تكوين ASA للوصول إلى خادم بريد SMTP في DMZ والشبكات الداخلية والخارجية

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز أمان قابل للتكيف (ASA) من Cisco للوصول إلى خادم بروتوكول نقل البريد البسيط (SMTP) الموجود في المنطقة المجردة من السلاح (DMZ) أو الشبكة الداخلية أو الشبكة الخارجية.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- ASA من Cisco الذي يشغل الإصدار 9.1 من البرنامج أو إصدار أحدث
- cisco 2800c sery مسحاج تخديد مع cisco ios ® برمجية إطلاق M6(4)15.1

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

التكوين

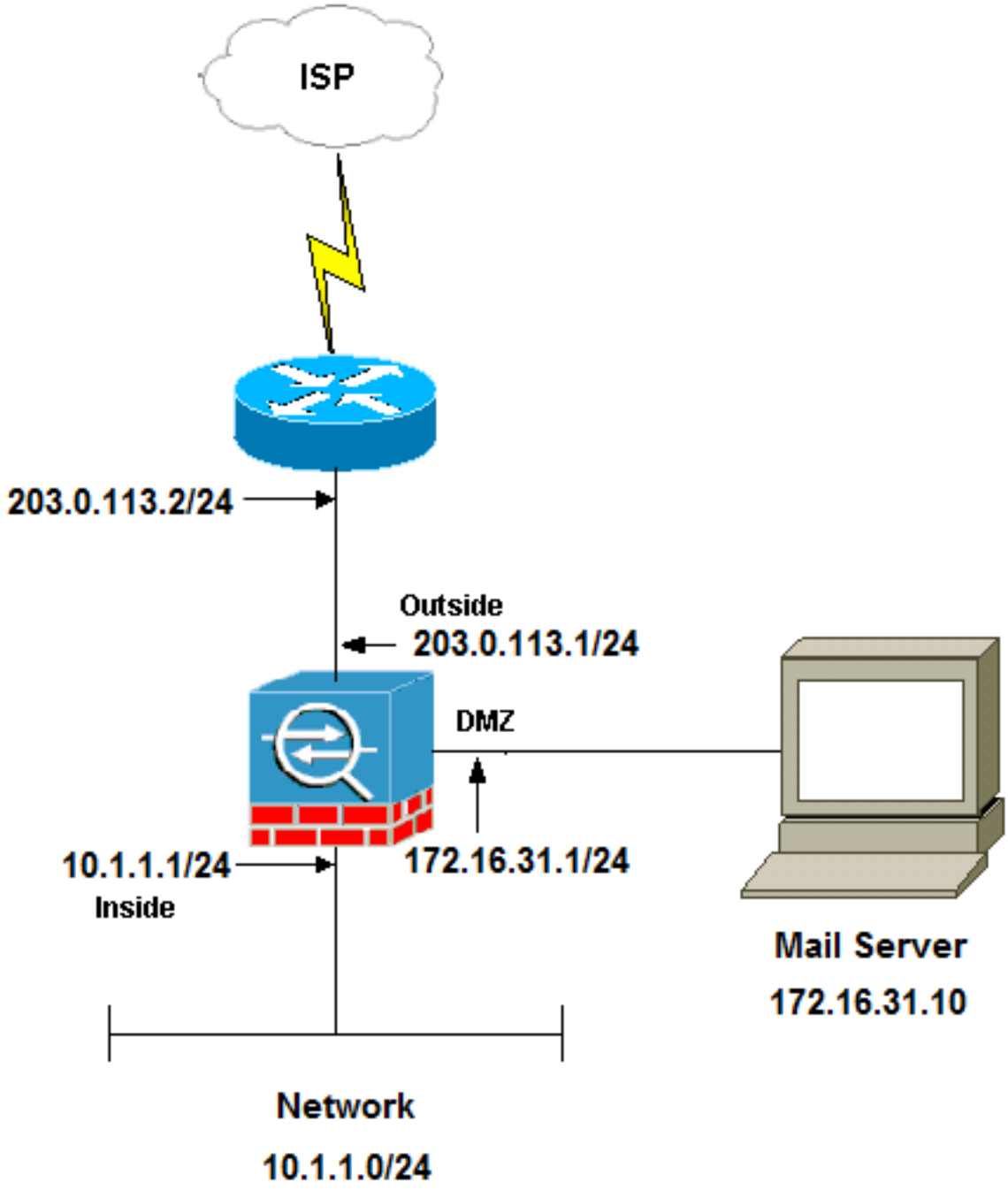
يصف هذا القسم كيفية تكوين ASA للوصول إلى خادم البريد في شبكة DMZ أو الشبكة الداخلية أو الشبكة الخارجية.

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

خادم البريد في شبكة DMZ

الرسم التخطيطي للشبكة

يستخدم التكوين الموضح في هذا القسم إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة أن يكون استعملت في هذا وثيقة قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يتلقى يكون استعملت في مختبر بيئة.

يحتوي إعداد الشبكة المستخدم في هذا المثال على ASA مع شبكة داخلية على **24/10.1.1.0** وشبكة خارجية على **24/203.0.113.0**. يوجد خادم البريد ذو عنوان **172.16.31.10** IP في شبكة DMZ. لكي يتم الوصول إلى خادم البريد بواسطة الشبكة الداخلية، يجب تكوين ترجمة عنوان الشبكة (NAT) للهوية.

in order for المستخدم خارجي أن ينفذ ال بريد نادل، أنت ينبغي شكلت ساكن إستاتيكي nat و منفذ قائمة، أي **خارج_int** في هذا مثال، in order to سمحت للمستخدمين الخارجيين أن ينفذ البريد نادل وربط قائمة الوصول إلى القارن خارجي.

تكوين ASA

هذا هو تكوين ASA لهذا المثال:

```
show run
Saved :
:
(ASA Version 9.1(2
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
passwd 2KFQnbNIdI.2KYOU encrypted
names

.Configure the dmz interface ---!

interface GigabitEthernet0/0
nameif dmz
security-level 50
ip address 172.16.31.1 255.255.255.0
!

.Configure the outside interface ---!

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0

.Configure inside interface ---!

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa912-k8.bin
ftp mode passive

This access list allows hosts to access ---!
.IP address 172.16.31.10 for the SMTP port from outside ---!

access-list outside_int extended permit tcp any4 host 172.16.31.10 eq smtp

object network obj1-10.1.1.0
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

.This network static does not use address translation ---!
.Inside hosts appear on the DMZ with their own addresses ---!

object network obj-10.1.1.0
```

```
subnet 10.1.1.0 255.255.255.0
nat (inside,dmz) static obj-10.1.1.0

!---This Auto-NAT uses address translation.
!---Hosts that access the mail server from the outside
!---use the 203.0.113.10 address.

object network obj-172.16.31.10
host 172.16.31.10
nat (dmz,outside) static 203.0.113.10

access-group outside_int in interface outside

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

timeout xlate 3:00:00
timeout pat-xlate 0:00:30
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
timeout floating-conn 0:00:00
!
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

!---The inspect esmtp command (included in the map) allows
!---SMTP/ESMTP to inspect the application.

policy-map global_policy
class inspection_default
inspect dns maximum-length 512
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
!

!---The inspect esmtp command (included in the map) allows
!---SMTP/ESMTP to inspect the application.

service-policy global_policy global
```

تكوين ESMTP TLS

إذا كنت تستخدم تشفير أمان طبقة النقل (TLS) لاتصالات البريد الإلكتروني، فعندئذ تقوم ميزة الفحص (الممكنة بشكل افتراضي) لبروتوكول نقل البريد البسيط الموسع (ESMTP) في ASA بإسقاط الحزم. للسماح برسائل البريد

الإلكتروني التي تم تمكين TLS بها، قم بتعطيل ميزة فحص ESMTP كما هو موضح في المثال التالي.

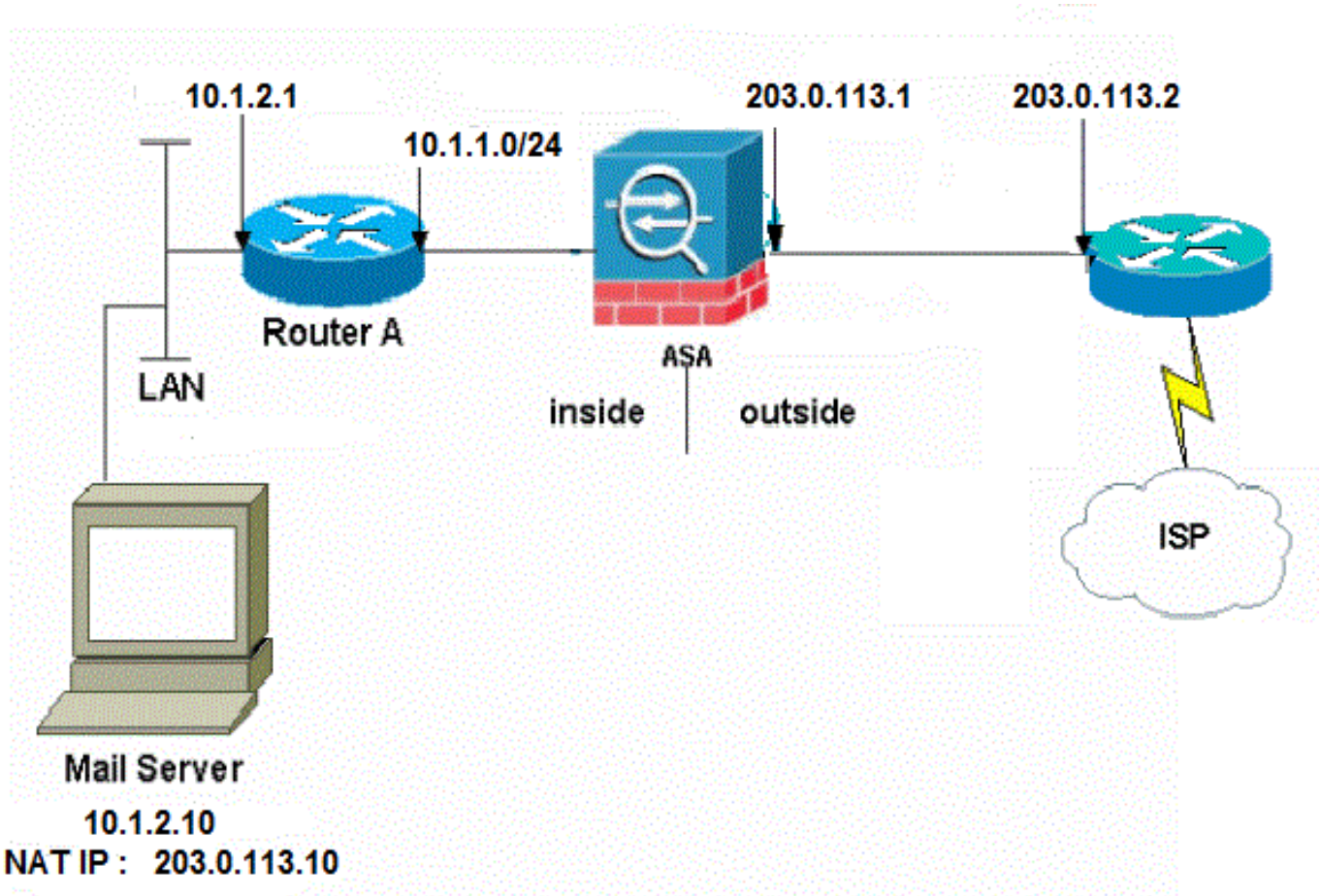
ملاحظة: راجع معرف تصحيح الأخطاء من Cisco CSCtn08326 (العملاء المسجلون فقط) للحصول على مزيد من المعلومات.

```
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

خادم البريد في الشبكة الداخلية

الرسم التخطيطي للشبكة

يستخدم التكوين الموضح في هذا القسم إعداد الشبكة التالي:



يحتوي إعداد الشبكة المستخدم في هذا المثال على ASA مع شبكة داخلية على **24/10.1.1.0** وشبكة خارجية على **24/203.0.113.0**. يوجد خادم البريد بعنوان IP **10.1.2.10** في الشبكة الداخلية.

تكوين ASA

هذا هو تكوين ASA لهذا المثال:

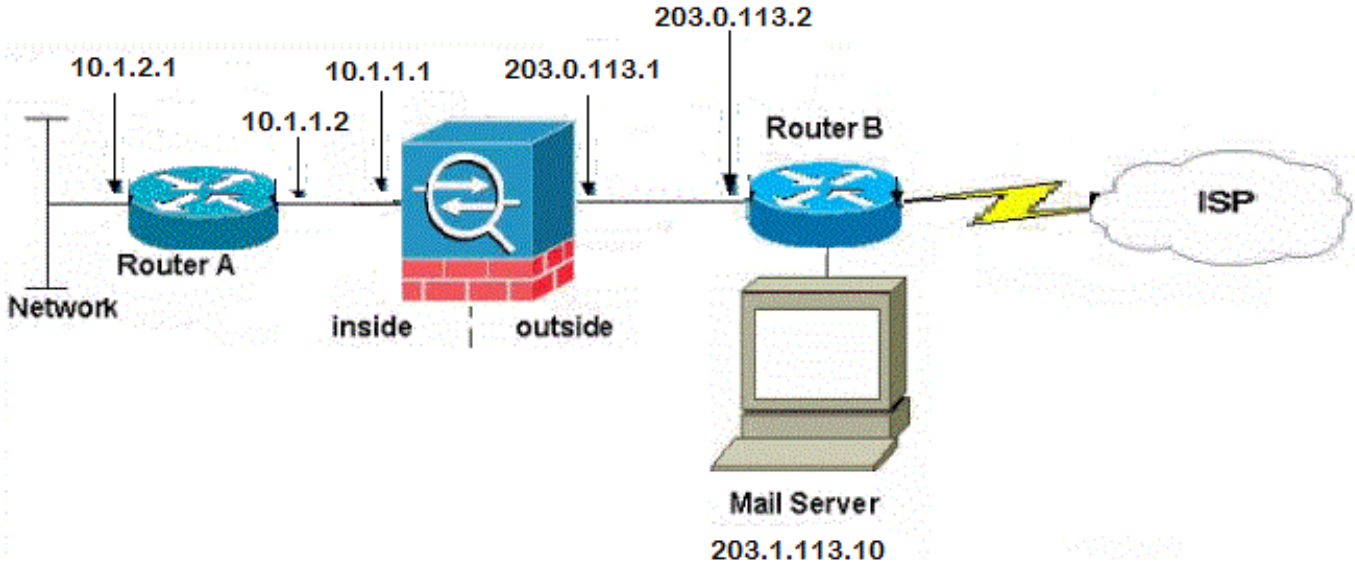
```
ASA#show run
Saved :
:
(ASA Version 9.1(2
!
--Omitted--
!

.Define the IP address for the inside interface ---!

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

.Define the IP address for the outside interface ---!

interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 203.0.113.1 255.255.255.0
!
--Omitted--

Create an access list that permits Simple ---!
Mail Transfer Protocol (SMTP) traffic from anywhere ---!
to the host at 203.0.113.10 (our server). The name of this list is ---!
.smtp. Add additional lines to this access list as required ---!
Note: There is one and only one access list allowed per ---!
.interface per direction, for example, inbound on the outside interface ---!
Because of limitation, any additional lines that need placement in ---!
the access list need to be specified here. If the server ---!
in question is not SMTP, replace the occurrences of SMTP with ---!
.www, DNS, POP3, or whatever else is required ---!

access-list smtp extended permit tcp any host 10.1.2.10 eq smtp

--Omitted--

Specify that any traffic that originates inside from the ---!
x network NATs (PAT) to 203.0.113.9 if.10.1.2 ---!
.such traffic passes through the outside interface ---!

object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic 203.0.113.9

Define a static translation between 10.1.2.10 on the inside and ---!
on the outside. These are the addresses to be used by 203.0.113.10 ---!
.the server located inside the ASA ---!

object network obj-10.1.2.10
host 10.1.2.10
nat (inside,outside) static 203.0.113.10

.Apply the access list named smtp inbound on the outside interface ---!

access-group smtp in interface outside

Instruct the ASA to hand any traffic destined for 10.1.2.0 ---!
.to the router at 10.1.1.2 ---!
```

```
route inside 10.1.2.0 255.255.255.0 10.1.1.2 1

!Set the default route to 203.0.113.2 ---.
!The ASA assumes that this address is a router address ---.

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1
```

خادم البريد في الشبكة الخارجية

الرسم التخطيطي للشبكة

يستخدم التكوين الموضح في هذا القسم إعداد الشبكة التالي:



تكوين ASA

هذا هو تكوين ASA لهذا المثال:

```
ASA#show run
Saved :
:
(ASA Version 9.1(2
!
--Omitted--
!Define the IP address for the inside interface ---.

interface GigabitEthernet0/2
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0

!Define the IP address for the outside interface ---.

interface GigabitEthernet0/1
nameif outside
security-level 0
```

```
ip address 203.0.113.1 255.255.255.0
!
--Omitted--

This command indicates that all addresses in the 10.1.2.x range ---!
that pass from the inside (GigabitEthernet0/2) to a corresponding global ---!
.destination are done with dynamic PAT ---!
As outbound traffic is permitted by default on the ASA, no ---!
.static commands are needed ---!

object network obj-10.1.2.0
subnet 10.1.2.0 255.255.255.0
nat (inside,outside) dynamic interface

.Creates a static route for the 10.1.2.x network ---!
The ASA forwards packets with these addresses to the router ---!
at 10.1.1.2 ---!
route inside 10.1.2.0 255.255.255.0 10.1.1.2 1

Sets the default route for the ASA Firewall at 203.0.113.2 ---!

route outside 0.0.0.0 0.0.0.0 203.0.113.2 1

--Omitted--

end :
```

التحقق من الصحة

أستخدم المعلومات المقدمة في هذا القسم للتحقق من أن التكوين لديك يعمل بشكل صحيح.

خادم البريد في شبكة DMZ

إختبار اتصال TCP

يختبر إختبار اتصال TCP الاتصال عبر TCP (الافتراضي هو بروتوكول رسائل التحكم في الإنترنت (ICMP)). يرسل إختبار اتصال TCP حزم syn ويعتبر إختبار الاتصال ناجحا إذا كان الجهاز الوجهة يرسل حزمة syn-ACK. يمكنك تشغيل إجرائي TCP متزامنين على الأكثر في كل مرة.

فيما يلي مثال:

```
ciscoasa(config)# ping tcp
Interface: outside
Target IP address: 203.0.113.10
Destination port: [80] 25
Specify source? [n]: y
Source IP address: 203.0.113.2
Source port: [0] 1234
Repeat count: [5] 5
Timeout in seconds: [2] 2
.Type escape sequence to abort
Sending 5 TCP SYN requests to 203.0.113.10 port 25
:from 203.0.113.2 starting port 1234, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

الاتصال

ASA هو جدار حماية ذو حالة، ويتم السماح لحركة مرور البيانات العائدة من خادم البريد بالعودة من خلال جدار الحماية لأنه يطابق اتصالا في جدول اتصال جدار الحماية. يتم السماح بحركة المرور التي تتطابق مع اتصال حالي من خلال جدار الحماية دون منعها بواسطة قائمة التحكم في الوصول إلى الواجهة (ACL).

في المثال التالي، يقوم العميل على الواجهة الخارجية بإنشاء اتصال بمضيف 203.0.113.10 لواجهة DMZ. يتم إجراء هذا الاتصال باستخدام بروتوكول TCP وقد كان خاملا لمدة ثانيتين. تشير علامات الاتصال إلى الحالة الحالية لهذا الاتصال:

```
ciscoasa(config)# show conn  address  172.16.31.10
in use, 2 most used 1
TCP outside  203.0.113.2:16678 dmz  172.16.31.10:25, idle 0:00:02, bytes 921, flags UIO
```

التسجيل

يقوم جدار حماية ASA بإنشاء syslog أثناء التشغيل العادي. نطاق syslogs في النطاق الترددي استنادا إلى تكوين التسجيل. يبدي هذا إنتاج إثنان syslog أن يظهر على المستوى ستة (*المعلوماتية* مستوى) والمستوى سبعة (*تصحيح الأخطاء* مستوى):

```
ciscoasa(config)# show logging  | i 172.16.31.10

ASA-7-609001: Built local-host dmz:172.16.31.10%

ASA-6-302013: Built inbound TCP connection 11 for outside:203.0.113.2/16678%
(to dmz:172.16.31.10/25 (203.0.113.10/25 (203.0.113.2/16678)
```

يشير بروتوكول syslog الثاني في هذا المثال 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، فإنه يقوم بتسجيل سبب لرفض الاتصال أو مؤشر عن العامل الذي منع إنشاء الاتصال.

على سبيل المثال، إذا لم يتم تكوين قائمة التحكم في الوصول (ACL) على الخارج للسماح **ب 172.16.31.10** على المنفذ 25، حينئذ سترى هذا السجل عند رفض حركة المرور:

٪ASA-4-106100: تم رفض TCP لقائمة الوصول خارج_int خارج/203.0.113.2(3756) -> (DMZ/172.16.31.10(25 ضرب-300 5 cnt ثانية فاصل

قد يحدث ذلك عندما تكون قائمة التحكم في الوصول (ACL) مفقودة أو مكونة بشكل غير صحيح كما هو موضح هنا:

```
access-list outside_int extended permit tcp any4 host 172.16.31.10 eq http

access-list outside_int extended deny ip any4 any4
```

ترجمات (NAT (Xlate

لتأكيد إنشاء الترجمات، يمكنك التحقق من جدول Xlate (ترجمة). يعرض الأمر **show xlate** ، عند دمجه مع الكلمة الأساسية المحلية وعنوان IP للمضيف الداخلي، جميع الإدخالات الموجودة في جدول الترجمة لذلك المضيف. يوضح الإخراج التالي أنه توجد ترجمة تم إنشاؤها حاليا لهذا المضيف بين المنطقة المنزوعة السلاح والواجهات الخارجية. تتم ترجمة عنوان IP الخاص بخادم DMZ إلى عنوان 203.0.113.10 لكل تكوين سابق. تشير العلامات المدرجة (**s** في هذا المثال) إلى أن الترجمة *ثابتة*.

```
ciscoasa(config)# show nat detail
    (Manual NAT Policies (Section 1
1) (dmz) to (outside) source static obj-172.16.31.10 obj-203.0.113.10
    translate_hits = 7, untranslate_hits = 6
    Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32

    (Auto NAT Policies (Section 2
1) (dmz) to (outside) source static obj-172.16.31.10 203.0.113.10
    translate_hits = 1, untranslate_hits = 5
    Source - Origin: 172.16.31.10/32, Translated: 203.0.113.10/32
2) (inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
3) (inside) to (outside) source dynamic obj1-10.1.1.0 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24

ciscoasa(config)# show xlate
4 in use, 4 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap, 
    s - static, T - twice, N - net-to-net
NAT from dmz:172.16.31.10 to outside:203.0.113.10
    flags s idle 0:10:48 timeout 0:00:00
NAT from inside:10.1.1.0/24 to dmz:10.1.1.0/24
    flags sI idle 79:56:17 timeout 0:00:00
NAT from dmz:172.16.31.10 to outside:203.0.113.10
    flags sT idle 0:01:02 timeout 0:00:00
NAT from outside:0.0.0.0/0 to dmz:0.0.0.0/0
    flags sIT idle 0:01:02 timeout 0:00:00
```

خادم البريد في الشبكة الداخلية

إختبار اتصال TCP

هنا مثال على إخراج إختبار اتصال TCP:

```
ciscoasa(config)# PING TCP
        Interface: outside
    Target IP address: 203.0.113.10
        Destination port: [80] 25
        Specify source? [n]: y
    Source IP address: 203.0.113.2
        Source port: [0] 1234
        Repeat count: [5] 5
    Timeout in seconds: [2] 2
.Type escape sequence to abort
Sending 5 TCP SYN requests to 203.0.113.10 port 25
:from 203.0.113.2 starting port 1234, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

الاتصال

هنا مثال على التحقق من الاتصال:

```
ciscoasa(config)# show conn  address  10.1.2.10
                                                in use, 2 most used 1
TCP outside  203.0.113.2:5672 inside  10.1.2.10:25, idle 0:00:05, bytes 871, flags UIO
```

التسجيل

هنا مثال syslog:

```
ASA-6-302013: Built inbound TCP connection 553 for outside:203.0.113.2/19198%
                    (to inside:10.1.2.10/25 (203.0.113.10/25 (203.0.113.2/19198)
```

ترجمات NAT (Xlate)

هنا مثال **عرض nat تفصيل** و**عرض xlate** أمر ينتج:

```
ciscoasa(config)# show nat detail

                                        (Auto NAT Policies (Section 2
inside) to (outside) source static obj-10.1.2.10 203.0.113.10) 1
                        translate_hits = 0, untranslate_hits = 15
    Source - Origin: 10.1.2.10/32, Translated: 203.0.113.10/32
      inside) to (dmz) source static obj-10.1.1.0 obj-10.1.1.0) 2
                        translate_hits = 0, untranslate_hits = 0
        Source - Origin: 10.1.1.0/24, Translated: 10.1.1.0/24
  inside) to (outside) source dynamic obj1-10.1.1.0 interface) 3
                        translate_hits = 0, untranslate_hits = 0
    Source - Origin: 10.1.1.0/24, Translated: 203.0.113.1/24

ciscoasa(config)# show xlate

NAT from inside:10.1.2.10 to outside:203.0.113.10
          flags s idle 0:00:03 timeout 0:00:00
```

خادم البريد في الشبكة الخارجية

إختبار اتصال TCP

هنا مثال على إخراج إختبار اتصال TCP:

```
ciscoasa# PING TCP
  Interface: inside
Target IP address: 203.1.113.10
     Destination port: [80] 25
        Specify source? [n]: y
  Source IP address: 10.1.2.10
        Source port: [0] 1234
          Repeat count: [5] 5
     Timeout in seconds: [2] 2
.Type escape sequence to abort
Sending 5 TCP SYN requests to 203.1.113.10 port 25
:from 10.1.2.10 starting port 1234, timeout is 2 seconds
                                                !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

الاتصال

هنا مثال على التحقق من الاتصال:

```
ciscoasa# show conn address 203.1.113.10
in use, 2 most used 1
TCP inside 10.1.2.10:13539 outside 203.1.113.10:25, idle 0:00:02, bytes 898, flags UIO
```

التسجيل

هنا مثال syslog:

```
ciscoasa# show logging | i 203.1.113.10

ASA-6-302013: Built outbound TCP connection 590 for outside:203.1.113.10/25%
(to inside:10.1.2.10/1234 (203.0.113.1/1234 (203.1.113.10/25)
```

ترجمات NAT (Xlate)

هنا مثال **عرض** أمر **xlate** ينتج:

```
ciscoasa# show xlate | i 10.1.2.10

TCP PAT from inside:10.1.2.10/1234 to outside:203.0.113.1/1234 flags ri idle
timeout 0:00:30 0:00:04
```

استكشاف الأخطاء وإصلاحها

يوفر ASA أدوات متعددة لاستكشاف أخطاء الاتصال وإصلاحها. إذا إستمرت المشكلة بعد التحقق من التكوين والتحقق من المخرجات الموضحة في القسم السابق، فقد تساعدك هذه الأدوات والتقنيات في تحديد سبب فشل الاتصال.

خادم البريد في شبكة DMZ

Packet-Tracer

تسمح لك وظيفة تعقب الحزمة على ASA بتحديد حزمة *محاكية* وعرض جميع الخطوات والفحوصات والوظائف 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 هذه الحزم الخمسة من أجل محاكاة حركة المرور. في المثال التالي، يتم إستخدام تعقب الحزمة لمحاكاة محاولة اتصال تطابق هذه المعايير:

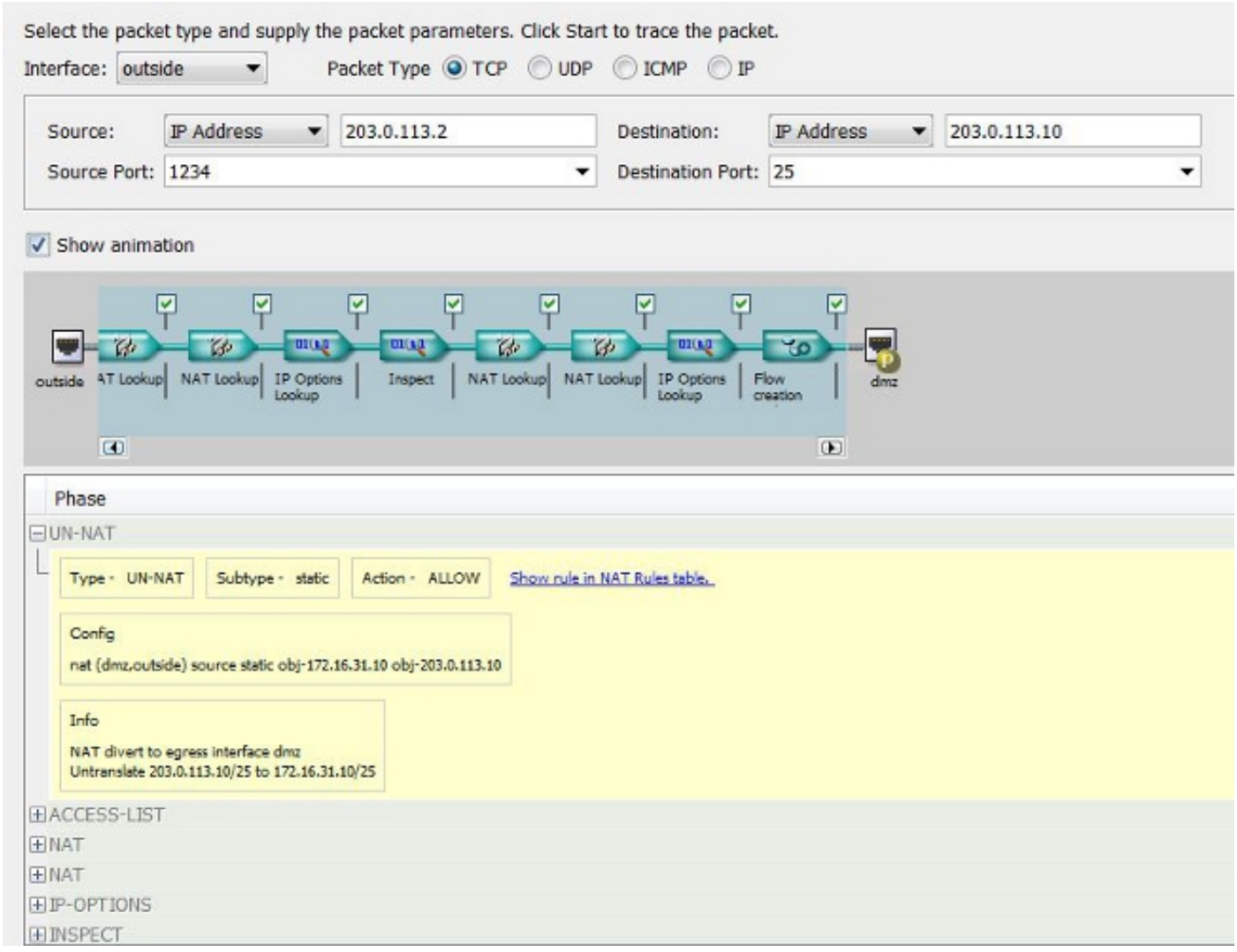
- تصل الحزمة المحاكاة إلى **الخارج**.
- البروتوكول الذي يتم إستخدامه هو **TCP**.
- عنوان IP الخاص بالعميل المحاكي هو **203.0.113.2**.
- يرسل العميل حركة مرور أن يكون مصدر من ميناء **1234**.
- يتم توجيه حركة المرور إلى خادم على عنوان **203.0.113.10** IP.

- حركة المرور موجهة إلى المنفذ **25**.

هنا مثال ربط tracer إنتاج:

```
packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

                                                Phase: 2
                                              Type: UN-NAT
                                           Subtype: static
                                             Result: ALLOW
                                                 :Config
nat (dmz,outside) source static obj-172.16.31.10 obj-203.0.113.10
                                          :Additional Information
                                  NAT divert to egress interface dmz
                          Untranslate 203.0.113.10/25 to 172.16.31.10/25

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

وفيما يلي مثال على مدير أجهزة حلول الأمان المعدلة (ASDM) من Cisco:



لاحظ أنه لا يوجد ذكر لواجهة *DMZ* في المخرجات السابقة. هذا من خلال ربط تصميم tracer. تخبرك الأداة كيفية معالجة جدار الحماية لهذا النوع من محاولات الاتصال، والتي تتضمن كيفية توجيهها ومن أي واجهة.

تلميح: للحصول على معلومات إضافية حول ميزة "تعقب الحزمة"، ارجع إلى قسم التتبع مع حزم التتبع في دليل تكوين *سلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6*.

التقاط الحزمة

يمكن أن يلتقط جدار حماية ASA حركة مرور البيانات التي تدخل الواجهات أو تتركها. وظيفة الالتقاط هذه مفيدة للغاية لأنها يمكن أن تثبت بشكل قاطع ما إذا كانت حركة المرور تصل إلى جدار الحماية أو تغادر منه. يوضح المثال التالي تكوين إلتقطين يسمان **capd** و**capout** على الواجهات DMZ والخارجية، على التوالي. تستخدم أوامر الالتقاط كلمة أساسية مطابقة، والتي تتيح لك أن تكون محددا حول حركة المرور التي تريد إلتقاطها.

بالنسبة لبطاقة **التقاط** CAPD في هذا المثال، يشار إلى أنك تريد مطابقة حركة المرور التي تمت رؤيتها على واجهة DMZ (المدخل أو المخرج) التي تطابق مضيف 203.0.113.2 TCP 172.16.31.10/host. بمعنى آخر، أنت تريد التقاط أي حركة مرور TCP التي يتم إرسالها من المضيف 172.16.31.10 إلى المضيف 203.0.113.2، أو العكس. يسمح إستخدام الكلمة الأساسية المطابقة لجدار الحماية بالتقاط حركة المرور تلك بشكل ثنائي الإتجاه. لا يشير أمر الالتقاط الذي تم تعريفه للواجهة الخارجية إلى عنوان IP لخادم البريد الداخلي نظرا لأن جدار الحماية يقوم بإجراء NAT على عنوان IP لخادم البريد هذا. ونتيجة لذلك، لا يمكنك المطابقة مع عنوان IP ذلك الخادم. بدلا من ذلك، يستخدم المثال التالي الكلمة **any** للإشارة إلى أن جميع عناوين IP المحتملة ستطابق هذا الشرط.

بعد تكوين عمليات الالتقاط، يجب بعد ذلك محاولة إنشاء اتصال مرة أخرى والمتابعة لعرض عمليات الالتقاط باستخدام الأمر **show capture <capture_name>**. في هذا المثال، يمكنك أن ترى أن المضيف الخارجي كان قادرا على الاتصال بخادم البريد، كما هو موضح من خلال مصافحة TCP الثلاثية التي يتم رؤيتها في عمليات الالتقاط:

```
ASA#  capture capd interface dmz match tcp host 172.16.31.10 any
ASA#  capture capout interface outside match tcp any host 203.0.113.10

ASA#   show capture capd

packets captured 3

   :S 780523448 :172.16.31.10.25 < 203.0.113.2.65281       11:31:23.432655 :1
                 <win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK (0)780523448
  :S 2123396067 :203.0.113.2.65281 < 172.16.31.10.25       11:31:23.712518 :2
 <ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8 (0)2123396067
ack 2123396068 .172.16.31.10.25 < 203.0.113.2.65281       11:31:23.712884 :3
                                                                  win 32768

ASA# show capture capout

packets captured 3

  :S 1633080465 :203.0.113.10.25 < 203.0.113.2.65281       11:31:23.432869 :1
                <win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK (0)1633080465
    :S 95714629 :203.0.113.2.65281 < 203.0.113.10.25       11:31:23.712472 :2
   <ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8 (0)95714629
ack 95714630 . :203.0.113.10.25 < 203.0.113.2.65281        11:31:23.712914 :3
                                                                  win 32768
```

خادم البريد في الشبكة الداخلية

Packet-Tracer

هنا مثال ربط tracer إنتاج:

```
CLI : packet-tracer input outside tcp 203.0.113.2 1234 203.0.113.10 25 detailed

--Omitted--

                                                                Phase: 2
                                                              Type: UN-NAT
                                                           Subtype: static
                                                             Result: ALLOW
                                                                   :Config
                                                  object network obj-10.1.2.10
                                        nat (inside,outside) static 203.0.113.10
                                                          :Additional Information
                                              NAT divert to egress interface inside
                                            Untranslate 203.0.113.10/25 to 10.1.2.10/25

                                                                Phase: 3
                                                            Type: ACCESS-LIST
                                                                 Subtype: log
                                                              Result: ALLOW
                                                                   :Config
                                                 access-group smtp in interface outside
                                  access-list smtp extended permit tcp any4 host 10.1.2.10 eq smtp
                                                          :Additional Information
                                                  :Forward Flow based lookup yields rule
                                in  id=0x77dd2c50, priority=13, domain=permit, deny=false
hits=1, user_data=0x735dc880, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
                                     src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
                  dst ip/id=10.1.2.10, mask=255.255.255.255, port=25, tag=0, dscp=0x0
                                               input_ifc=outside, output_ifc=any
```

خادم البريد في الشبكة الخارجية

Packet-Tracer

هنا مثال ربط tracer إنتاج:

```
CLI :  packet-tracer input inside tcp 10.1.2.10 1234 203.1.113.10 25 detailed

--Omitted--

                                                                Phase: 2
                                                            Type: ROUTE-LOOKUP
                                                                Subtype: input
                                                              Result: ALLOW
                                                                   :Config
                                                          :Additional Information
                                                in 203.1.113.0 255.255.255.0 outside

                                                                Phase: 3
                                                              Type: NAT
                                                                   :Subtype
                                                              Result: ALLOW
                                                                   :Config
```

```
object network obj-10.1.2.0
nat (inside,outside) dynamic interface
:Additional Information
Dynamic translate 10.1.2.10/1234 to 203.0.113.1/1234
:Forward Flow based lookup yields rule
in id=0x778b14a8, priority=6, domain=nat, deny=false
hits=11, user_data=0x778b0f48, cs_id=0x0, flags=0x0, protocol=0
src ip/id=10.1.2.0, mask=255.255.255.0, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
input_ifc=inside, output_ifc=outside
```

معلومات ذات صلة

- رسائل Cisco ASA Series Syslog
- التقاط حزمة ASA باستخدام CLI ومثال تكوين ASDM
- دليل تكوين واجهة سطر الأوامر Cisco ASA Series، الإصدار 9.0 - تكوين كائن الشبكة NAT
- دعم & توثيق - سيسكو سيستمز

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).