Dépanner les problèmes d'inspection du pare-feu de stratégie basé sur la zone IOS lors de la configuration de NAT NVI

Contenu

Introduction

Ce document décrit un problème d'inspection qui se produit lorsque le pare-feu basé sur une zone IOS (ZBF) est configuré avec l'interface virtuelle de traduction d'adresses de réseau (NAT NVI) dans un routeur Cisco IOS.

L'objectif principal de ce document est d'expliquer pourquoi ce problème se produit et de vous fournir la solution requise pour permettre au trafic requis de traverser le routeur dans ce type d'implémentation.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration ZBF Cisco dans les routeurs IOS.
- Configuration NVI NAT Cisco dans les routeurs IOS.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeurs à services intégrés (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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

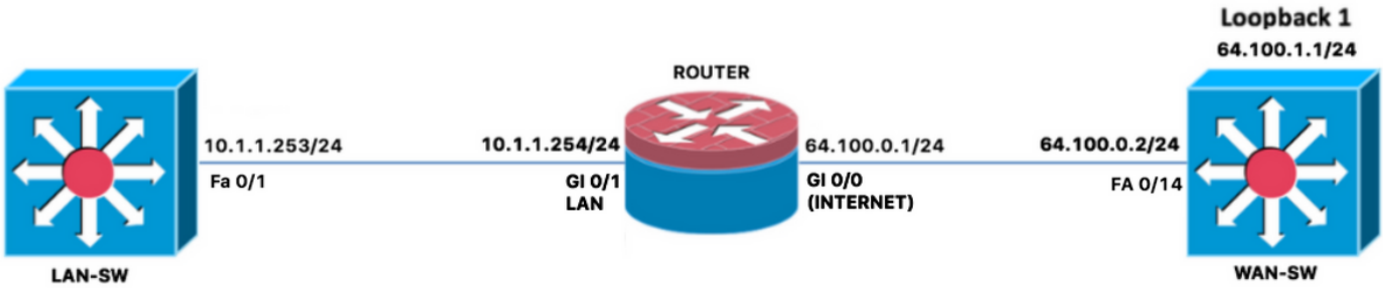
Pour plus d'informations sur NAT NVI et sur la façon de le configurer sur les routeurs Cisco, reportez-vous à la section suivante :

La fonction NAT NVI (Network Address Translation Virtual Interface) supprime la nécessité de configurer une interface en tant que NAT interne ou NAT externe. Une interface peut être configurée pour utiliser NAT ou non. NVI autorise le trafic entre les VRF (VPN Routing/Forwarding) qui se chevauchent sur le même routeur de périphérie du fournisseur (PE) et le trafic de l'intérieur vers l'intérieur entre les réseaux qui se chevauchent.

Interface virtuelle NAT

Problème : problèmes d'inspection du pare-feu de stratégie basé sur la zone IOS lors de la configuration de NAT NVI

Le ZBF rencontre des problèmes pour inspecter le trafic ICMP et TCP lorsque NAT NVI est configuré, voici un exemple de ce problème. Il est confirmé que le trafic TCP et ICMP n'est pas inspecté de l'intérieur vers l'extérieur lorsque le ZBF est configuré avec NAT NVI dans le **ROUTEUR** du routeur comme indiqué dans l'image.



Vérifiez la configuration ZBF réelle appliquée au **ROUTEUR** du routeur et confirmez ce qui suit :

```
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)
```

Lorsque le trafic est envoyé via le **ROUTEUR** du routeur, a confirmé les résultats suivants :

Lorsque la configuration NAT a été appliquée avec l'**adresse ipnat inside et ipnat outside affectés aux interfaces du routeur, ainsi que l'ipnat inside** instruction nat pour la NAT dynamique, les requêtes ping n'ont pas été transmises de l'adresse IP **LAN-SW** 10.1.1.253 vers 64.100.1.1 sur le commutateur **WAN-SW**.

Même après que les zones ZBF ont été supprimées des interfaces du routeur, le trafic n'a pas traversé le routeur, il a commencé à passer après la règle NAT a été modifiée comme suit :

```
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
```

Après cela, réappliquez les zones ZBF dans les interfaces du routeur.

```
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
```

Dès que les zones ZBF ont été réappliquées dans les interfaces du routeur, a confirmé que le ZBF a commencé à afficher les messages syslog de suppression pour les réponses de la zone OUTSIDE à la zone auto :

```
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**: À partir des messages du journal, vous pouvez confirmer dans le premier journal AUDIT_TRAIL lorsque la session Telnet TCP est initiée pour la première fois de la zone INSIDE à la zone OUTSIDE, mais ensuite le trafic de retour est revenu à tort au ZBF de la zone OUTSIDE à la zone auto en raison de la NAT NVI et de la manière dont il traite le trafic lorsque le ZBF est en place.

Il est confirmé, la seule façon de forcer le trafic de retour à passer par le ZBF est d'appliquer une règle d'action de passage pour autoriser le trafic de retour de la zone EXTSIDE à l'auto-zone, cette règle a été appliquée pour le trafic icmp et TCP à des fins de test et pour les deux il a été confirmé qu'il fonctionnait bien et a permis le trafic de retour comme requis.

> **Note**: L'application d'une règle d'action de passage dans la paire de zones entre la zone EXTSIDE et la zone auto n'est pas recommandée pour résoudre ce problème, car il est très nécessaire que le trafic de retour soit inspecté et automatiquement autorisé par le ZBF.

Solution

Le ZBF ne prend pas en charge NAT NVI, la seule solution à ce problème est d'appliquer les solutions de contournement mentionnées dans le pare-feu de zone CSCsh12490 et le bogue NAT NVI n'interopèrent pas, ici les détails :

1. Supprimez le ZBF et appliquez le pare-feu classique (CBAC) à la place, ce qui n'est bien sûr pas la meilleure option, car le CBAC est une solution de pare-feu de fin de vie pour les routeurs IOS et n'est pas pris en charge sur les routeurs IOS-XE.

OU

2. Supprimez la configuration NAT NVI du routeur IOS et appliquez la configuration NAT interne/externe normale à la place.

> **Astuce** : Une autre solution possible consisterait à conserver la NAT NVI configurée dans le routeur et à supprimer la configuration ZBF, puis à appliquer les stratégies de sécurité requises sur tout autre périphérique de sécurité doté de fonctionnalités de sécurité.

Bogues associés

Le pare-feu de zone CSCsh12490 et la NAT NVI ne fonctionnent pas

CSCek35625 Améliorations de l'interopérabilité NVI et FW

CSCvf17266 DOC : Guide de configuration ZBF : restrictions manquantes liées à NAT NVI

Informations connexes

- Interface virtuelle NAT
- Guide de configuration de la sécurité : Pare-feu de stratégie basé sur les zones, Cisco IOS version 15M&T
- Exemple de configuration d'une application de pare-feu virtuel basé sur la zone et de pare-feu Cisco IOS classique