种的路由器实施。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- 在IOS路由器的Cisco ZBF配置。
- 在IOS路由器的Cisco NAT NVI配置。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 集成服务路由器(ISR G1)
- IOS 15M&T

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.如果您的网络实际，请保证您了解所有命令的潜在影响。

背景信息

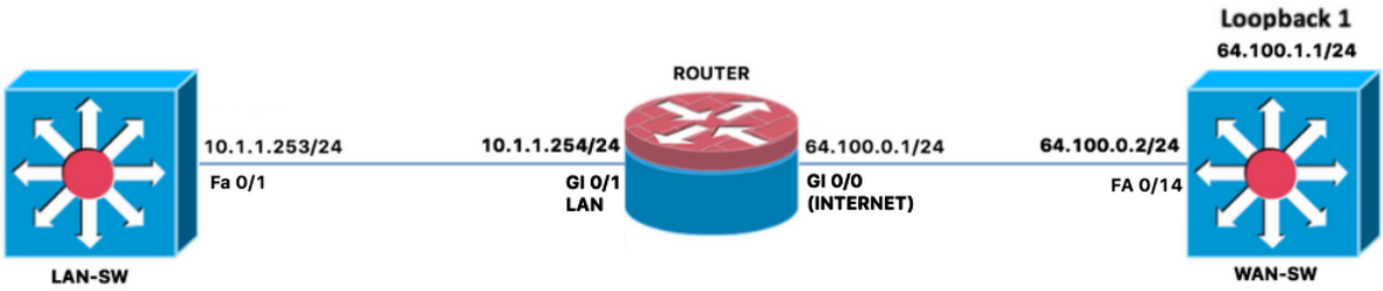
这里关于什么NAT NVI是和如何的更详细的资料配置它在Cisco路由器：

网络地址转换虚拟接口(NAT NVI)功能去除需求从外部配置接口作为内部的NAT或NAT。可以配置接口使用NAT或不使用NAT。NVI允许交迭的VPN路由/转发(VRF)之间的从里边数据流在同一个服务商边缘路由器和数据流对在重叠网络之间的里面。

NAT虚拟接口

问题： 当配置时， IOS区域根据策略防火墙检查问题NAT NVI

ZBF有检查的问题ICMP和TCP通信流，当配置时NAT NVI，这里此问题示例。 如镜像所显示时，当ZBF与在路由器**路由器的**NAT NVI一起被配置被确认TCP和ICMP数据流没有从自外部区域的里面检查。



检查实际ZBF配置适用于路由器**路由器**并且确认了以下：

```
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)
```

当数据流通过路由器**路由器**被发送，被确认下个结果：

当NAT配置运用了与**内部的ipnat**和**ipnat外部**分配到路由器接口，与**ipnat一起在**动态NAT的nat语句

里面， ping没有从**LAN-SW** 10.1.1.253 IP地址通过到在**WAN-SW**交换机的64.100.1.1。

在ZBF区域从路由器接口以后被去除了，数据流没有穿过路由器，它开始通过通过，在更改后NAT规则如下：

```
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
```

在此以后，重新应用路由器接口的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
```

当ZBF区域在路由器接口重新应用，被确认ZBF开始显示回复的丢弃系统消息从外部区域给自身区域：

```
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
```

> **Note**:从日志消息，您在第一本AUDIT_TRAIL日志能确认，当TCP远程登录会话从自外部区域时的里面首先被起动，另一方面，但是回程数据流错误来自到ZBF自自身区域的外部由于处理数据流的NAT NVI和方式，当ZBF到位时。

被确认，强制回程数据流的唯一方法穿过ZBF是运用用通过操作规则允许从外部区域的回程数据流到自身区域，此规则为icmp和TCP通信流适用，当测试目的和被确认它的两个的良好工作并且允许回程数据流如所需求。

> **Note**:要运用在区域对的一条用通过操作规则在外部区域和自身区域之间，不是此问题的推荐的解决方案，这是因为对于回程数据流高度是必需的获得检查和自动地准许由ZBF。

解决方案

ZBF不支持NAT NVI，此问题的唯一的解决方案是应用在CSCsh12490区域防火墙提及的其中任一个解决方法，并且NVI NAT不兼容Bug，这里详细资料：

1. 去除ZBF并且适用经典防火墙(CBAC)，当然是不是最佳的选项，并且这是因为CBAC已经是生活IOS路由器的防火墙解决方案一个末端，并且IOS-XE路由器不支持。

或者

2. 从IOS路由器去除NAT NVI配置并且运用正常里面/外部NAT配置。

> **提示**：另一个可能的解决方法是保留NAT NVI被配置在路由器和去除ZBF配置，然后运用在其他安全设备的必需的安全策略以安全功能。

相关Bug

CSCsh12490区域防火墙和NVI NAT不兼容

CSCek35625 NVI和FW互通性增进

CSCvf17266 DOCS ：ZBF配置指南缺少限制与NAT NVI关连

Related Information

- NAT虚拟接口
- 安全配置指南：基于区域的策略防火墙， Cisco IOS Release 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