# Fehlerbehebung bei Problemen mit der IOS Zone-basierten Firewall-Inspektion bei der Konfiguration der NAT NVI

## Inhalt



## Einführung

Dieses Dokument beschreibt ein Inspektionsproblem, das auftritt, wenn die IOS Zone-Based Firewall (ZBF) zusammen mit der Network Address Translation Virtual Interface (NAT NVI) in einem Cisco IOS-Router konfiguriert wird.

In diesem Dokument wird in erster Linie erläutert, warum dieses Problem auftritt, und es wird Ihnen die Lösung bereitgestellt, die erforderlich ist, damit der erforderliche Datenverkehr bei dieser Implementierung durch den Router geleitet werden kann.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ZBF-Konfiguration in IOS-Routern.
- Cisco NAT NVI-Konfiguration in IOS-Routern.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Integrated Services Router (ISR G1)
- IOS 15M&T

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

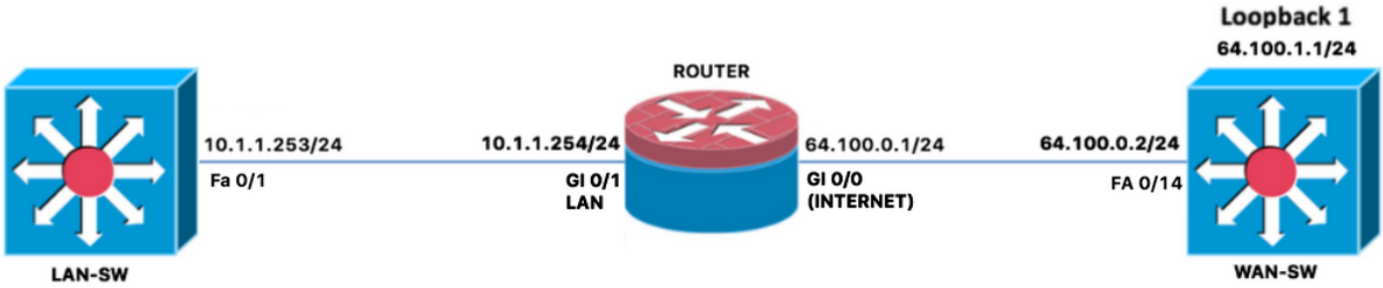
Hier finden Sie weitere Informationen zu NAT NVI und dessen Konfiguration auf den Cisco Routern:

Mit der Network Address Translation Virtual Interface (NAT NVI)-Funktion ist es nicht mehr erforderlich, eine Schnittstelle als NAT innerhalb oder außerhalb zu konfigurieren. Eine Schnittstelle kann so konfiguriert werden, dass sie NAT verwendet oder NAT nicht verwendet. Die NVI ermöglicht den Datenverkehr zwischen überlappenden VPN Routing/Forwarding (VRFs) im selben Provider Edge (PE)-Router und dem Datenverkehr zwischen internen und überlappenden Netzwerken.

Virtuelle NAT-Schnittstelle

## Problem: IOS Zone-Based Policy Firewall Inspection-Probleme bei der Konfiguration von NAT NVI

Das ZBF hat Probleme bei der Überprüfung von ICMP- und TCP-Datenverkehr, wenn NAT NVI konfiguriert ist. Hier ein Beispiel für dieses Problem. Es wird bestätigt, dass der TCP- und ICMP-Datenverkehr von innen nach außen nicht überprüft wird, wenn das ZBF zusammen mit NAT NVI im Router-**ROUTER** konfiguriert ist, wie im Bild gezeigt.




Die tatsächliche ZBF-Konfiguration für den Router-**ROUTER** überprüft und Folgendes bestätigt:

```
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)
```

Wenn Datenverkehr über den Router-**ROUTER** gesendet wird, wurden die nächsten Ergebnisse bestätigt:

Bei Anwendung der NAT-Konfiguration mit der **IPnat inside und ipnat outside assigned to the router interfaces, with the ipnat inside** nat-Anweisung für die dynamische NAT; die Pings wurden nicht übertragen von die **LAN-SW** 10.1.1.253 IP-Adresse an 64.100.1.1 auf dem **WAN-SW-**Switch.

Selbst nachdem die ZBF-Zonen von den Routerschnittstellen entfernt wurden, durchlief der Datenverkehr nicht den Router, sondern wurde danach weitergeleitet. Die NAT-Regel wurde wie folgt geändert:

```
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
```

Danach werden die ZBF-Zonen an den Routerschnittstellen erneut angewendet.

```
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
```

Sobald die ZBF-Zonen an den Routerschnittstellen erneut angewendet wurden, bestätigte das ZBF, dass die Syslog-Meldungen für die Antworten der OUTSIDE-Zone auf die Selbstzone angezeigt wurden:

```
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
```

> **Hinweis**: Aus den Protokollmeldungen können Sie im ersten AUDIT_TRAIL-Protokoll bestätigen, wann die TCP-Telnet-Sitzung zuerst von der INSIDE zur OUTSIDE-Zone initiiert wird, aber dann kam der Datenrückverkehr fälschlicherweise von der OUTSIDE zur Selbstzone zurück, da die NAT NVI verwendet wurde und wie der Datenverkehr bei der ZBF-Einrichtung verarbeitet wird.

Es wird bestätigt, dass die einzige Möglichkeit, den Rückverkehr durch das ZBF zu erzwingen, darin besteht, eine Pass-Action-Regel anzuwenden, die den Rückverkehr aus der OUTSIDE-Zone zur Selbstzone zulässt. Diese Regel wurde für den ICMP- und TCP-Datenverkehr als Testzwecke angewendet und sowohl für die Bestätigung als auch für die Bestätigung, dass er ordnungsgemäß funktionierte und den Rückverkehr wie erforderlich erlaubte.

> **Hinweis**: Die Anwendung einer Pass-Action-Regel im Zonenpaar zwischen der OUTSIDE-Zone und der Selbstzone ist keine empfohlene Lösung für dieses Problem, da es sehr wichtig ist, dass der Rückverkehr überprüft und automatisch vom ZBF zugelassen wird.

# Lösung

Das ZBF unterstützt NAT NVI nicht. Die einzige Lösung für dieses Problem besteht darin, eine der im CSCsh12490 Zone Firewall und NVI NAT genannten Workarounds anzuwenden, die nicht kompatibel sind. Hier einige Details:

1. Entfernen Sie die ZBF, und wenden Sie stattdessen die klassische Firewall (CBAC) an. Dies ist natürlich nicht die beste Option, da CBAC bereits eine End-of-Life-Firewall-Lösung für die IOS-Router ist und von den IOS-XE-Routern nicht unterstützt wird.

ODER

2. Entfernen Sie die NAT NVI-Konfiguration vom IOS-Router, und wenden Sie stattdessen die normale interne/externe NAT-Konfiguration an.

> **Tipp**: Eine weitere mögliche Problemumgehung wäre, die NAT NVI im Router zu konfigurieren und die ZBF-Konfiguration zu entfernen und dann die erforderlichen Sicherheitsrichtlinien auf jedem anderen Sicherheitsgerät mit Sicherheitsfunktionen anzuwenden.

## Zugehörige Fehler

CSCsh12490 Zone Firewall und NVI NAT arbeiten nicht zusammen

CSCek35625 NVI- und FW-Interoperabilitätsverbesserungen

CSCvf17266 DOC: Fehlende Einschränkungen für NAT NVI im ZBF-Konfigurationsleitfaden

## Zugehörige Informationen

- Virtuelle NAT-Schnittstelle
- Leitfaden zur Sicherheitskonfiguration: Zonenbasierte Firewall, Cisco IOS-Version 15M&T
- Konfigurationsbeispiel für die klassische und zonenbasierte virtuelle Firewall der Cisco IOS Firewall