ASA الإصدار 9.(x) توصيل ثلاث شبكات داخلية مع مثال تكوين الإنترنت

المحتويات

المقدمة

يقدم هذا المستند معلومات حول كيفية إعداد جهاز الأمان القابل للتكيف (ASA) من Cisco الإصدار 9.1(5) للاستخدام مع ثلاث شبكات داخلية. يتم إستخدام المسارات الثابتة على الموجهات لضمان البساطة.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) من Cisco، الإصدار 9.1(5).

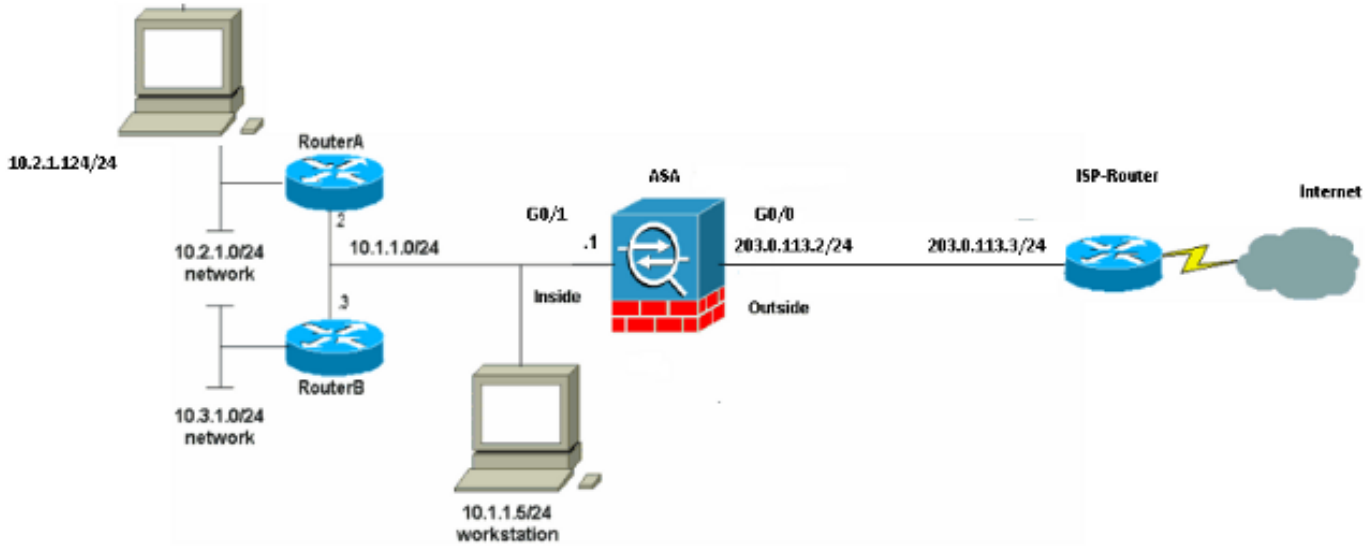
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

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

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة



ملاحظة: ال ip ليس خاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. مه rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

تكوين ASA 9.1

يستخدم هذا المستند هذه التكوينات. إن يتلقى أنت الإنتاج من **كتابة terminal** أمر من ك cisco أداة، أنت يستطيع استعملت إنتاج مترجم (يسجل زبون فقط) أن يعرض ممكن إصدار ونقطة معينة.

التكوينات

- تكوين الموجه A
- تكوين الموجه B
- ASA مراجعة 9.1 والتكوين اللاحق

تكوين الموجه A

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

```
hostname RouterA
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
memory-size iomem 25
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.2.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line 33
no activation-character
```

```
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password ww
login
!
!
end

RouterA#
```

تكوين الموجه B

```
RouterB#show running-config
Building configuration...

Current configuration : 1132 bytes
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterB
!
boot-start-marker
boot-end-marker
!
!
no network-clock-participate slot 1
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
ip cef
!
!
!
!
ip audit po max-events 100
no ip domain lookup
no ftp-server write-enable
!
!
!
!
!
no crypto isakmp enable
!
!
!
interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
duplex auto
speed auto
no cdp enable
```

```
!
interface FastEthernet0/1
ip address 10.3.1.1 255.255.255.0
duplex auto
speed auto
!
interface IDS-Sensor1/0
no ip address
shutdown
hold-queue 60 out
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.2
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
stopbits 1
line 33
no activation-character
no exec
transport preferred none
transport input all
transport output all
line aux 0
line vty 0 4
password cisco
login
!
!
end

RouterB#
```

ASA مراجعة 9.1 والتكوين اللاحق

```
ASA#show run
: Saved
:
ASA Version 9.1(5)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
```

```
!
boot system disk0:/asa915-k8.bin

ftp mode passive

!--- Enable informational logging to see connection creation events

logging on
logging buffered informational

!--- Output Suppressed

!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- object will get 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

!--- Output Suppressed

!--- Define a default route to the ISP router.


route outside 0.0.0.0 0.0.0.0 203.0.113.3 1

!--- Define a route to the INTERNAL router with network 10.2.1.0.

route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

!--- Define a route to the INTERNAL router with network 10.3.1.0.

route inside 10.3.1.0 255.255.255.0 10.1.1.3 1

: end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show.** استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show.**

حاول الوصول إلى موقع ويب عبر HTTP باستخدام مستعرض ويب. يستخدم هذا المثال موقعا يتم استضافته في 198.51.100.100. إذا نجح الاتصال، يمكن رؤية هذا الإخراج على واجهة سطر أوامر ASA.

الاتصال

```
ASA(config)# show connection address 10.2.1.124
16 in use, 918 most used
TCP outside 198.51.100.100:80 inside 10.2.1.124:18711, idle 0:00:16, bytes 1937,
flags UIO
```

ASA هو جدار حماية ذو حالة، ويتم السماح لحركة مرور البيانات العائدة من خادم الويب عبر جدار الحماية لأنه يطابق ***الاتصال*** في جدول اتصال جدار الحماية. يتم السماح بحركة المرور التي

قمئاق ةطساوب اهرظح متي الو ةيامحلا رادج للاخ نم اقبسم دوجوم لاصتا عم قباطتت
مكحتلا في لوصولا (ACL) ةهجاولل.

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 | include 10.2.1.124

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.2.1.124/18711 to outside:203.0.113.2/18711

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.2.1.124/18711 (203.0.113.2/18711)
```

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

في هذا المثال، 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 هذه 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 NAT

```
ASA(config)# show xlate local 10.2.1.124
2 in use, 180 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.2.1.124/18711 to outside:203.0.113.2/18711 flags ri idle
0:12:03 timeout 0:00:30
```

كجزء من هذا التشكيل، شكلت برهن in order to تمجرت الداخلي مضيف عنوان إلى عنوان أن
يكون routable على الإنترنت. in order to أكدت أن هذا ترجمة يكون خلقت، أنت يستطيع
فحصت ال nat ترجمة (xlate) 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 203.0.113.2
لكل تكوين خاص بنا. تشير العلامات المدرجة، r، إلى أن الترجمة **ديناميكية** وخريطة
portmap. يمكن العثور على مزيد من المعلومات حول تكوينات NAT المختلفة في [المعلومات
حول NAT](#).

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

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

تطبيق Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 10.2.1.124 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
```

تسمح لك وظيفة تعقب الحزمة على ASA بتحديد 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 **10.2.1.124**.
- يرسل العميل حركة مرور sourced من المنفذ **1234**.
- يتم توجيه حركة المرور إلى خادم على عنوان IP **198.51.100.100**.
- 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 تتبع الحزم في حزم التتبع باستخدام أداة تعقب الحزم.

أسر

```
ASA# capture capin interface inside match tcp host 10.2.1.124 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#   show capture capin

3 packets captured

  1: 11:31:23.432655       10.2.1.124.18711 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       198.51.100.100.80 > 10.2.1.124.18711: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.2.1.124.18711 > 198.51.100.100.80: . ack 2123396068
win 32768
```

```
ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       203.0.113.2.18711 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       198.51.100.100.80 > 203.0.113.2.18711: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       203.0.113.2.18711 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

نكمي نأ طقتلي رادج ةيامح ASA ةكرح رورم تانايبلا يتلا لخدت تاهجاولا وأ اهكرتت. ةفيظو ةيامحلا رادج ىلإ رورملا ةكرح تلصو اذإ عطاق لكشب تبثت نأ نكمي اهنأل ةعئار هذه طاقتلالا تاهجاولا ىلع **capout** و**Capin** نايمسي نيطقتلإ نيوكت قباسلا لاثملا رهظأ .هنم ترداغ وأ حمسي يأ ،**match** حاتفملا ةملكلا طاقتلالا رماوأ تلمعتسا .يلاوتلا ىلع ةيجراخلاو ةيلخادلا هطقتلت نأ ديرت تنأ رورملا ةكرح ام لوح صاخ نوكي نأ تنأ.

ةبسنلاب **طاقتلال** Capin، تمت ةراشإلا ىلإ كنأ ديرت ةقباطم ةكرح رورملا يتلا متت اهتيؤر ىلع ةهجاولا ةيلخادلا (لخدم وأ جرخم) يتلا قباطت **فيضم TCP 10.2.1.124 فيضملا** **198.51.100.100**. ىنعمب رخآ، تنأ ديرت طاقتلالا يأ ةكرح رورم TCP يتلا متي اهلاسرإ نم **فيضملا 10.2.1.124** ىلإ **فيضملا 198.51.100.100** وأ **سكعلا**. حمسي مادختسإ ةملكلا ةيساسألا **match** رادج ةيامحلا طاقتلاب ةكرح رورم تانايبلا كلت لكشب يئانث هاجتإلا. ال ةيامحلا رادج نأل يلخادلا ليمعلل IP ناونع ىلإ ةيجراخلا ةهجاولل فرعملا طاقتلالا رمأ ريشي IP ناونع **ةقباطم** كنكمي ال ،كلذل ةجيتنو .ليمعلاب صاخلا IP ناونع ىلع برض ءارجإب موقي ةلمتحملا IP نيوانع عيمج نأ ىلإ ةراشإلل **يأ** لاثملا اذه مدختسي ،كلذ نم الدب .ليمعلل اذه طرشلا اذه قباطتس.

ضرع عباتت مث ،ىرخأ ةرم لاصتا ءاشنإ كلذ دعب لواحت ،طاقتلالا تايلمع نيوكت دعب نأ كنكمي ،لاثملا اذه يف .**show capture *<capture_name>*** رمألا مادختساب طاقتلالا تايلمع ىرت نأ ليمعلا ناك اردان ىلع لاصتالا مداخلاب امك وه حضوم نم لالخ ةحفاصم TCP 3-Way يتلا تمت اهتيؤر يف تايلمع طاقتلالا.

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).