NAT NVI が設定されるとき IOS ゾーンによって基づくポリシー ファイアウォール インスペクション問題を解決して下さい

目次

概要

この資料は IOS ゾーン ベースのファイアウォール（ZBF）が Cisco IOS ルータの仮想インターフェイス（NAT NVI）とともにネットワーク アドレス変換（NAT）設定されるとき起こるインスペクション問題を記述したものです。

この資料の主要な意図がこの問題が説明することなぜ起こる、パススルーに必須トラフィックにこの種類の実装かのルータを与えるために必要なソリューションを与えます。

前提条件

要件

次の項目に関する知識が推奨されます。

- IOS ルータの Cisco ZBF 設定。
- IOS ルータの Cisco NAT NVI 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くものです。

- 統合サービス ルータ（ISR G1）
- IOS 15M&T

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響につい

て確実に理解しておく必要があります。

背景説明

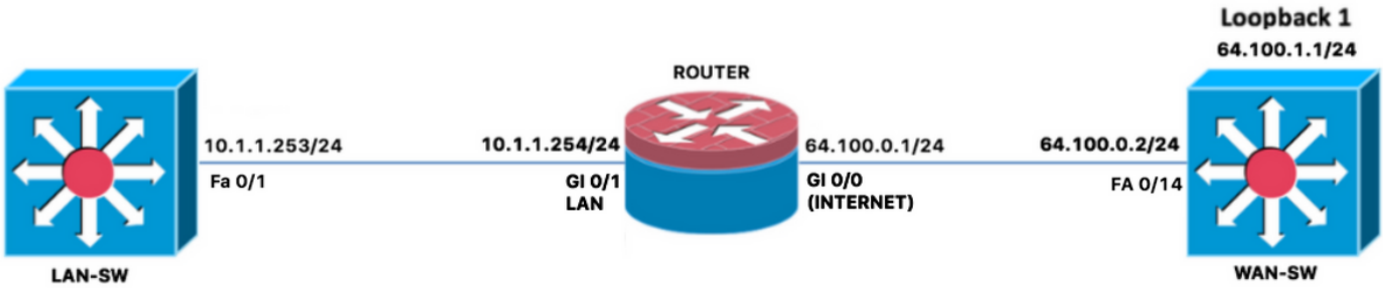
であるもの NAT NVI がおよび Ciscoルータでそれを設定する方法ここににについての更に詳しい情報を:

ネットワーク アドレス変換 (NAT) 仮想インターフェイス (NAT NVI) 機能は内部 NAT か NAT でインターフェイスを外部で設定するために要件を取除きます。 インターフェイスは NAT を使用するか、または NAT を使用しないために設定することができます。 NVI は (VRF)、およびオーバーラップ ネットワーク間の内部にトラフィックを同じ Provider Edge （ PE ）ルータで VPN Routing/Forwarding (VRF) ARP エントリ サポート オーバーラップされる間の内側からトラフィック可能にします。

NAT 仮想インターフェイス

問題： NAT NVI が設定される場合の IOS ゾーン ベースのポリシー ファイアウォール インスペクション問題

NAT NVI が設定されるとき ZBF に ICMP および TCPトラフィックを点検する問題が、ここにこの問題の例あります。 それは内部から外部ゾーンへの ZBF がイメージに示すようにルータ **ルータ**の NAT NVI とともに設定されるとき TCP および ICMP トラフィック点検されません確認されます。



ルータ **ルータ**に適用された実際の ZBF 設定をチェックし、次を確認しました:

```
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 **ルータ**を通して送信 される時、次の結果確認される:

NAT 設定が**内部**およびルータ インターフェイスに割り当てられた ipnat **外部** ipnat と適用されたときにダイナミック NAT のための NAT 文**の中の** ipnat とともに、ping は **LAN-SW** IP アドレス 10.1.1.253 から **WAN-SW** スイッチの 64.100.1.1 への渡りませんでした。

ZBF ゾーンがルータ インターフェイスから取除かれた後でさえも、トラフィックはパススルーに次の通り NAT ルールが変更された後パススルー ルータ、それ開始しました:

```
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
```

これの後、ルータ インターフェイスの ZBF ゾーン再適用される。

```
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 インターフェイスで再適用されたらすぐ、ZBF 外部ゾーンからの自己ゾーンへの応答のためのドロップする syslog メッセージを表示し始めました確認された:

```
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、TCP Telnetセッションが内部から外部ゾーンへの最初に始められるが、一方ではリターントラフィックは外部から ZBF が時トラフィックを処理する方法および NAT NVI による自己ゾーンへの ZBF に不正確に戻りましたとき最初の AUDIT_TRAIL ログで確認できます。

それは確認されます、パススルーにリターントラフィックを強制する唯一の方法は ZBF 外部ゾーンから自己ゾーンにリターントラフィックを許可するパス操作ルールを適用することですそれがそれ確認された両方のためのテストの目的がおよびうまく働き、リターントラフィックを要求に応じて可能にしたと同時にこのルールは icmp および TCPトラフィックに適用しました。

> **注:** 外部ゾーンと自己ゾーン間のゾーン ペアのパス操作ルールを適用するために、この問題のための推奨される ソリューションではないです、リターントラフィックが ZBF によって点検され、自動的に割り当てられて得ることができるように非常に必要となるこれはという理由によります。

解決策

ZBF は NAT NVI を、この問題のための唯一のソリューションの CSCsh12490 ゾーン ファイアウォールで述べられる回避策適用することですサポートしないし、NVI NAT は不具合を、ここに詳細相互運用しません:

1. ZBF を取除き、CBAC が IOS ルータのためのライフ ファイアウォール ソリューションの既に終わりであり、IOS ルータでサポートされない当然ない最もよいオプションであるこれによってがという理由による標準的なファイアウォール (CBAC) を代りに適用すれば。

または

2. NAT NVI 設定を IOS ルータから取除き、標準内部/外部 NAT 設定を代りに適用して下さい。

> **ヒント**： もう一つの可能性のある回避策は NAT NVI を設定してルータでおき、ZBF 設定を取除くことそしてセキュリティ機能の他のどの安全 装置の必須セキュリティポリシーも適用します。

関連バグ

CSCsh12490 ゾーン ファイアウォールおよび NVI NAT は相互運用しません

CSCek35625 NVI および FW 相互運用性機能拡張

CSCvf17266 DOCS: ZBF コンフィギュレーション ガイド抜けた制限は NAT NVI に関連していました

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