Resolución de Problemas de Inspección de Firewall de Política Basada en Zona IOS cuando NAT NVI está Configurado

Contenido

Introducción

Este documento describe un problema de inspección que ocurre cuando el firewall basado en zonas (ZBF) IOS se configura junto con la interfaz virtual de traducción de direcciones de red (NAT NVI) en un router Cisco IOS.

La intención principal de este documento es explicar por qué ocurre este problema y proporcionarle la solución necesaria para permitir que el tráfico requerido pase a través del router en este tipo de implementación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Cisco ZBF en routers IOS.
- Configuración NAT NVI de Cisco en routers IOS.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers de servicios integrados (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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

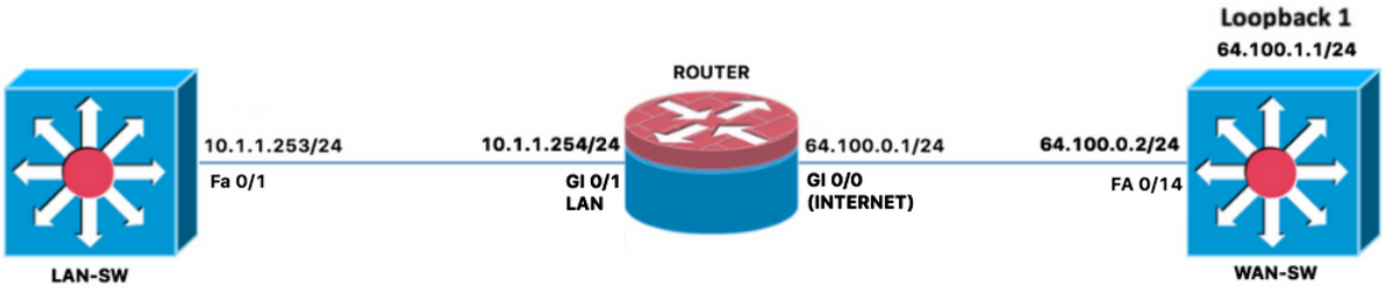
Aquí encontrará más detalles sobre qué es NAT NVI y cómo configurarlo en los routers de Cisco:

La función Network Address Translation Virtual Interface (NAT NVI) elimina el requisito de configurar una interfaz como NAT interna o NAT externa. Se puede configurar una interfaz para que use o no NAT. NVI permite el tráfico entre el routing/reenvío de VPN superpuestos (VRF) en el mismo router de borde del proveedor (PE) y el tráfico desde el interior hasta el interior entre redes superpuestas.

Interfaz virtual NAT

Problema: Problemas de Inspección de Firewall de Política Basada en Zona de IOS cuando NAT NVI está Configurado

El ZBF tiene problemas para inspeccionar el tráfico ICMP y TCP cuando se configura NAT NVI, aquí un ejemplo de este problema. Se confirma que el tráfico TCP e ICMP no se inspecciona desde el interior a las zonas exteriores cuando el ZBF se configura junto con NAT NVI en el **ROUTER** del router como se muestra en la imagen.



Verificó la configuración ZBF real aplicada al router **ROUTER** y confirmó lo siguiente:

```
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)
```

Cuando se envía tráfico a través del router **ROUTER**, se confirman los siguientes resultados:

Cuando se aplicó la configuración NAT con la **ipnat inside e ipnat outside asignados a las interfaces del router, junto con el ipnat inside** nat para la NAT dinámica, los pings no pasaron la dirección IP **LAN-SW** 10.1.1.253 a 64.100.1.1 en el switch **WAN-SW**.

Incluso después de que las zonas ZBF fueron eliminadas de las interfaces del router, el tráfico no pasó a través del router, comenzó a pasar después la regla NAT se modificó de la siguiente manera:

```
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
```

Después de esto, se volvieron a aplicar las zonas ZBF en las interfaces del router.

```
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
```

Tan pronto como se volvieron a aplicar las zonas ZBF en las interfaces del router, se confirmó que el ZBF comenzó a mostrar los mensajes de syslog de descarte para las respuestas de la zona EXTERNA a la zona autónoma:

```
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
```

> **Nota:** Desde los mensajes de registro, puede confirmar en el primer registro AUDIT_TRAIL cuando la sesión Telnet TCP se inicia por primera vez desde el interior a la zona EXTERNA, pero luego el tráfico de retorno regresó erróneamente al ZBF desde el exterior a la zona autónoma debido al NAT NVI y la forma en que procesa el tráfico cuando el ZBF está en su lugar.

Se confirma, la única manera de forzar el paso del tráfico de retorno a través del ZBF es aplicar una regla de acción de paso para permitir el tráfico de retorno desde la zona EXTERNA a la zona autónoma, esta regla se aplicó para el tráfico icmp y TCP como propósitos de prueba y para ambos se confirmó que funcionó bien y permitió el tráfico de retorno según se requería.

> **Nota:** Para aplicar una regla de acción de paso en el par de zonas entre la zona EXTERNA y la zona autónoma, no es una solución recomendada para este problema, esto se debe a que es muy necesario que el tráfico de retorno sea inspeccionado y permitido automáticamente por el ZBF.

Solución

El ZBF no soporta NAT NVI, la única solución para este problema es aplicar cualquiera de las soluciones mencionadas en el CSCsh12490 Zone Firewall y NVI NAT no interoperan bug, aquí los detalles:

1. Quite el ZBF y aplique el firewall clásico (CBAC) en su lugar, lo que por supuesto no es la mejor opción y esto se debe a que el CBAC es una solución de firewall de fin de vida útil para los routers IOS y no es compatible con los routers IOS-XE.

O

2. Quite la configuración NAT NVI del router IOS y aplique la configuración normal NAT interna/externa en su lugar.

> **Consejo:** Otra solución alternativa posible sería mantener el NAT NVI configurado en el router y quitar la configuración ZBF y, a continuación, aplicar las políticas de seguridad necesarias en cualquier otro dispositivo de seguridad con capacidades de seguridad.

Errores relacionados

CSCsh12490 Zone Firewall y NVI NAT no interoperan

Mejoras en la interoperabilidad CSCek35625 NVI y FW

CSCvf17266 DOC: Guía de configuración de ZBF que carece de restricciones relacionadas con NAT NVI

Información Relacionada

- Interfaz virtual NAT
- Guía de configuración de seguridad: Firewall de políticas basado en zonas, Cisco IOS Release 15M&T
- Ejemplo de Configuración de Aplicación de Firewall Virtual Clásico y Basado en Zona de Cisco IOS Firewall