أستكشاف أخطاء فحص جدار الحماية المستند إلى منطقة IOS وإصلاحها عند تكوين NAT NVI

المحتويات

المقدمة

يصف هذا المستند مشكلة تفتيش تحدث عند تكوين جدار الحماية المستند إلى منطقة IOS (ZBF) مع الواجهة الظاهرية لترجمة عنوان الشبكة (NAT NVI) في موجه Cisco IOS.

الغرض الرئيسي من هذا المستند هو شرح سبب حدوث هذه المشكلة وتزويدك بالحل المطلوب للسماح لحركة المرور المطلوبة بالمرور عبر الموجه في هذا النوع من التنفيذ.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين Cisco ZBF في موجهات IOS.
- تكوين Cisco NAT NVI في موجهات IOS.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- موجهات الخدمات المتكاملة (ISR G1)
- IOS 15M&T

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

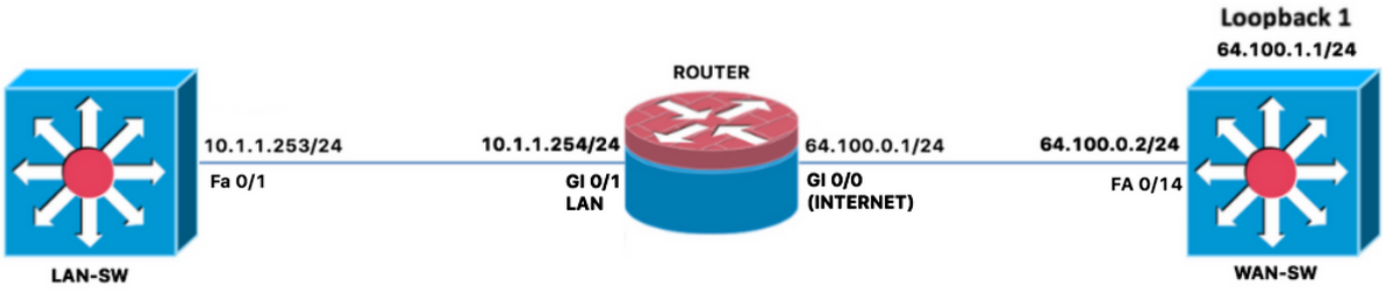
هنا المزيد من التفاصيل حول ما NAT NVI وكيف أن يشكل هو على ال cisco مسحاج تخديد:

ال شبكة عنوان ترجمة قارن فعلي (NAT NVI) يزيل سمة المتطلب أن يشكل قارن إما NAT داخلي وأ NAT خارجي. قارن يستطيع كنت شكلت أن يستعمل NAT وأ ال يستعمل NAT. يسمح NVI حركة مرور بين توجيه/إعادة توجيه VPN متداخل (VRFs) في نفس موجه حافة الموفر (PE)، وحركة مرور البيانات من الداخل إلى الداخل بين الشبكات المتداخلة.

[الواجهة الظاهرية NAT]

مشكلة: مشاكل فحص جدار الحماية المستند إلى منطقة IOS عند تكوين NAT NVI

يواجه ZBF مشاكل في فحص حركة مرور ICMP و TCP عند تكوين NAT NVI، هنا مثال على هذه المشكلة. تم تأكيد عدم فحص حركة مرور TCP و ICMP من الداخل إلى المناطق الخارجية عند تكوين ZBF مع NAT NVI في **الموجه** كما هو موضح في الصورة.



تحقق من تكوين ZBF الفعلي الذي تم تطبيقه على **الموجه** وأكد ما يلي:

```
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)
```

عند إرسال حركة المرور من خلال **المجوم**، تم تأكيد النتائج التالية:

عندما تقبط ال nat تشكيل مع ال **ipnat في الداخل وiNAT في الخارج مخصص لواجهات الموجه، مع الجزاء في الداخل** عبارة nat ل NAT حركي، ال تمر من ال **LAN-SW** 10.1.1.253 إلى عنوان 64.100.1.1 على محول **WAN-SW**.

حتى بعد إزالة مناطق ZBF من واجهات الموجه، لم تمر حركة المرور عبر الموجه، وبدأت في المرور بعد تم تغيير قاعدة NAT كما يلي:

```
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
```

بعد ذلك، قم بإعادة تطبيق مناطق ZBF في واجهات الموجه.

```
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
```

بمجرد إعادة تطبيق مناطق ZBF في واجهات الموجه، أكدت أن ZBF بدأ في عرض رسائل syslog للإفلات الخاصة بالردود من المنطقة الخارجية إلى المنطقة الذاتية:

```
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
```

> **ملاحظة**: من رسائل السجل، يمكنك التأكيد في سجل AUDIT_TRAIL الأول عندما يتم بدء جلسة عمل برنامج Telnet ل TCP أولا من الداخل إلى المنطقة الخارجية، ولكن بعد ذلك عادت حركة مرور الإرجاع بشكل خاطئ إلى ZBF من الخارج إلى المنطقة الذاتية بسبب NAT NVI والطريقة التي تعالج بها حركة مرور البيانات عندما يكون ZBF في موضعه.

تم تأكيد ذلك، الطريقة الوحيدة لإجبار حركة المرور العائدة على المرور عبر ZBF هي تطبيق قاعدة إجراء تمرير للسماح بحركة المرور العائدة من المنطقة الخارجية إلى المنطقة الذاتية، وقد تم تطبيق هذه القاعدة على حركة مرور ICMP و TCP كأغراض إختبار وللكليهما تم التأكد من أنها تعمل بشكل جيد وسمحت بحركة المرور العائدة كما هو مطلوب.

> **ملاحظة**: لا يعتبر تطبيق قاعدة إجراءات المرور في زوج إجراءات المرور في المنطقة بين المنطقة الخارجية والمنطقة الذاتية حلا مستحسنا لهذه المشكلة، وذلك لأنه مطلوب بشدة لمعاينة حركة المرور العائدة والسماح بها تلقائيا بواسطة ZBF.

الحل

لا يدعم بروتوكول ZBF NAT NVI، والحل الوحيد لهذه المشكلة هو تطبيق أي من الحلول المذكورة في [جدار حماية منطقة CSCsh12490 والموقع NVI NAT ليغشتب](#) الخطأ، انه التفاصيل:

1. قم بإزالة بروتوكول ZBF وتطبيق جدار الحماية التقليدي (CBAC) بدلا من ذلك، وهو بالطبع ليس الخيار الأفضل، وهذا يرجع لأن CBAC هو حل جدار حماية نهاية الحياة بالفعل لموجهات IOS وهو غير مدعوم على موجهات IOS-XE.

أو

2. قم بإزالة تكوين NAT NVI من موجه IOS وطبق تكوين NAT الداخلي/الخارجي العادي بدلا من ذلك.

> **تلميح**: هناك حل بديل آخر ممكن وهو الحفاظ على تكوين NAT NVI في الموجه وإزالة تكوين ZBF، ثم تطبيق سياسات الأمان المطلوبة في أي جهاز أمان آخر بقدرات أمان.

الأخطاء ذات الصلة

لا يتفاعل جدار حماية المنطقة [CSCsh](#)12490 و NVI NAT

تحسينات قابلية التشغيل البيني [ل CSCek](#)35625 NVI و FW

[CSCvf17266](#) DOC: دليل تكوين ZBF يفتقد قيود متعلقة ب NAT NVI

معلومات ذات صلة

- [الواجهة الظاهرية NAT](#)

- دليل تكوين الأمان: جدار حماية السياسات القائمة على المناطق، الإصدار 15M&T من Cisco IOS
- مثال تكوين تطبيق جدار الحماية الظاهري Cisco IOS Firewall التقليدي المستند إلى المناطق

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).