Risoluzione dei problemi di ispezione del firewall per i criteri basati sulla zona IOS quando NAT NVI è configurato

Sommario

Introduzione

In questo documento viene descritto un problema di ispezione che si verifica quando IOS Zone-Based Firewall (ZBF) viene configurato insieme a Network Address Translation Virtual Interface (NAT NVI) in un router Cisco IOS.

Lo scopo principale di questo documento è spiegare il motivo per cui il problema si verifica e fornire la soluzione necessaria per consentire il passaggio del traffico richiesto attraverso il router in questo tipo di implementazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione Cisco ZBF in router IOS.
- Configurazione di Cisco NAT NVI nei router IOS.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

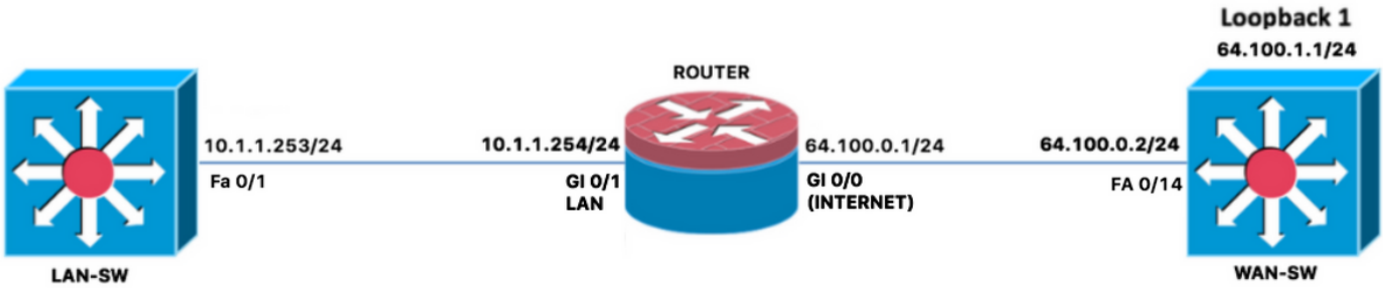
Ecco ulteriori dettagli su NAT NVI e su come configurarlo sui router Cisco:

La funzionalità NAT NVI (Network Address Translation Virtual Interface) elimina la necessità di configurare un'interfaccia come NAT interna o NAT esterna. Un'interfaccia può essere configurata per utilizzare o meno NAT. La tecnologia NVI consente il traffico tra VRF (VPN Routing/Forwarding) sovrapposti nello stesso router Provider Edge (PE) e il traffico dall'interno all'interno tra reti sovrapposte.

Interfaccia virtuale NAT

Problema: problemi di ispezione del firewall per i criteri basati sulla zona IOS quando NAT NVI è configurato

La ZBF ha problemi a ispezionare il traffico ICMP e TCP quando è configurato NAT NVI, qui un esempio di questo problema. È confermato che il traffico TCP e ICMP non viene ispezionato dall'interno verso le zone esterne quando la ZBF è configurata insieme a NAT NVI nel router **ROUTER**, come mostrato nell'immagine.



È stata verificata la configurazione ZBF applicata al router **ROUTER** e è stato confermato quanto segue:

```
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 il traffico viene inviato tramite il router **ROUTER**, confermare i risultati successivi:

Quando la configurazione NAT è stata applicata con il protocollo **ipnat inside e ipnat external assegnati alle interfacce del router, insieme all'ipnat inside** istruzione nat per il NAT dinamico, i ping non sono stati passati da l'indirizzo IP **LAN-SW** 10.1.1.253 su 64.100.1.1 sullo switch **WAN-SW**.

Anche dopo aver rimosso le zone ZBF dalle interfacce del router, il traffico non ha attraversato il router, ma ha iniziato a passare dopo la regola NAT è stata modificata come segue:

```
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
```

Quindi, riapplicare le zone ZBF nelle interfacce 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
```

Non appena le zone ZBF sono state riapplicate nelle interfacce del router, la conferma che ZBF ha iniziato a visualizzare i messaggi di syslog di drop per le risposte dalla zona ESTERNA alla zona interna:

```
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:** Dai messaggi di log, è possibile confermare nel primo log AUDIT_TRAIL quando la sessione telnet TCP viene avviata per la prima volta dall'interno verso l'esterno, ma poi il traffico di ritorno erroneamente è tornato allo ZBF dall'esterno verso l'interno a causa della NAT NVI e del modo in cui elabora il traffico quando lo ZBF è in posizione.

È confermato, l'unico modo per forzare il traffico di ritorno per passare attraverso la ZBF è applicare una regola di azione di superamento per consentire il traffico di ritorno dalla zona ESTERNA alla zona self-zone, questa regola è stata applicata per il traffico ICMP e TCP come scopo di test e per entrambi è stato confermato che ha funzionato bene e permesso il traffico di ritorno come richiesto.

> **Nota:** L'applicazione di una regola di azione pass nella coppia di zone tra la zona OUTSIDE e la zona self-zone non è una soluzione consigliata per questo problema, in quanto è fortemente richiesto per il traffico di ritorno per essere ispezionato e automaticamente consentito dalla ZBF.

Soluzione

Lo ZBF non supporta NAT NVI, l'unica soluzione per questo problema è applicare una delle soluzioni indicate in CSCsh12490 Zone Firewall e NVI NAT non interagiscono con il bug, qui i dettagli:

1. Rimuovere lo ZBF e applicare il firewall classico (CBAC), che ovviamente non è l'opzione migliore, in quanto la CBAC è una soluzione firewall già fuori uso per i router IOS e non è supportata sui router IOS-XE.

O

2. Rimuovere la configurazione NAT NVI dal router IOS e applicare la normale configurazione NAT interna/esterna.

> **Suggerimento**: Un'altra possibile soluzione potrebbe essere mantenere la NAT NVI configurata nel router e rimuovere la configurazione ZBF, quindi applicare i criteri di sicurezza richiesti in qualsiasi altro dispositivo di sicurezza con funzionalità di sicurezza.

Bug correlati

CSCsh12490 Zone Firewall e NVI NAT non interagiscono

Miglioramenti interoperabilità CSCek35625 NVI e FW

CSCvf17266 DOC: Nella guida alla configurazione di ZBF mancano le restrizioni relative a NAT NVI

Informazioni correlate

- Interfaccia virtuale NAT
- Guida alla configurazione della protezione: Policy Firewall basato su zone, Cisco IOS release 15M&T
- Esempio di configurazione di un'applicazione Cisco IOS Firewall classica e Virtual Firewall basata su zona