يرباط ASA 8.4(x) شبكة داخلية واحدة بمثال تكوين الإنترنت

المحتويات

المقدمة

يوضح هذا المستند كيفية إعداد جهاز الأمان القابل للتكيف (ASA) من Cisco مع الإصدار 8.4(1) للاستخدام على شبكة داخلية واحدة.

ارجع إلى PIX/ASA: توصيل شبكة داخلية واحدة بمثال تكوين الإنترنت لنفس التكوين على ASA مع الإصدارات 8.2 والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى ASA مع الإصدار 8.4(1).

تم إنشاء المعلومات المُقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

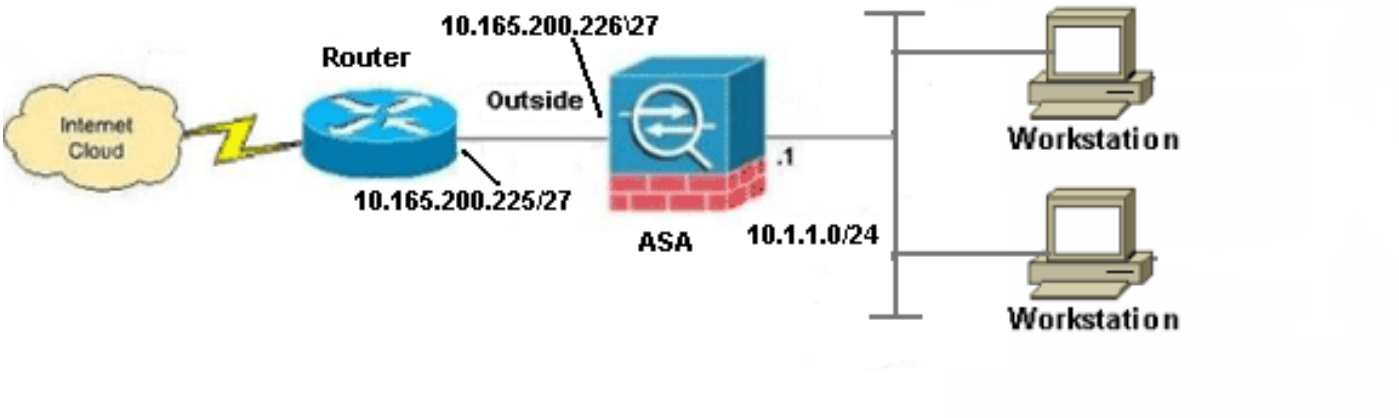
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

تكوين ASA 8.4

يستخدم هذا المستند التكوينات التالية:

- تكوين الموجّه
- ASA 8.4 والتكوين اللاحق

تكوين الموجّه

```
...Building configuration

:Current configuration
!
```

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R3640_out
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/1
ip address 10.165.200.225 255.255.255.224
no ip directed-broadcast

!
ip classless
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

ASA 8.4 والتكوين اللاحق

```
ASA#show run
Saved :
:
(ASA Version 8.4(1
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

.Configure the outside interface ---!

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.165.200.226 255.255.255.224
```

```
.Configure the inside interface ---!

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
management-only
!
boot system disk0:/asa841-k8.bin

ftp mode passive
!
.Creates an object called OBJ_GENERIC_ALL ---!
Any host IP not already matching another configured ---!
NAT rule will Port Address Translate (PAT) to the outside interface IP ---!
.on the ASA (or 10.165.200.226) for Internet bound traffic ---!
!
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
!
nat (inside,outside) source dynamic OBJ_GENERIC_ALL interface
!
route outside 0.0.0.0 0.0.0.0 10.165.200.225
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
```

```
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
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 rsh
inspect rtsp
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect sip
inspect netbios
inspect tftp
inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
end :
```

ملاحظة: للحصول على مزيد من المعلومات حول تكوين ترجمة عنوان الشبكة (NAT) وترجمة عنوان المنفذ (PAT) على الإصدار 8.4 من ASA، ارجع إلى المعلومات حول NAT.

للحصول على مزيد من المعلومات حول تكوين قوائم الوصول في الإصدار 8.4 من ASA، ارجع إلى معلومات حول قوائم الوصول.

التحقق من الصحة

حاول الوصول إلى موقع ويب عبر HTTP باستخدام مستعرض ويب. يستخدم هذا المثال موقعا يتم إستضافته في 198.51.100.100. إذا نجح الاتصال، يمكن رؤية هذا الإخراج على ASA CLI:

الاتصال

```
ASA(config)# show connection address 10.1.1.154
in use, 98 most used 6
,TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937
flags UIO
```

ASA هو جدار حماية ذو حالة، ويتم السماح لحركة مرور البيانات العائدة من خادم الويب عبر جدار الحماية لأنه يطابق ***اتصالا*** في جدول اتصال جدار الحماية. يسمح بحركة المرور التي تطابق اتصال موجود مسبقا من خلال جدار الحماية دون أن يتم حظرها بواسطة قائمة التحكم في الوصول (ACL) للواجهة.

في الإخراج السابق، قام العميل الموجود على الواجهة الداخلية بإنشاء اتصال بالمضيف 198.51.100.100 الموجود خارج الواجهة. يتم إجراء هذا الاتصال باستخدام بروتوكول TCP وقد كان خاملا لمدة ست ثوان. تشير علامات الاتصال إلى الحالة الحالية لهذا الاتصال. يمكن العثور على مزيد من المعلومات حول علامات الاتصال في علامات اتصال ASA

.TCP

Syslog

```
ASA(config)# show log | in 10.1.1.154

:Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside
to outside:10.165.200.226/58799 10.1.1.154/58799

:Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside
(to inside:10.1.1.154/58799 (10.165.200.226/58799 (198.51.100.100/80) 198.51.100.100/80
```

يقوم جدار حماية ASA بإنشاء syslog أثناء التشغيل العادي. نطاق syslogs في النطاق الترددي استنادا إلى تكوين التسجيل. يظهر الإنتاج إثنان syslog أن يكون رأيت على المستوى ستة، أو **'information'** مستوى.

في هذا مثال، هناك إثنان syslog ولدت. الأولى هي رسالة سجل تشير إلى أن جدار الحماية قام بإنشاء **ترجمة**، وخاصة ترجمة TCP ديناميكية (PAT). هو يشير المصدر عنوان ومنفذ وال يترجم عنوان ومنفذ بما أن الحركة مرور يعبر من الداخل إلى الواجهات الخارجية.

ويشير syslog الثاني إلى أن جدار الحماية قام بإنشاء **اتصال** في جدول الاتصال الخاص به لحركة المرور المحددة بين العميل والخادم. إذا تم تكوين جدار الحماية لحظر محاولة الاتصال هذه، أو قام عامل آخر بمنع إنشاء هذا الاتصال (قيود الموارد أو احتمال حدوث خطأ في التكوين)، فلن يقوم جدار الحماية بإنشاء سجل يشير إلى إنشاء الاتصال. وبدلا من ذلك، سيقوم بتسجيل سبب رفض الاتصال أو مؤشر على العامل الذي منع إنشاء الاتصال.

ترجمات (Xlate) NAT

```
ASA(config)# show xlate local 10.1.1.154
in use, 80 most used 3
,Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
timeout 0:00:30 0:02:42
```

كجزء من هذا تشكيل، شكلت ضرب in order to ترجمت الداخلي مضيف عنوان إلى عنوان أن يكون routable على الإنترنت. in order to أكدت أن هذا ترجمة يكون خلقت، أنت يستطيع فحصت ال xlate (ترجمة) طاولة. يعرض الأمر **show xlate** ، عند دمجه مع الكلمة الأساسية **المحلية** وعنوان IP للمضيف الداخلي، جميع الإدخالات الموجودة في جدول الترجمة لذلك المضيف. تظهر المخرجات السابقة أن هناك ترجمة بنيت حاليا لهذا المضيف بين الواجهات الداخلية والخارجية. تتم ترجمة عنوان IP والمنفذ المضيف الداخلي إلى عنوان 10.165.200.226 لكل تكوين خاص بنا. تشير العلامات المدرجة، i r، إلى أن الترجمة **ديناميكية** وخريطة **portmap**. يمكن العثور على مزيد من المعلومات حول تكوينات NAT المختلفة هنا: معلومات حول NAT.

استكشاف الأخطاء وإصلاحها

يوفر ASA أدوات متعددة لاستكشاف أخطاء الاتصال وإصلاحها. إذا إستمرت المشكلة بعد التحقق من التكوين والتحقق من الإخراج المدرج سابقا، فقد تساعد هذه الأدوات والتقنيات في تحديد سبب فشل الاتصال.

Packet-Tracer

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 1234 198.51.100.100 80

--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

تتيح لك وظيفة **متتبع الحزم** على ASA تحديد حزمة *محاكية* ورؤية جميع الخطوات والتحقق والدوال المختلفة التي يمر بها جدار الحماية عندما يعالج حركة مرور البيانات. باستخدام هذه الأداة، من المفيد تحديد مثال لحركة المرور التي تعتقد *أنه* يجب السماح لها بالمرور من خلال جدار الحماية، واستخدام تلك الحزمة 5 لمحاكاة حركة المرور. في المثال السابق، يتم إستخدام تعقب الحزمة لمحاكاة محاولة اتصال تطابق هذه المعايير:

- تصل الحزمة المحاكاة إلى **الداخل**.
- البروتوكول المستخدم هو **TCP**.
- عنوان IP الخاص بالعميل المحاكي هو **10.1.1.154**.
- يرسل العميل حركة مرور sourced من المنفذ **1234**.
- يتم توجيه حركة المرور إلى خادم على عنوان **198.51.100.100** IP.
- معد الحركة مرور إلى ميناء **80**.

لاحظ أنه لم يتم ذكر الواجهة **خارج** الأمر. هذا من خلال ربط تصميم tracer. تخبرك الأداة كيفية معالجة جدار الحماية لهذا النوع من محاولات الاتصال، والتي تتضمن كيفية توجيهها، ومن أي واجهة. يمكن العثور على مزيد من المعلومات حول أداة تعقب الحزم في حزم التتبع باستخدام أداة تعقب الحزم.

أسر

```
ASA# capture capin interface inside match tcp host 10.1.1.154 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#  show capture capin

packets captured 3

 1: 11:31:23.432655       10.1.1.154.58799 > 198.51.100.100.80 : S 780523448
    <mss 1460,nop,wscale 2,nop,nop,sackOK (0)780523448> win 8192
 2: 11:31:23.712518       198.51.100.100.80 > 10.1.1.154.58799 : S 2123396067
    <mss 1024,nop,nop,sackOK,nop,wscale 8 (0)2123396067> ack 780523449 win 8192
 3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80 . : ack 2123396068
    win 32768


ASA# show capture capout

packets captured 3

 1: 11:31:23.432869       10.165.200.226.58799 > 198.51.100.100.80 : S 1633080465
    <mss 1380,nop,wscale 2,nop,nop,sackOK (0)1633080465> win 8192
 2: 11:31:23.712472       198.51.100.100.80 > 10.165.200.226.58799 : S 95714629
    <mss 1024,nop,nop,sackOK,nop,wscale 8 (0)95714629> ack 1633080466 win 8192
 3: 11:31:23.712914       10.165.200.226.58799 > 198.51.100.100.80 . : ack 95714630
```

<win 32768/pre>
يمكن أن يلتقط جدار حماية ASA حركة مرور البيانات التي تدخل الواجهات أو تتركها. وظيفة الالتقاط هذه رائعة لأنها يمكن أن تثبت بشكل قاطع إذا وصلت حركة المرور إلى جدار الحماية أو غادرت منه. أظهر المثال السابق تكوين إلتقطين يسميان **Capin** و**capout** على الواجهات الداخلية والخارجية على التوالي. استعملت أوامر الالتقاط الكلمة المفتاح **match**، أي يسمح أنت أن يكون خاص حول ما حركة المرور أنت تريد أن تلتقطه.

من أجل **التقاط** Capin، أشارت إلى أنك تريد مطابقة حركة المرور التي تتم رؤيتها على الواجهة الداخلية (مدخل أو مخرج) التي تطابق **مضيف 10.1.1.154 المضيف TCP 198.51.100.100**. بمعنى آخر، أنت تريد التقاط أي حركة مرور TCP التي يتم إرسالها من **المضيف 10.1.1.154** إلى **المضيف 198.51.100.100** أو **العكس**. يسمح إستخدام الكلمة الأساسية **match** جدار الحماية بالتقاط حركة مرور البيانات تلك بشكل ثنائي الإتجاه. لا يشير أمر الالتقاط المعرف للواجهة الخارجية إلى عنوان IP للعميل الداخلي لأن جدار الحماية يقوم بإجراء ضرب على عنوان IP الخاص بالعميل. ونتيجة لذلك، لا يمكنك **مطابقة** عنوان IP هذا للعميل. بدلا من ذلك، يستخدم هذا المثال **أي** للإشارة إلى أن جميع عناوين IP المحتملة ستطابق هذا الشرط.

بعد تكوين عمليات الالتقاط، تحاول بعد ذلك إنشاء اتصال مرة أخرى، ثم تتابع عرض عمليات الالتقاط باستخدام الأمر **show capture <*capture_name*>**. في هذا المثال، يمكنك أن ترى أن العميل كان قادرا على الاتصال بالخادم كما هو موضح من خلال مصافحة TCP 3-Way التي تمت رؤيتها في عمليات الالتقاط.

معلومات ذات صلة

- مدير أجهزة حلول الأمان المعدلة من Cisco
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- طلبات التعليقات (RFCs)
- 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).