Probleemoplossing voor IOS Zone-gebaseerde beleidsfirewallinspectie wanneer NAT NVI is ingesteld

Inhoud

Inleiding

Dit document beschrijft een inspectieprobleem dat zich voordoet wanneer de IOS Zone-Based Firewall (ZBF) in een Cisco IOS-router is ingesteld samen met Network adresomzetting virtuele interface (NAT NVI).

De belangrijkste bedoeling van dit document is om uit te leggen waarom dit probleem zich voordoet en u de oplossing te bieden die nodig is om het vereiste verkeer door de router te laten lopen in dit soort implementatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ZBF-configuratie in IOS-routers.
- Cisco NAT NVI-configuratie in IOS-routers.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Geïntegreerde services routers (ISR G1)
- IOS 15M&T

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

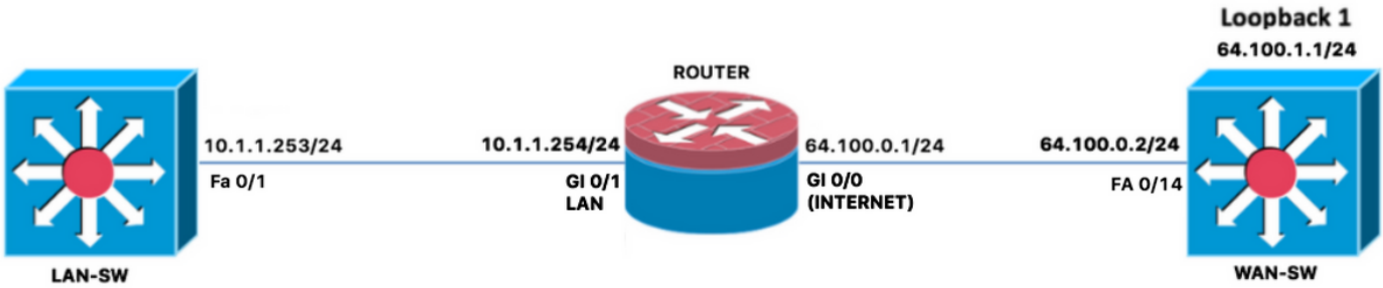
Hier vindt u meer informatie over wat NAT NVI is en hoe u deze op de Cisco-routers kunt configureren:

De functie Network Address Translation Virtual Interface (NAT NVI) verwijdert de noodzaak om een interface te configureren als NAT binnen of NAT buiten. Een interface kan worden ingesteld om NAT te gebruiken of niet NAT te gebruiken. NVI staat verkeer tussen overlappende VPN Routing/Forwarding (VRF's) in de zelfde PE-router (Provider Edge) en verkeer van binnen naar binnen tussen overlappende netwerken toe.

NAT virtuele interface

Probleem: IOS Zone-Based Policy Firewall Inspection Problemen bij configuratie NAT NVI

De ZBF heeft problemen om ICMP- en TCP-verkeer te inspecteren wanneer NAT NVI is geconfigureerd, hier een voorbeeld van dit probleem. Er wordt bevestigd dat het TCP- en ICMP-verkeer niet van de binnenkant naar de externe zones wordt geïnspecteerd wanneer de ZBF samen met NAT NVI is geconfigureerd in de router **ROUTER** zoals in de afbeelding wordt getoond.



Controleer de eigenlijke ZBF-configuratie die op de router **ROUTER** is toegepast en bevestigde het volgende:

```
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)
```

Wanneer het verkeer door de router **ROUTER** wordt verzonden, bevestigde de volgende resultaten:

Wanneer de NAT-configuratie werd toegepast met de **ipnat binnen en ipnat buiten toegewezen aan de routerinterfaces, samen met de ingang binnen** Geen verklaring voor de dynamische NAT, de pings waren niet van het **LAN-SW** 10.1.1.253 IP-adres naar 64.10.1.1 via de **WAN-SW**-schakelaar.

Zelfs nadat de ZBF zones van de router interfaces werden verwijderd, ging het verkeer niet door de router, het begon door te geven na de NAT-regel werd als volgt gewijzigd:

```
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
```

Nadat dit, pas de ZBF zones in de routerinterfaces opnieuw toe.

```
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
```

Zodra de ZBF-zones opnieuw werden toegepast in de routerinterfaces, bevestigde de ZBF dat de druppelberichten voor de antwoorden van de BUITENzone op de zelfzone werden weergegeven:

```
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
```

> Opmerking: Uit de logberichten kunt u in het eerste AUDIT_TRAIL-logbestand bevestigen wanneer de TCP-telnetsessie voor het eerst wordt gestart vanuit INSIDE naar de BUITENzone, maar toen kwam het retourverkeer onterecht terug naar de ZBF vanuit de BUITENKANT naar de zelfzone vanwege de NAT-zone en de manier waarop het verkeer wordt verwerkt nadat de ZBF is geïnstalleerd.

De enige manier om het retourverkeer door de ZBF te laten passeren, is door middel van een "pass action"-regel die het retourverkeer van de BUITENzone naar de zelfzone mogelijk maakt, deze regel werd toegepast voor het icmp- en TCP-verkeer als testdoeleinden en voor beide werd bevestigd dat deze goed werkte en het retourverkeer naar wens mogelijk maakte.

> Opmerking: Een passageregel toepassen in het zonepaar tussen de BUITENzone en de zelfzone is geen aanbevolen oplossing voor dit probleem, omdat het zeer nodig is dat het retourverkeer wordt geïnspecteerd en automatisch door de ZBF wordt toegestaan.

Oplossing

De ZBF ondersteunt NAT NVI niet. De enige oplossing voor dit probleem is om een van de in de CSCsh12490 Zone Firewall en NVI NAT genoemde beperkingen op het gebruik van insecten toe te passen, hier zie je de details:

1. Verwijder de ZBF en pas in plaats daarvan de klassieke firewall (CBAC) toe, die natuurlijk niet de beste optie is en dit is omdat CBAC een reeds end-of-life firewalloplossing voor de IOS-routers is en niet op de IOS-XE routers wordt ondersteund.

OF

2. Verwijder de NAT NVI-configuratie van de IOS-router en pas in plaats daarvan de normale interne/externe NAT-configuratie toe.

> **Tip**: Een andere mogelijke oplossing is om de NAT NVI in de router geconfigureerd te houden en de ZBF-configuratie te verwijderen, dan het gewenste beveiligingsbeleid toe te passen op een ander beveiligingsapparaat met beveiligingsfuncties.

Verwante bellen

CSCsh12490 Zone firewall en NVI NAT werken niet samen

Verbeteringen in interoperabiliteit van CSC35625 NVI en FW

CSCvf17266 DOC: ZBF-configuratiehandleiding voor ontbrekende beperkingen in verband met NAT NVI

Gerelateerde informatie

- NAT virtuele interface
- Security configuratiegids: Zone-Based Policy Firewall, Cisco IOS release 15M&T
- Cisco IOS-configuratievoorbeeld voor cloudfirewall en Zone-gebaseerde virtuele firewall