Identificar e Solucionar Problemas de Inspeção de Firewall de Política Baseada em Zona IOS quando NAT NVI está Configurado

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Informações de Apoio
Problema: problemas de inspeção do firewall de política baseado em zona do IOS quando NAT NVI está configurado
Solução
Erros relacionados
Informações Relacionadas

Introduction

Este documento descreve um problema de inspeção que acontece quando o IOS Zone-Based Firewall (ZBF) é configurado juntamente com a Network Address Translation Virtual Interface (NAT NVI) em um roteador Cisco IOS.

A principal intenção deste documento é explicar por que esse problema acontece e fornecer a solução necessária para permitir que o tráfego necessário passe pelo roteador nesse tipo de implementação.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco ZBF em roteadores IOS.
- Configuração do Cisco NAT NVI em roteadores IOS.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteadores de serviços 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. Se a rede estiver

ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

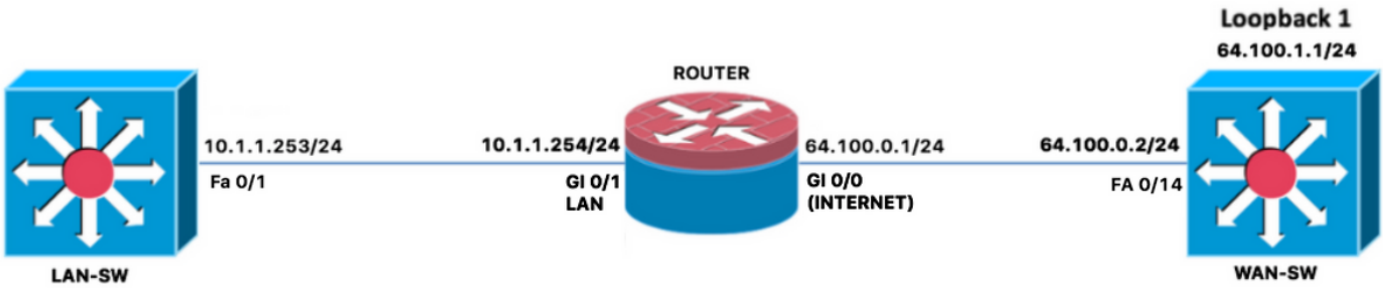
Aqui estão mais detalhes sobre o que é NAT NVI e como configurá-lo nos roteadores Cisco:

O recurso Network Address Translation Virtual Interface (NAT NVI) remove o requisito de configurar uma interface como NAT interno ou NAT externo. Uma interface pode ser configurada para usar NAT ou não usar NAT. O NVI permite o tráfego entre o Roteamento/Encaminhamento de VPN sobreposto (VRFs) no mesmo roteador de Borda do Provedor (PE) e o tráfego de dentro para dentro entre redes sobrepostas.

Interface virtual NAT

Problema: problemas de inspeção do firewall de política baseado em zona do IOS quando NAT NVI está configurado

O ZBF tem problemas para inspecionar o tráfego ICMP e TCP quando o NAT NVI está configurado, aqui está um exemplo desse problema. É confirmado que o tráfego TCP e ICMP não é inspecionado de dentro para fora quando o ZBF é configurado juntamente com NAT NVI no roteador **ROUTER**, como mostrado na imagem.



Verificada a configuração ZBF real aplicada ao roteador **ROUTER** e confirmada o seguinte:

```
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)
```

Quando o tráfego é enviado através do roteador **ROUTER**, confirmamos os próximos resultados:

Quando a configuração NAT foi aplicada com o **ipnat inside e ipnat outside atribuídos às interfaces do roteador, juntamente com o ipnat inside** instrução nat para o NAT dinâmico, os pings não passaram de o endereço IP **LAN-SW** 10.1.1.253 para 64.100.1.1 no switch **WAN-SW**.

Mesmo depois que as zonas ZBF foram removidas das interfaces do roteador, o tráfego não passou pelo roteador, ele começou a passar após a regra NAT foi alterada da seguinte maneira:

```
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
```

Depois disso, reaplicadas as zonas ZBF nas interfaces do roteador.

```
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
```

Assim que as zonas ZBF foram reaplicadas nas interfaces do roteador, confirmou que o ZBF começou a exibir as mensagens de queda do syslog para as respostas da zona EXTERNA para a autozona:

```
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**: A partir das mensagens de registro, você pode confirmar no primeiro registro AUDIT_TRAIL quando a sessão telnet do TCP é iniciada pela primeira vez da zona INTERNA para a EXTERNA, mas o tráfego de retorno errado voltou para o ZBF do EXTERIOR para a autozona devido ao NAT NVI e à maneira como ele processa o tráfego quando o ZBF está no lugar.

Confirmado, a única maneira de forçar o tráfego de retorno a passar pelo ZBF é aplicar uma regra de ação de passagem para permitir o tráfego de retorno da zona OUTSIDE para autozona, essa regra foi aplicada para o tráfego icmp e TCP como finalidade de teste e, para ambos, foi confirmado que funcionou bem e permitiu o tráfego de retorno conforme necessário.

> **Note**: Para aplicar uma regra de ação de passagem no par de zonas entre a zona EXTERNA e a zona de saída, não é uma solução recomendada para esse problema, isso ocorre porque é altamente necessário para que o tráfego de retorno seja inspecionado e automaticamente permitido pelo ZBF.

Solução

O ZBF não suporta NAT NVI, a única solução para esse problema é aplicar qualquer uma das soluções alternativas mencionadas no firewall de zona CSCsh12490 e NAT NVI não interoperam com bug, aqui os detalhes:

1. Remova o ZBF e aplique o firewall clássico (CBAC), que não é, obviamente, a melhor opção, porque o CBAC é uma solução de firewall já no fim da vida útil para os roteadores IOS e não é suportado nos roteadores IOS-XE.

OU

2. Remova a configuração NAT NVI do roteador IOS e aplique a configuração normal de NAT interno/externo.

> **Tip**: Outra solução possível seria manter o NAT NVI configurado no roteador e remover a configuração do ZBF, depois aplicar as políticas de segurança necessárias em qualquer outro dispositivo de segurança com recursos de segurança.

Erros relacionados

O firewall de zona CSCsh12490 e o NAT NVI não interoperam

Melhorias de interoperabilidade CSCek35625 NVI e FW

CSCvf17266 DOC: Guia de configuração ZBF sem restrições relacionadas ao NAT NVI

Informações Relacionadas

- Interface virtual NAT
- Guia de configuração de segurança: Firewall de política baseado em zona, Cisco IOS versão 15M&T
- Exemplo de configuração do aplicativo de firewall virtual baseado em zona e Clássico do Cisco IOS Firewall