أستكشاف أخطاء الاتصالات وإصلاحها من ASA و PIX الخالل

المحتويات

المقدمة

يقدم هذا المستند أفكار واقتراحات أستكشاف الأخطاء وإصلاحها خاصة عند إستخدام جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco ASA 5500 Series وجهاز الأمان Cisco PIX 500 Series Security Appliance.
وفي كثير من الأحيان، عندما تنقطع التطبيقات أو مصادر الشبكة أو لا تكون متاحة، تميل جدران الحماية (PIX أو ASA) إلى أن تكون هدفا رئيسيا ويلقى عليها اللوم باعتبارها السبب في حالات انقطاع التيار. مع بعض الاختبار على ASA أو PIX، يمكن للمسؤول تحديد ما إذا كان ASA/PIX يتسبب في المشكلة أم لا.

ارجع إلى PIX/ASA: إنشاء الاتصال واستكشاف أخطائه وإصلاحها من خلال جهاز أمان Cisco لمعرفة المزيد حول أستكشاف الأخطاء وإصلاحها المتعلقة بالواجهة على أجهزة أمان Cisco.

ملاحظة: يركز هذا المستند على ASA و PIX. بمجرد اكتمال أستكشاف الأخطاء وإصلاحها على ASA أو PIX، قد يكون من الضروري أستكشاف أخطاء الأجهزة الأخرى وإصلاحها (الموجهات والمحولات والخوادم وما إلى ذلك).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco ASA 5510 مع OS 7.2.1 و 8.3.

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

المنتجات ذات الصلة

هذا وثيقة يستطيع أيضا كنت استعملت مع هذا جهاز وبرمجية صيغة:

- ASA و PIX OS 7.0 و 7.1 و 8.3 والإصدارات اللاحقة
- وحدة خدمات جدار الحماية (FWSM) 2.2 و 2.3 و 3.1

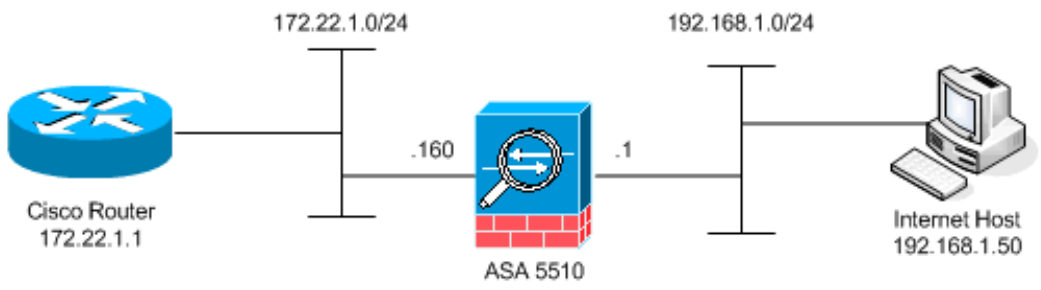
ملاحظة: يمكن أن تختلف الأوامر المحددة وبناء الجملة بين إصدارات البرامج.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يفترض المثال أن ASA أو PIX قيد الإنتاج. يمكن أن يكون تكوين ASA/PIX بسيطا نسبيا (50 خطا فقط من التكوين) أو معقدا (من مئات إلى آلاف خطوط التكوين). يمكن أن يكون المستخدمون (العملاء) أو الخوادم على شبكة آمنة (في الداخل) أو شبكة غير آمنة (DMZ أو خارجها).



يبدأ ال ASA مع هذا تشكيل. ويقصد بالتكوين أن يعطي المختبر نقطة مرجعية.

التكوين الأولي ASA

```
ciscoasa#show running-config
Saved :
:
(ASA Version 7.2(1
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/2
nameif dmz
security-level 50
ip address 10.1.1.1 255.255.255.0
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list outside_acl extended permit tcp any host
172.22.1.254 eq www
access-list inside_acl extended permit icmp 192.168.1.0
255.255.255.0 any
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq www
access-list inside_acl extended permit tcp 192.168.1.0
255.255.255.0 any eq telnet
pager lines 24
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no asdm history enable
arp timeout 14400
global (outside) 1 172.22.1.253
nat (inside) 1 192.168.1.0 255.255.255.0


The above NAT statements are replaced by the ---!
following statements !--- for ASA 8.3 and later. object
network obj-192.168.1.0 subnet 192.168.1.0 255.255.255.0
nat (inside,outside) dynamic 172.22.1.253 static
(inside,outside) 192.168.1.100 172.22.1.254 netmask
255.255.255.255 !--- The above Static NAT statement is
replaced by the following statements !--- for ASA 8.3
and later. object network obj-172.22.1.254 host
172.22.1.254 nat (inside,outside) static 192.168.1.100
access-group outside_acl in interface outside access-
group inside_acl in interface inside timeout xlate
```

```
    3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
  h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
       0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
    disconnect 0:02:00 timeout uauth 0:05:00 absolute no
 snmp-server location no snmp-server contact snmp-server
        enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
         0 ! class-map inspection_default match default-
      inspection-traffic ! ! policy-map type inspect dns
    preset_dns_map parameters message-length maximum 512
       policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
    inspect h323 ras inspect netbios inspect rsh inspect
rtsp inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
     policy global_policy global prompt hostname context
   Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

المشكلة

يتصل المستخدم بقسم تقنية المعلومات ويبلغ عن توقف التطبيق X عن العمل. تصعيد الحادث إلى مسؤول ASA/PIX. لا يعرف المسؤول إلا القليل عن هذا التطبيق المعين. مع إستخدام ASA/PIX، يكتشف المسؤول المنافذ والبروتوكولات التي يستخدمها التطبيق X بالإضافة إلى ما قد يكون سبب المشكلة.

الحل

يحتاج مسؤول ASA/PIX إلى جمع أكبر قدر ممكن من المعلومات من المستخدم. وتتضمن المعلومات المفيدة ما يلي:

- عنوان IP المصدر—عادة ما تكون محطة العمل أو الكمبيوتر الخاص بالمستخدم.
- عنوان IP للوجهة—عنوان IP للخادم الذي يحاول المستخدم أو التطبيق توصيله.
- المنافذ والبروتوكولات التي يستخدمها التطبيق

غالبا ما يكون المسؤول محظوظا إذا كان قادرا على الحصول على جواب لأحد هذه الاسئلة. على سبيل المثال، يتعذر على المسؤول تجميع أي معلومات. تعد مراجعة رسائل syslog ل ASA/PIX مثالية، ولكن من الصعب تحديد موقع المشكلة إذا لم يكن المسؤول يعرف ما الذي يجب البحث عنه.

الخطوة 1 - اكتشاف عنوان IP للمستخدم

هناك عدة طرق لاكتشاف عنوان IP للمستخدم. هذا المستند حول ASA و PIX، لذلك يستخدم هذا المثال ASA و PIX لاكتشاف عنوان IP.

يحاول المستخدم الاتصال ب ASA/PIX. يمكن أن يكون هذا الاتصال ICMP أو Telnet أو SSH أو HTTP. يجب أن يكون للبروتوكول المختار نشاط محدود على ASA/PIX. في هذا المثال المحدد، يقوم المستخدم بقطع الواجهة الداخلية ل ASA.

يحتاج المسؤول إلى إعداد واحد أو أكثر من هذه الخيارات ثم مطالبة المستخدم بتشغيل الواجهة الداخلية ل ASA.

- **Syslog**تأكد من تمكين التسجيل. يلزم تعيين مستوى التسجيل على **تصحيح الأخطاء**. يمكن إرسال التسجيل إلى مواقع مختلفة. يستخدم هذا المثال المخزن المؤقت لسجل ASA. قد تحتاج إلى خادم تسجيل خارجي في بيئات الإنتاج.

```
ciscoasa(config)#logging enable
ciscoasa(config)#logging buffered debugging
```

يقطع المستخدم الواجهة الداخلية ل 192.168.1.1 (ping ASA). يتم عرض هذا الإخراج.

```
ciscoasa#show logging
Output is suppressed. %ASA-6-302020: Built ICMP connection for faddr 192.168.1.50/512 ---!
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
ASA-6-302021: Teardown ICMP connection for faddr 192.168.1.50/512%
gaddr 192.168.1.1/0 laddr 192.168.1.1/0
.The user IP address is 192.168.1.50 ---!
```

- **ميزة التقاط ASA**يحتاج المسؤول إلى إنشاء قائمة وصول تحدد حركة مرور البيانات التي يحتاج ASA إلى التقاطها. بعد تحديد قائمة الوصول، يتضمن الأمر **capture** قائمة الوصول ويطبقها على واجهة.

```
ciscoasa(config)#access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#capture inside_interface access-list inside_test interface inside
```

يقطع المستخدم الواجهة الداخلية ل 192.168.1.1 (ping ASA). يتم عرض هذا الإخراج.

```
ciscoasa#show capture inside_interface
icmp: echo request :192.168.1.1 < 192.168.1.50 13:04:06.284897 :1
.The user IP address is 192.168.1.50 ---!
```

ملاحظة: لتنزيل ملف الالتقاط إلى نظام مثل الموجود، يمكنك القيام بذلك كما يوضح هذا الإخراج.

```
]//:Open an Internet Explorer and browse with this https link format: https ---!
```

ارجع إلى ASA/PIX: التقاط الحزم باستخدام CLI ومثال تكوين ASDM لمعرفة المزيد حول التقاط الحزم في ASA.

- **تصحيح الأخطاء**يتم إستخدام أمر **debug icmp trace** لالتقاط حركة مرور ICMP الخاصة بالمستخدم.

```
ciscoasa#debug icmp trace
```

يقطع المستخدم الواجهة الداخلية ل 192.168.1.1 (ping ASA). يتم عرض هذا الإخراج على وحدة التحكم.

```
#ciscoasa
Output is suppressed. ICMP echo request from 192.168.1.50 to 192.168.1.1 ID=512 ---!
seq=5120 len=32
ICMP echo reply from 192.168.1.1 to 192.168.1.50 ID=512 seq=5120 len=32
.The user IP address is 192.168.1.50 ---!
```

لتعطيل **تتبع ICMP**، أستخدم أحد الأوامر التالية:**لا يوجد تتبع ICMP لتصحيح الأخطاءإلغاء تصحيح أخطاء تتبع ICMPإلغاء تصحيح أخطاء الكل**، **إلغاء تصحيح أخطاء الكل**، أو **إلغاء الكل**

يساعد كل خيار من هذه الخيارات الثلاثة المسؤول على تحديد عنوان IP المصدر. في هذا المثال، عنوان IP المصدر للمستخدم هو 192.168.1.50. يكون المسؤول مستعدا لمعرفة المزيد حول التطبيق X وتحديد سبب المشكلة.

الخطوة 2 - تحديد سبب المشكلة

بالإشارة إلى المعلومات المدرجة في قسم الخطوة 1 في هذا المستند، يعلم المسؤول الآن مصدر جلسة عمل التطبيق X. يكون المسؤول مستعدا لمعرفة المزيد حول التطبيق X ولبدء تحديد مكان المشاكل المحتملة.

يحتاج مسؤول ASA/PIX إلى إعداد ASA لواحد على الأقل من هذه الاقتراحات المدرجة. بمجرد أن يكون المسؤول جاهزا، يقوم المستخدم ببدء التطبيق X ويحد من جميع الأنشطة الأخرى حيث أن النشاط الإضافي للمستخدم قد يتسبب في حدوث إرتباك أو تضليل مسؤول ASA/PIX.

- **مراقبة رسائل syslog**.ابحث عن عنوان IP المصدر للمستخدم الذي قمت بتحديد موقعه في الخطوة 1. يقوم المستخدم بتهيئة التطبيق X. يصدر مسؤول ASA الأمر **show logging** ويعرض الإخراج.

```
ciscoasa#show logging
Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-6- ---!
305011: Built dynamic TCP translation from inside:192.168.1.50/1107 to
```

```
outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP connection 90 for
outside:172.22.1.1/80
(to inside:192.168.1.50/1107 (172.22.1.254/1025 (172.22.1.1/80)
```

تكشف السجلات أن الغاية عنوان 172.22.1.1، البروتوكول هو TCP، الغاية ميناء HTTP/80، وأن حركة مرور أرسلت إلى القارن خارجي.

- **تعديل عوامل تصفية الالتقاط.**تم إستخدام الأمر **access-list inside_test** مسبقا ويتم إستخدامه هنا.

```
ciscoasa(config)#access-list inside_test permit ip host 192.168.1.50 any
This ACL line captures all traffic from 192.168.1.50 !--- that goes to or through the ---!
ASA. ciscoasa(config)#access-list inside_test permit ip any host 192.168.1.50 any
This ACL line captures all traffic that leaves !--- the ASA and goes to 192.168.1.50. ---!
ciscoasa(config)#no access-list inside_test permit icmp any host 192.168.1.1
ciscoasa(config)#clear capture inside_interface
Clears the previously logged data. !--- The no capture inside_interface removes/deletes ---!
.the capture
```

يقوم المستخدم بتهيئة التطبيق X. ثم يصدر مسؤول ASA الأمر **show capture inside_interface** ويعرض الإخراج.

```
ciscoasa(config)#show capture inside_interface
:172.22.1.1.80 < 192.168.1.50.1107 15:59:42.749152 :1
<S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK
:172.22.1.1.80 < 192.168.1.50.1107 15:59:45.659145 :2
<S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK
:172.22.1.1.80 < 192.168.1.50.1107 15:59:51.668742 :3
<S 3820777746:3820777746(0) win 65535 <mss 1460,nop,nop,sackOK
```

توفر حركة المرور التي تم الاستيلاء عليها للمسؤول العديد من المعلومات القيمة:غاية عنوان-172.22.1.1رقم المنفذ—http/80بروتوكول—TCP (لاحظ علامة النظام أو S)بالإضافة إلى ذلك، يعرف المسؤول أيضا أن حركة مرور البيانات للتطبيق X تصل إلى ASA.إذا كان الإخراج هو إخراج الأمر **show capture inside_interface** هذا، فإن حركة مرور التطبيق إما أنها لم تصل أبدا إلى ASA أو أن عامل تصفية الالتقاط لم يتم تعيينه على التقاط حركة مرور البيانات:

```
ciscoasa#show capture inside_interface
packet captured 0
packet shown 0
```

في هذه الحالة، يجب أن يفكر المسؤول في التحقق من كمبيوتر المستخدم وأي موجه أو أجهزة شبكة أخرى في المسار بين كمبيوتر المستخدم و ASA.**ملاحظة:** عند وصول حركة المرور إلى واجهة، يقوم الأمر **capture** بتسجيل البيانات قبل أن تقوم أي نهج أمان ASA بتحليل حركة المرور. على سبيل المثال، ترفض قائمة الوصول جميع حركة المرور الواردة على الواجهة. لا يزال الأمر **capture** يقوم بتسجيل حركة المرور. وبعد ذلك يحلل نهج أمان ASA حركة مرور البيانات.

- **تصحيح الأخطاءلا** يعرف المسؤول التطبيق X وبالتالي لا يعرف أي من خدمات تصحيح الأخطاء لتمكين تحقيق التطبيق X. قد لا يكون تصحيح الأخطاء أفضل خيار لاستكشاف الأخطاء وإصلاحها في هذه النقطة.

بفضل المعلومات المجموعة في الخطوة 2، يحصل مسؤول ASA على عدة وحدات بت من المعلومات القيمة. يعرف المسؤول حركة المرور التي تصل إلى الواجهة الداخلية ل ASA، وعنوان IP للمصدر، وعنوان IP للوجهة وتطبيق الخدمة X الذي يستخدمه (TCP/80). من خلال syslogs، يعلم المسؤول أيضا أنه تم السماح بالاتصال في البداية.

الخطوة 3 - تأكيد حركة مرور التطبيقات ومراقبتها

يريد مسؤول ASA التأكد من أن حركة مرور التطبيق X قد تركت ASA وكذلك مراقبة أي حركة مرور مرتجعة من خادم X للتطبيق.

- **مراقبة رسائل syslog.**تصفية رسائل syslog لعنوان IP للمصدر (192.168.1.50) أو عنوان IP للوجهة (172.22.1.1). من سطر الأوامر، تبدو تصفية رسائل syslog مثل **show logging | يتضمن 192.168.1.50** أو **show logging | يتضمن 172.22.1.1**. في هذا المثال، يتم إستخدام الأمر **show logging** بدون عوامل تصفية. يتم منع المخرجات لتسهيل القراءة.

```
ciscoasa#show logging
```

```
Output is suppressed. %ASA-7-609001: Built local-host inside:192.168.1.50 %ASA-7- ---!
609001: Built local-host outside:172.22.1.1 %ASA-6-305011: Built dynamic TCP translation
from inside:192.168.1.50/1107 to outside:172.22.1.254/1025 %ASA-6-302013: Built outbound TCP
connection 90 for outside:172.22.1.1/80 (172.22.1.1/80) to inside:192.168.1.50/1107
(172.22.1.254/1025) %ASA-6-302014: Teardown TCP connection 90 for outside:172.22.1.1/80
to inside:192.168.1.50/1107 duration 0:00:30 bytes 0 SYN Timeout
ASA-7-609002: Teardown local-host outside:172.22.1.1 duration 0:00:30%
ASA-6-305012: Teardown dynamic TCP translation from inside:192.168.1.50/1107%
to outside:172.22.1.254/1025 duration 0:01:00
ASA-7-609002: Teardown local-host inside:192.168.1.50 duration 0:01:00%
```

تشير رسالة syslog إلى إغلاق الاتصال بسبب انتهاء مهلة SYN. وهذا يفيد المسؤول أنه لم يتم تلقي استجابات خادم X للتطبيق بواسطة ASA. يمكن أن تختلف أسباب إنهاء رسالة syslog.يتم تسجيل مهلة SYN بسبب إنهاء اتصال إجباري بعد 30 ثانية من حدوث ذلك بعد اكتمال تأكيد الاتصال الثلاثي. وتحدث هذه المشكلة عادة إذا فشل الخادم في الاستجابة لطلب اتصال، وفي معظم الحالات، لا يتصل بالتكوين على PIX/ASA.لحل هذه المشكلة، ارجع إلى قائمة التحقق هذه:تأكد من إدخال الأمر الثابت بشكل صحيح وأنه لا يتداخل مع أوامر ثابتة أخرى، على سبيل المثال،

```
static (inside,outside) x.x.x.x  y.y.y.y netmask 255.255.255.255
```

الساكن إستاتيكي nat في ASA 8.3 وفيما بعد يستطيع كنت شكلت كما هو موضح هنا:

```
object network obj-y.y.y.y
 host y.y.y.y
nat (inside,outside) static x.x.x.x
```

تأكد من وجود قائمة الوصول للسماح بالوصول إلى عنوان IP العالمي من الخارج وأنه مرتبط بالواجهة:

```
access-list OUTSIDE_IN extended permit tcp any host x.x.x.x eq www
access-group OUTSIDE_IN in interface outside
```

من أجل اتصال ناجح بالخادم، يجب أن تشير العبارة الافتراضية الموجودة على الخادم إلى واجهة DMZ الخاصة ب PIX/ASA.ارجع إلى رسائل نظام ASA للحصول على مزيد من المعلومات حول رسائل syslog.

- **إنشاء عامل تصفية التقاط جديد.**من رسائل حركة المرور و syslog السابقة التي تم التقاطها، يعلم المسؤول أن التطبيق X يجب أن يترك ال ASA من خلال الواجهة الخارجية.

```
ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80
When you leave the source as 'any', it allows !--- the administrator to monitor any ---!
network address translation (NAT). ciscoasa(config)#access-list outside_test permit tcp host
172.22.1.1 eq 80 any
When you reverse the source and destination information, !--- it allows return traffic ---!
to be captured. ciscoasa(config)#capture outside_interface access-list outside_test
interface outside
```

يحتاج المستخدم إلى بدء جلسة عمل جديدة مع التطبيق X. بعد أن يبدأ المستخدم جلسة عمل تطبيق X جديدة، يحتاج مسؤول ASA إلى إصدار الأمر **show capture outside_interface** على ASA.

```
ciscoasa(config)#show capture outside_interface
                                packets captured 3
                  :172.22.1.1.80 < 172.22.1.254.1026 16:15:34.278870 :1
<S 1676965539:1676965539(0) win 65535 <mss 1380,nop,nop,sackOK
                  :172.22.1.1.80 < 172.22.1.254.1027 16:15:44.969630 :2
<S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK
                  :172.22.1.1.80 < 172.22.1.254.1027 16:15:47.898619 :3
<S 990150551:990150551(0) win 65535 <mss 1380,nop,nop,sackOK
                                packets shown 3
```

يظهر الالتقاط حركة مرور تخرج من الواجهة الخارجية ولكن لا يبدي أي حركة مرور رد من الخادم 172.22.1.1. يوضح هذا الالتقاط البيانات عند تركها في وضع ASA.

- **أستخدم خيار packet-tracer.**من الأقسام السابقة، تعلم مسؤول ASA معلومات كافية لاستخدام خيار **الحزمة-tracer** في ASA.**ملاحظة:** يدعم ASA أمر **packet-tracer** الذي يبدأ في الإصدار 7.2.

```
ciscoasa#packet-tracer input inside tcp 192.168.1.50 1025 172.22.1.1 http
This line indicates a source port of 1025. If the source !--- port is not known, any ---!
number can be used. !--- More common source ports typically range !--- between 1025 and
```

65535. Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: FLOW-LOOKUP Subtype: Result: ALLOW Config: Additional Information: Found no matching flow, creating a new flow Phase: 4 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 172.22.1.0 255.255.255.0 outside Phase: 5 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: **access-group inside_acl in interface inside**
access-list inside_acl extended permit tcp 192.168.1.0 255.255.255.0 any eq www
:Additional Information

Phase: 6
Type: IP-OPTIONS
:Subtype
Result: ALLOW
:Config
:Additional Information

Phase: 7
Type: CAPTURE
:Subtype
Result: ALLOW
:Config
:Additional Information

Phase: 8
Type: NAT
:Subtype
Result: ALLOW
:Config
nat (inside) 1 192.168.1.0 255.255.255.0
match ip inside 192.168.1.0 255.255.255.0 outside any
(dynamic translation to pool 1 (172.22.1.254
translate_hits = 6, untranslate_hits = 0
:Additional Information
Dynamic translate 192.168.1.50/1025 to 172.22.1.254/1028
using netmask 255.255.255.255

Phase: 9
Type: NAT
Subtype: host-limits
Result: ALLOW
:Config
nat (inside) 1 192.168.1.0 255.255.255.0
match ip inside 192.168.1.0 255.255.255.0 outside any
(dynamic translation to pool 1 (172.22.1.254
translate_hits = 6, untranslate_hits = 0
:Additional Information

Phase: 10
Type: CAPTURE
:Subtype
Result: ALLOW
:Config
:Additional Information

Phase: 11
Type: CAPTURE
:Subtype
Result: ALLOW
:Config
:Additional Information

Phase: 12
Type: IP-OPTIONS

```
                                                                :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                :Additional Information

                                                          Phase: 13
                                                      Type: CAPTURE
                                                             :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                :Additional Information

                                                          Phase: 14
                                                Type: FLOW-CREATION
                                                             :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                :Additional Information
                                New flow created with id 94, packet dispatched to next module

                                                          Phase: 15
                                                      Type: ROUTE-LOOKUP
                                              Subtype: output and adjacency
                                                      Result: ALLOW
                                                             :Config
                                                :Additional Information
                                    found next-hop 172.22.1.1 using egress ifc outside
                                                          adjacency Active
                                    next-hop mac address 0030.a377.f854 hits 11
  The MAC address is at Layer 2 of the OSI model. !--- This tells the administrator the ---!
  next host !--- that should receive the data packet. Result: input-interface: inside input-
   status: up input-line-status: up output-interface: outside output-status: up output-line-
                                                          status: up Action: allow
```

أهم إنتاج من **الربط-tracer** أمر الأخير خط، أي يكون : .

تظهر الخيارات الثلاثة في الخطوة 3 كل خيار للمسؤول أن ASA غير مسؤول عن مشاكل التطبيق X. تترك حركة مرور X التطبيق ASA ولا يتلقى ASA أي رد من خادم X للتطبيق.

ما هي الخطوة التالية؟

هناك العديد من المكونات التي تسمح للتطبيق X بالعمل بشكل صحيح للمستخدمين. تتضمن المكونات كمبيوتر المستخدم، وعميل التطبيق X، والتوجيه، وسياسات الوصول، وخادم التطبيق X. في المثال السابق، أثبتنا أن ASA يستلم ويعيد التطبيق x حركة مرور. يجب أن يشترك الآن مسؤولو الخادم والتطبيق X. يجب على المسؤولين التحقق من تشغيل خدمات التطبيقات ومراجعة أي سجلات على الخادم والتحقق من تلقي الخادم والتطبيق X لحركة مرور المستخدم.

المشكلة: إنهاء رسالة خطأ اتصال وكيل TCP

تتلقى رسالة الخطأ هذه:

```
PIX|ASA-5-507001: Terminating TCP-Proxy connection from%
- interface_inside:source_address/source_port to interface_outside:dest_address/dest_port
reassembly limit of limit bytes exceeded
```

الحل

الشرح: تعرض هذه الرسالة عند تجاوز حد مخزن إعادة التجميع المؤقت أثناء تجميع مقاطع TCP.

- *source_address/source_port* - عنوان IP المصدر ومنفذ المصدر للحزمة التي تبدأ الاتصال.
- *dest_address/dest_port* - عنوان IP للوجهة ومنفذ الوجهة للحزمة التي تبدأ الاتصال.
- *interface_inside* - يصل اسم الواجهة التي بدأت الاتصال عليها.
- *interface_outside* - اسم الواجهة التي تخرج عليها الحزمة التي بدأت الاتصال.
- *الحد* - حد الاتصال الجنيني الذي تم تكوينه لفئة حركة المرور.

الحل الخاص بهذه المشكلة هو تعطيل فحص RTSP في جهاز الأمان كما هو موضح.

```
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  no inspect rtsp
```

راجع معرف تصحيح الأخطاء من CSCsl15229 Cisco (العملاء المسجلون فقط) للحصول على مزيد من التفاصيل.

المشكلة: "ASA-6-110003٪: فشل التوجيه في تحديد موقع الخطوة التالية للبروتوكول من واجهة src" رسالة الخطأ

يقوم ASA بإسقاط حركة مرور البيانات باستخدام :ASA-6-110003 src:src ip/src port : رسالة خطأ IP/Dest port.

الحل

يحدث هذا الخطأ عندما يحاول ASA العثور على الخطوة التالية على جدول توجيه الواجهة. بشكل نموذجي، يتم تلقي هذه الرسالة عندما يكون لدى ASA ترجمة (xlate) مبنية على واجهة واحدة ومسار يشير إلى واجهة مختلفة. فحصت ل misconfiguration على ال nat عبارة. قد يحل حل الخطأ حل حل مشكلة عدم التكوين.

المشكلة: تم حظر الاتصال بواسطة ASA مع رسالة الخطأ " ASA-5-٪305013: قواعد NAT غير المتماثلة المتطابقة للتدفقات الأمامية والعكسية"

تم حظر الاتصال بواسطة ASA، وتم تلقي رسالة الخطأ هذه:

```
ASA-5-305013: Asymmetric NAT rules matched for forward%
    and reverse flows; Connection protocol src
  interface_name:source_address/source_port dest
interface_name:dest_address/dest_port denied due to NAT reverse path
.failure
```

الحل

عندما يتم تنفيذ ال nat، يحاول ASA أيضا أن يعكس الربط ويتحقق ما إذا كان هذا يضرب أي ترجمة. إن لا يصطدم أي أو مختلف nat ترجمة، بعد ذلك هناك حالة عدم توافق. أنت بشكل عام ترى هذا خطأ رسالة عندما هناك مختلف nat قاعدة يشكل ل خارج وقادم حركة مرور مع ال نفسه مصدر وغاية. تحقق من بيان NAT لحركة المرور المعنية.

مشكلة: خطأ في الاستلام - ASA-5-321001٪: حد 'conns' للمورد الذي تم

الوصول إليه للنظام وهو 10000

الحل

يدل هذا الخطأ على أن إتصالات الخادم الموجودة عبر ASA قد وصلت إلى الحد الأقصى. قد يكون هذا مؤشرا على هجوم رفض الخدمة (DoS) على خادم في شبكتك. أستخدم MPF على ASA وقلل حد الاتصالات الجنينية. قم أيضا بتمكين "اكتشاف الاتصال المعطل" (DCD). أحلت هذا تشكيل snippet:

```
class-map limit
match access-list limit
!
policy-map global_policy
class limit
set connection embryonic-conn-max 50
set connection timeout embryonic 0:00:10 dcd
!
access-list limit line 1 extended permit tcp any host x.x.x.x
```

المشكلة: خطأ الاستلام ٪PIX-1-106021: رفض التحقق من المسار العكسي لـ TCP/UDP من src_addr إلى dest_addr على الواجهة int_name

الحل

يتم تلقي رسالة السجل هذه عند تمكين التحقق من المسار العكسي. أصدرت هذا أمر in order to حللت المشكلة وأعجزت العكسي ممر تدقيق:

```
no ip verify reverse-path interface
```

المشكلة: انقطاع اتصال الإنترنت بسبب الكشف عن التهديد

إستلمت هذا خطأ رسالة على ال ASA:

```
ASA-4-733100: [Miralix Licen 3000] drop rate-1 exceeded. Current burst%
rate is 100 per second, max configured rate is 10; Current average rate is 4
per second, max configured rate is 5; Cumulative total count is 2526
```

الحل

يتم إنشاء هذه الرسالة عن طريق اكتشاف التهديدات بسبب التكوين الافتراضي عند اكتشاف سلوك حركة مرور شاذ. تركز الرسالة على MirrorEx Licen 3000 وهو منفذ TCP/UDP. حددت الأداة أن يكون يستعمل ميناء 3000. تحقق من إحصائيات ASDM الرسومية للكشف عن التهديدات والتحقق من أعلى الهجمات لمعرفة ما إذا كانت تعرض المنفذ 3000 وعنوان IP المصدر. إذا كان جهازا شرعيا، فيمكنك زيادة معدل اكتشاف التهديدات الأساسية على ASA لحل رسالة الخطأ هذه.

معلومات ذات صلة

- مرجع أمر ASA من Cisco
- مرجع أمر PIX من Cisco
- خطأ Cisco ASA ورسائل النظام
- خطأ Cisco PIX ورسائل النظام
- دعم أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- دعم أجهزة الأمان Cisco PIX 500 Series Security Appliances
- الدعم التقني والمستندات - Cisco Systems

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).