配置NAT NVI時，排除基於IOS區域的策略防火牆檢查問題

目錄

簡介

本檔案介紹在Cisco IOS路由器中設定IOS區域型防火牆(ZBF)與網路位址轉譯虛擬介面(NAT NVI)時發生的檢查問題。

本文的主要目的是解釋為什麼會發生此問題，並提供在這種實施中允許所需的流量通過路由器所需的解決方案。

必要條件

需求

思科建議您瞭解以下主題：

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

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 整合式服務路由器(ISR G1)
- IOS 15M&T

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

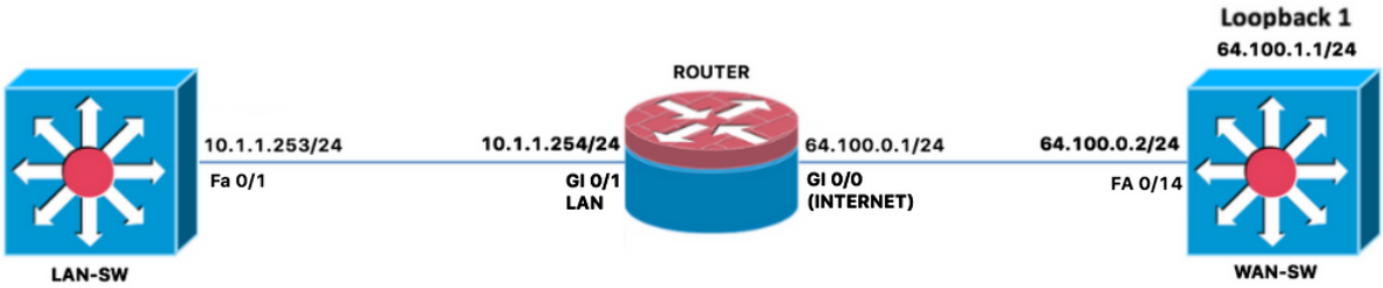
以下進一步詳細介紹什麼是NAT NVI以及如何在Cisco路由器上配置它：

網路地址轉換虛擬介面(NAT NVI)功能取消了將介面配置為NAT內部或NAT外部的要求。可以將介面配置為使用NAT或不使用NAT。NVI允許同一提供商邊緣(PE)路由器中的重疊VPN路由/轉發(VRF)之間的流量，以及重疊網路之間從內部到內部的流量。

NAT虛擬介面

問題：配置NAT NVI時，IOS基於區域的策略防火牆檢查問題

設定NAT NVI時，ZBF在檢查ICMP和TCP流量時遇到問題，以下為此問題的范例。如圖所示，確認ZBF與路由器NAT NVI一起設定時，不會檢查從內部到外部區域的TCP和ICMP流量。



已檢查應用於路由器ROUTER的實際ZBF配置，並確認以下內容：

```
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)
```

流量透過路由器**ROUTER**傳送時，已確認下一個結果：

將NAT配置與IP一起應用時,**nat inside和ipnat outside與ipnat inside一起分配給路由器介面** nat語句用於動態NAT，ping不是從 將**LAN-SW** 10.1.1.253 IP地址分配給64.100.1.1 在**WAN-SW交換機**上。

即使從路由器介面刪除ZBF區域後，流量仍然沒有通過路由器，而是開始通過 nat規則更改如下：

```
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
```

然後，在路由器介面中重新應用ZBF區域。

```
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
```

在路由器介面中重新應用ZBF區域後，確認ZBF開始顯示從OUTSIDE區域到自身區域的應答的丟棄系統日誌消息：

```
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
```

附註：從日誌消息中，您可以在第一個AUDIT_TRAIL日誌中確認TCP telnet會話最初從INSIDE發起到OUTSIDE區域的時間，但由於NAT NVI以及ZBF在位時處理流量的方式，返回流量錯誤地從OUTSIDE返回到自區域。

經確認，強制返回流量通過ZBF的唯一方法是應用允許返回流量從OUTSIDE區域進入自區域，此規則已應用於icmp和TCP流量作為測試目的，並且兩者均確認該規則工作正常，並且已根據需要允許返回流量。

> **附註**：在OUTSIDE區域和自區域之間的區域對中應用傳遞操作規則，不是針對此問題的推薦解決方案，這是因為返回流量極需由ZBF檢查並自動允許。

解決方案

ZBF不支援NAT NVI，此問題的唯一解決方案是應用CSCsh12490 Zone Firewall和NVI NAT do not interoperate bug中提到的任何解決方法，此處提供詳細信息：

1.刪除ZBF並改用傳統防火牆(CBAC)，這當然不是最佳選項，這是因為CBAC已經是IOS路由器生命週期終止的防火牆解決方案，而IOS-XE路由器不支援它。

或

2.從IOS路由器中刪除NAT NVI配置，改為應用正常的內部/外部NAT配置。

> **提示：**另一種可能的解決方法是保持路由器中配置NAT NVI並刪除ZBF配置，然後將所需的安全策略應用到具有安全功能的任何其他安全裝置中。

相關錯誤

CSCsh12490區域防火牆和NVI NAT不能互操作

CSCek35625 NVI和防火牆互操作性增強功能

CSCvf17266文檔：ZBF配置指南缺少與NAT NVI相關的限制

相關資訊

- NAT虛擬介面
- 安全配置指南：基於區域的策略防火牆，Cisco IOS版本15M&T
- Cisco IOS防火牆經典和基於區域的虛擬防火牆應用配置示例