# NAT NVIが設定されている場合のIOSゾーンベースポリシーファイアウォールインスペクションの問題のトラブルシューティング

## 内容



## 概要

このドキュメントでは、IOSゾーンベースファイアウォール(ZBF)がCisco IOSルータのネットワークアドレス変換仮想インターフェイス(NAT NVI)と一緒に設定されている場合に発生するインスペクションの問題について説明します。

このドキュメントの主な目的は、この問題が発生する理由を説明し、この種の実装で必要なトラフィックがルータを通過できるようにするために必要なソリューションを提供することです。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- IOSルータでのCisco ZBFの設定。
- IOSルータでのCisco NAT NVIの設定

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- サービス統合型ルータ(ISR G1)
- IOS 15M&T

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

# 背景説明

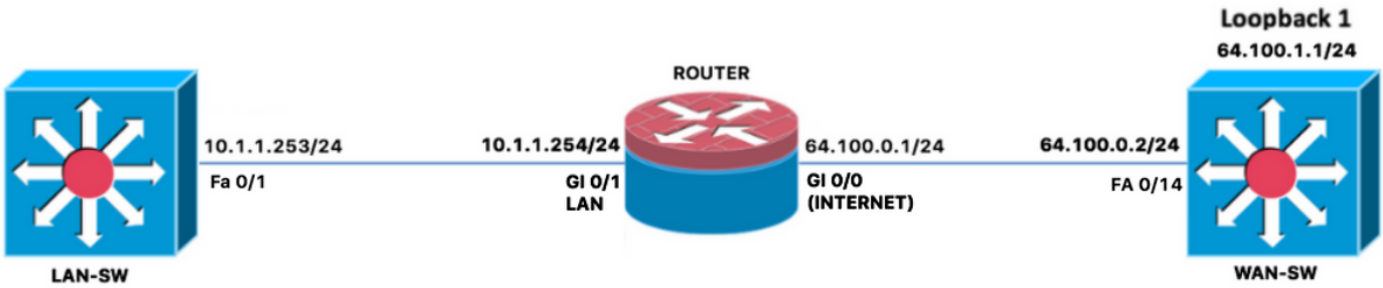
次に、NAT NVIの概要と、CiscoルータでのNAT NVIの設定方法の詳細を示します。

ネットワークアドレス変換仮想インターフェイス(NAT NVI)機能を使用すると、インターフェイスをNAT内部またはNAT外部として設定する必要がなくなります。インターフェイスは、NATを使用するように設定することも、NATを使用しないように設定することもできます。NVIを使用すると、同じプロバイダーエッジ(PE)ルータ内のオーバーラップするVPNルーティング/フォワーディング(VRF)間のトラフィックと、オーバーラップするネットワーク間の内部から内部へのトラフィックが許可されます。

NAT仮想インターフェイス

# 問題：NAT NVIが設定されている場合のIOSゾーンベースポリシーファイアウォールインスペクションの問題

ZBFにはICMPとTCPのトラフィックを検査する問題があります。この問題の例を示します。図に示すように、ルータROUTERでNAT NVIと共にTCPとICMPのトラフィックを内部ゾーンから外部検査に検査検査しない検査しません。




ルータROUTERに適用されている実際のZBF設定を確認し、次のことを確認した。

```
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)
```

トラフィックがルータROUTERを経由して送信されると、次の結果が確認されます。

ipnat insideおよびipnat outsideをルータインターフェイスに割り当て、ipnat inside ダイナミックNATに対するnat文で、pingが LAN-SW 10.1.1.253のIPアドレスを64.100.1.1に WAN-SWスイッチ

ZBFゾーンがルータインターフェイスから削除された後でも、トラフィックがルータを通過しなかった場合でも、その後に通過が開始されます NATルールは次のように変更されました。

```
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
```

その後、ルータインターフェイスでZBFゾーンを再適用します。

```
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
```

ZBFゾーンがルータインターフェイスに再適用されるとすぐに、ZBFがOUTSIDEゾーンからセルフゾーンへの応答のドロップsyslogメッセージを表示し始めたことを確認します。

```
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**：ログメッセージから、最初のAUDIT_TRAILログで、TCP telnetセッションが最初にINSIDEからOUTSIDEゾーンに開始されたときに確認できますが、NAT NVIとZBFが存在する場合のトラフィックの処理方法により、リターントラフィックがOUTSIDEからセルフゾーンに戻戻されました。

ZBFを強制的にリターントラフィックを通過させる唯一の方法は、OUTSIDEゾーンからセルフゾーンへのリターントラフィックを許可するパスアクションルールを適用し、このルールはテスト目的としてicmpとTCPトラフィックに適用されました。

> **注**：OUTSIDEゾーンとセルフゾーンの間のゾーンペアにパスアクションルールを適用するには、この問題の推奨ソリューションではありません。これは、リターントラフィックが検査され、ZBFによって自動的に許可されるために非常に必要であるためです。

# 解決方法

ZBFはNAT NVIをサポートしていません。この問題の唯一の解決策は、CSCsh12490 Zone FirewallとNVI NATが相互運用しないバグに記載されている回避策を適用することです。詳細を次に示します。

1. ZBFを取り外し、代わりにclassic firewall(CBAC)を適用します。これは当然、最善の選択肢ではありません。これは、CBACがIOSルータのサポート終了のファイアウォールソリューションであり、IOS-XEルータではサポートされていないためです。

または

2. IOSルータからNAT NVI設定を削除し、代わりに通常の内部/外部NAT設定を適用します。

> **ヒント**：もう1つの回避策として、ルータで設定されたNAT NVIを維持し、ZBF設定を削除し、セキュリティ機能を備えた他のセキュリティデバイスに必要なセキュリティポリシーを適用する方法があります。

# 関連バグ

CSCsh12490 Zone FirewallとNVI NATが相互運用しない

CSCek35625 NVIおよびFW相互運用性の拡張

CSCvf17266 DOC:ZBFコンフィギュレーションガイドにNAT NVIに関連する制限がない

## 関連情報

- NAT仮想インターフェイス
- セキュリティの設定ガイド：ゾーンベース ポリシー ファイアウォール、Cisco IOS リリース 15M&T
- Cisco IOS Firewall Classic とゾーンベースの仮想ファイアウォール アプリケーションの設定例