Configurazione dell'ASA per l'accesso al server di posta SMTP nelle reti DMZ, interne ed esterne

Sommario

Introduzione

In questo documento viene descritto come configurare un'appliance Cisco Adaptive Security (ASA) per accedere a un server SMTP (Simple Mail Transfer Protocol) situato nella zona demilitarizzata (DMZ), nella rete interna o nella rete esterna.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA con software versione 9.1 o successive
- Cisco serie 2800C Router con software Cisco IOS® versione 15.1(4)M6

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

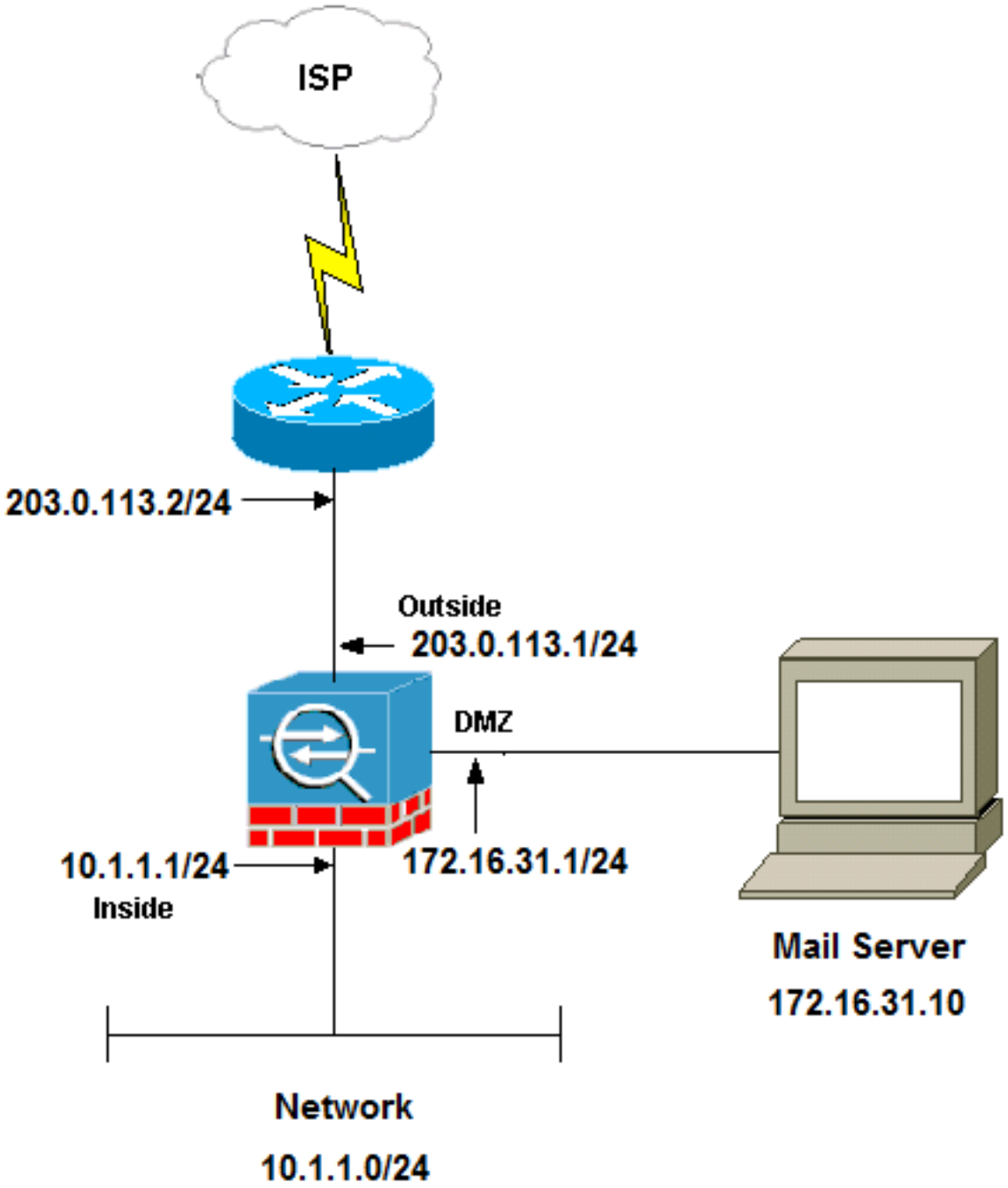
In questa sezione viene descritto come configurare l'ASA in modo che raggiunga il server di posta nella rete DMZ, nella rete interna o nella rete esterna.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Server di posta nella rete DMZ

Esempio di rete

La configurazione descritta in questa sezione utilizza la seguente configurazione di rete:



> **Nota:** Gli schemi di indirizzamento IP utilizzati in questo documento non sono legalmente indirizzabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

L'installazione di rete usata in questo esempio ha un'appliance ASA con una rete interna in **10.1.1.0/24** e una rete esterna in **203.0.113.0/24**. Il server di posta con indirizzo IP **172.16.31.10** si

trova nella rete DMZ. Affinché il server di posta sia accessibile dalla rete interna, è necessario configurare l'identità NAT (Network Address Translation).

Per consentire agli utenti esterni di accedere al server di posta, è necessario configurare un NAT statico e un elenco degli accessi, che nell'esempio riportato è **outside_int**, per consentire agli utenti esterni di accedere al server di posta e associare l'elenco degli accessi all'interfaccia esterna.

Configurazione ASA

Questa è la configurazione ASA dell'esempio:

```
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
```

Configurazione TLS ESMTP

Se si usa la crittografia Transport Layer Security (TLS) per la comunicazione e-mail, la funzione di ispezione Extended Simple Mail Transfer Protocol (ESMTP) (abilitata per impostazione predefinita) nell'appliance ASA scarta i pacchetti. Per consentire l'invio di e-mail con TLS abilitato, disabilitare la funzione di ispezione ESMTP come mostrato nell'esempio successivo.

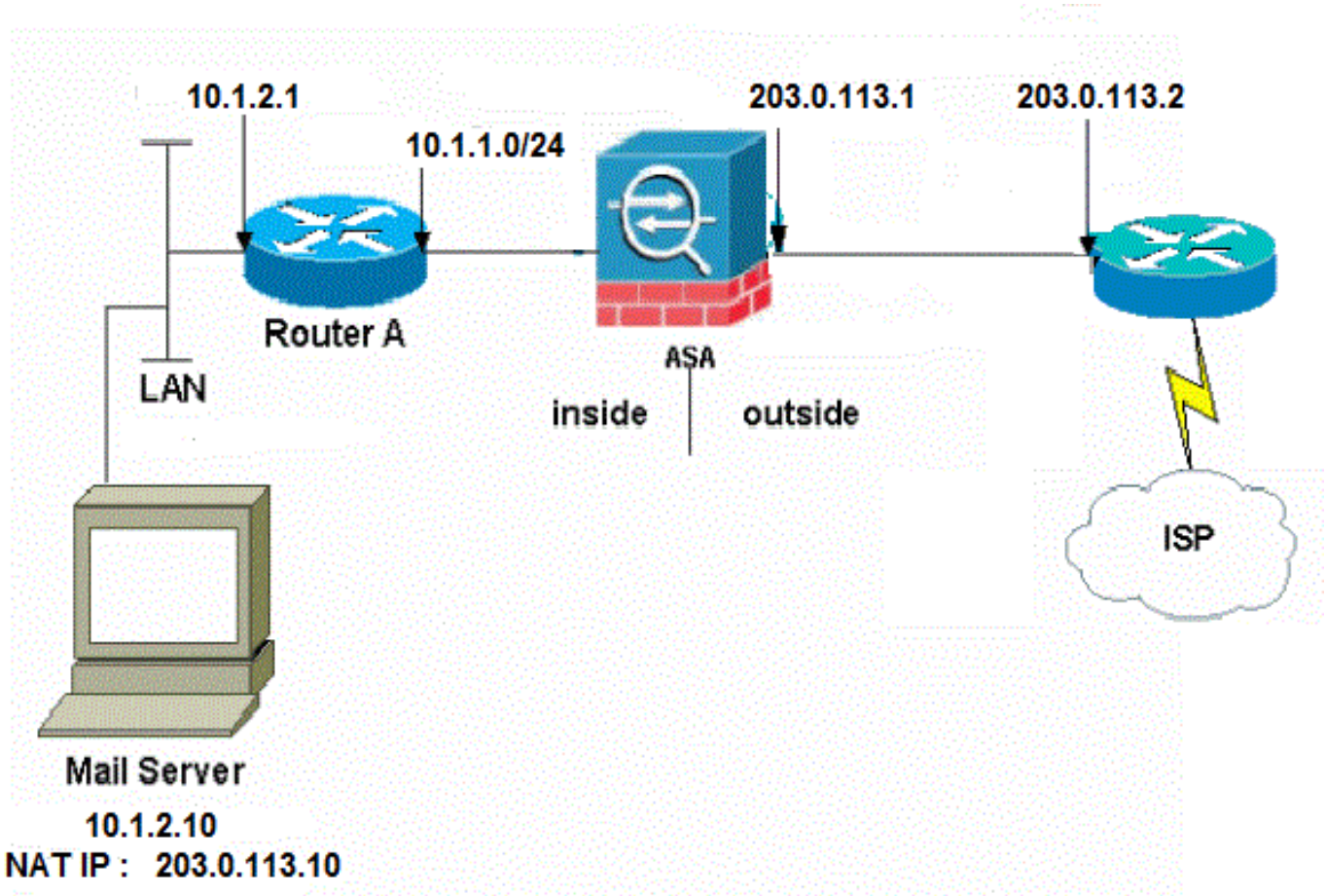
> **Nota:** per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtn08326 (solo utenti registrati).

```
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
```

Server di posta nella rete interna

Esempio di rete

La configurazione descritta in questa sezione utilizza la seguente configurazione di rete:



L'installazione della rete usata in questo esempio ha un'appliance ASA con una rete interna in **10.1.1.0/24** e una rete esterna in **203.0.113.0/24**. Il server di posta con indirizzo IP **10.1.2.10** si trova nella rete interna.

Configurazione ASA

Questa è la configurazione ASA dell'esempio:

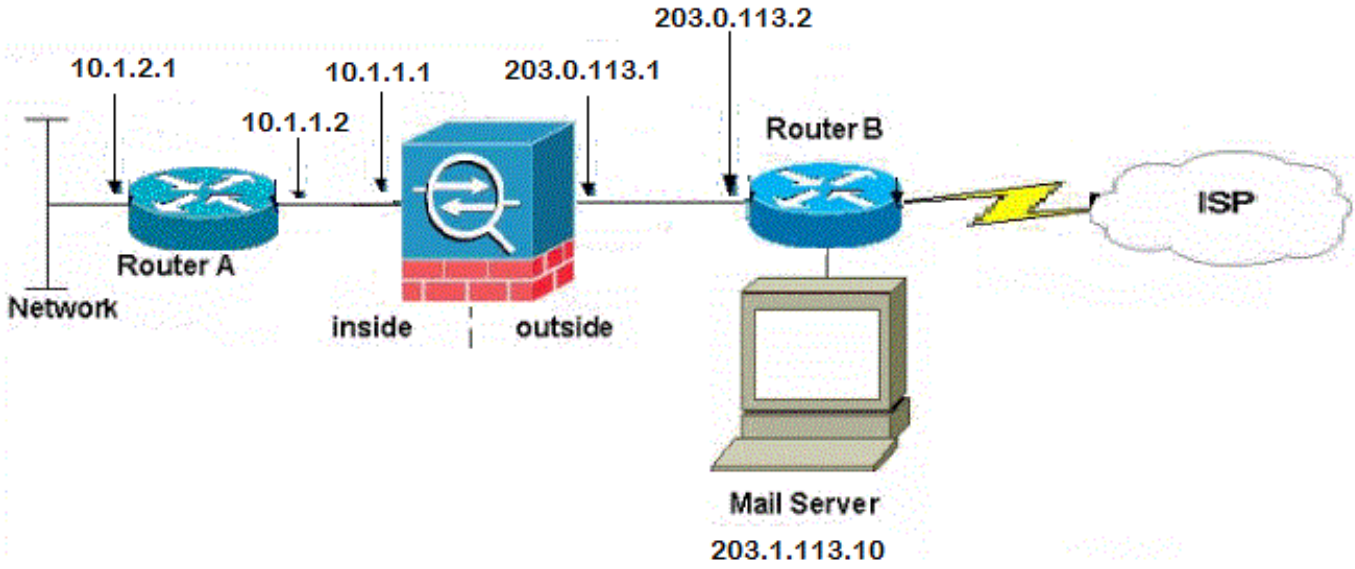
```
ASA#show run
: Saved
:
ASA Version 9.1(2)
!
--Omitted--
!

!--- 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
!--- 10.1.2.x network NATs (PAT) to 203.0.113.9 if
!--- 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
!--- 203.0.113.10 on the outside. These are the addresses to be used by
!--- 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
```

Server di posta nella rete esterna

Esempio di rete

La configurazione descritta in questa sezione utilizza la seguente configurazione di rete:



Configurazione ASA

Questa è la configurazione ASA dell'esempio:

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni contenute in questa sezione.

Server di posta nella rete DMZ

Ping TCP

Il comando ping TCP verifica una connessione su TCP (l'impostazione predefinita è Internet Control Message Protocol (ICMP)). Un ping TCP invia pacchetti SYN e considera riuscito il ping se il dispositivo di destinazione invia un pacchetto SYN-ACK. È possibile eseguire al massimo due ping TCP simultanei alla volta.

Di seguito è riportato un esempio:

```
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
```

Connessione

L'ASA è un firewall con stato e il traffico di ritorno dal server di posta può tornare indietro attraverso il firewall perché corrisponde a una connessione nella tabella delle connessioni del firewall. Il traffico che corrisponde a una connessione corrente può passare attraverso il firewall senza essere bloccato da un Access Control List (ACL) di interfaccia.

Nell'esempio successivo, il client sull'interfaccia esterna stabilisce una connessione con l'host 203.0.113.10 dell'interfaccia DMZ. Questa connessione viene effettuata con il protocollo TCP ed è rimasta inattiva per due secondi. I flag di connessione indicano lo stato corrente della connessione:

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

Registrazione

Il firewall ASA genera syslog durante il normale funzionamento. L'intervallo dei syslog è espresso in dettaglio in base alla configurazione di registrazione. Questo output mostra due syslog visualizzati al livello sei (il livello *informativo*) e al livello sette (il livello di *debug*):

```
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
(203.0.113.2/16678) to dmz:172.16.31.10/25 (203.0.113.10/25)
```

Il secondo syslog in questo esempio indica che il firewall ha creato una connessione nella relativa tabella di connessione per questo traffico specifico tra il client e il server. Se il firewall è stato configurato per bloccare il tentativo di connessione o altri fattori hanno impedito la creazione della connessione (vincoli di risorse o una possibile configurazione errata), il firewall non genererà un registro che indichi che la connessione è stata creata. Registra invece un motivo per cui la connessione viene negata o un'indicazione sul fattore che ha impedito la creazione della connessione.

Ad esempio, se l'ACL esterno non è configurato per autorizzare la porta 172.16.31.10 sulla porta 25, sarà possibile visualizzare questo registro quando il traffico viene rifiutato:

%ASA-4-106100: access-list outside_int negato da tcp outside/203.0.113.2(3756) ->

dmz/172.16.31.10(25) hit-cnt intervallo 5 300 secondi

Questo si verifica quando un ACL è mancante o non configurato correttamente, come mostrato di seguito:

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

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

Traduzioni NAT (Xlate)

Per confermare la creazione delle traduzioni, è possibile controllare la tabella Xlate (traduzione). Il comando **show xlate**, quando combinato con la parola chiave local e l'indirizzo IP dell'host interno, mostra tutte le voci presenti nella tabella di conversione per quell'host. L'output successivo mostra che è attualmente in corso una conversione per questo host tra la DMZ e le interfacce esterne. L'indirizzo IP del server DMZ viene convertito nell'indirizzo 203.0.113.10 in base alla configurazione precedente. I flag elencati (**s** in questo esempio) indicano che la traduzione è *statica*.

```
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
```

Server di posta nella rete interna

Ping TCP

Di seguito è riportato un esempio di output del ping 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
```

Connessione

Di seguito è riportato un esempio di verifica della connessione:

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

Registrazione

Di seguito è riportato un esempio di syslog:

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

Traduzioni NAT (Xlate)

Di seguito sono riportati alcuni esempi di output del comando **show nat detail** e **show xlate**:

```
ciscoasa(config)# show nat detail

Auto NAT Policies (Section 2)
1 (inside) to (outside) source static obj-10.1.2.10 203.0.113.10
   translate_hits = 0, untranslate_hits = 15
   Source - Origin: 10.1.2.10/32, 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

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

Server di posta nella rete esterna

Ping TCP

Di seguito è riportato un esempio di output del ping 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
```

Connessione

Di seguito è riportato un esempio di verifica della connessione:

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

Registrazione

Di seguito è riportato un esempio di syslog:

```
ciscoasa# show logging | i 203.1.113.10

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

Traduzioni NAT (Xlate)

Di seguito è riportato un esempio di output del comando **show xlate**:

```
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
0:00:04 timeout 0:00:30
```

Risoluzione dei problemi

L'appliance ASA fornisce diversi strumenti per risolvere i problemi di connettività. Se il problema persiste dopo aver verificato la configurazione e verificato gli output descritti nella sezione

precedente, questi strumenti e tecniche possono essere utili per determinare la causa dell'errore di connettività.

Server di posta nella rete DMZ

Packet-Tracer

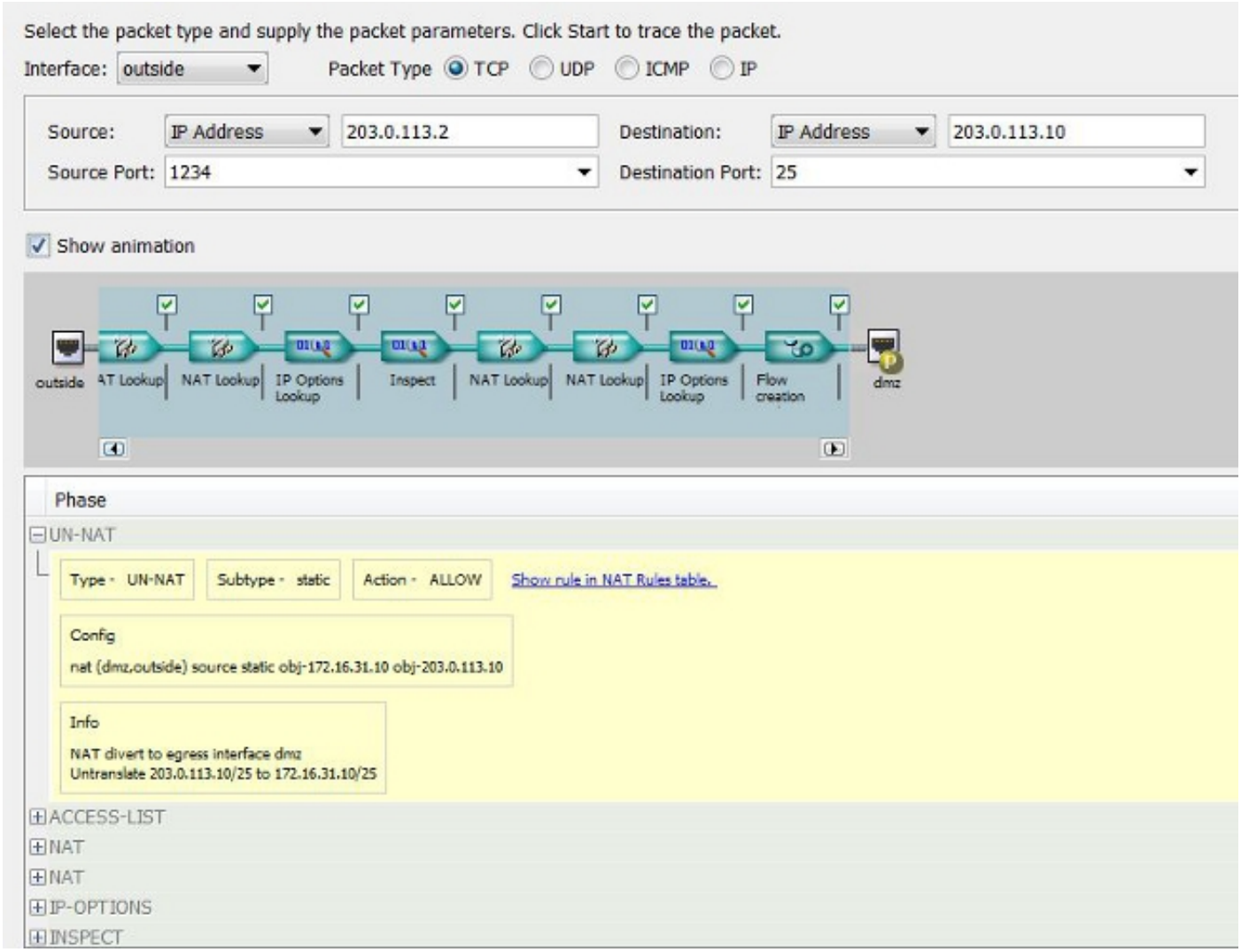
La funzionalità di tracciamento dei pacchetti sull'appliance ASA consente di specificare un pacchetto *simulato* e di visualizzare tutte le fasi, i controlli e le funzioni attraversati dal firewall quando elabora il traffico. Con questo strumento, è utile identificare un esempio di traffico che si ritiene *debba* essere autorizzato a passare attraverso il firewall e usare quel cinque tuple per simulare il traffico. Nell'esempio successivo, viene usato il packet tracer per simulare un tentativo di connessione che soddisfi questi criteri:

- Il pacchetto simulato arriva all'**esterno**.
- Il protocollo utilizzato è **TCP**.
- L'indirizzo IP del client simulato è **203.0.113.2**.
- Il client invia il traffico proveniente dalla porta **1234**.
- Il traffico è destinato a un server all'indirizzo IP **203.0.113.10**.
- Il traffico è destinato al porto **25**.

Di seguito è riportato un esempio di output del comando packet tracer:

```
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
```

Di seguito è riportato un esempio in Cisco Adaptive Security Device Manager (ASDM):



Si noti che nelle uscite precedenti non c'è alcun riferimento all'interfaccia *DMZ*. Questo è dovuto al design del tracer dei pacchetti. Lo strumento indica il modo in cui il firewall elabora il tipo di tentativo di connessione, incluse le modalità di instradamento e di uscita dell'interfaccia.

> **Suggerimento**: Per ulteriori informazioni sulla funzione packet tracer, consultare la sezione Traccia dei pacchetti con Packet Tracer nella *guida alla configurazione di Cisco ASA serie 5500 dalla CLI, versione 8.4 e 8.6*.

Acquisizione pacchetti

Il firewall ASA può acquisire il traffico in entrata o in uscita dalle interfacce. Questa funzionalità di acquisizione è molto utile perché può dimostrare in modo definitivo se il traffico arriva a un firewall o se ne esce. Nell'esempio seguente viene mostrata la configurazione di due clip denominate **capd** e **capout** rispettivamente sulla DMZ e sulle interfacce esterne. I comandi di acquisizione utilizzano una parola chiave match che consente di essere specifici sul traffico che si desidera acquisire.

Per il **capd di acquisizione** illustrato in questo esempio, viene indicato che si desidera far corrispondere il traffico visualizzato sull'interfaccia DMZ (in entrata o in uscita) che corrisponde all'host TCP 172.16.31.10/host 203.0.113.2. In altre parole, si desidera acquisire il traffico TCP inviato dall'host 172.16.31.10 all'host 203.0.113.2, o viceversa. L'utilizzo della parola chiave match consente al firewall di acquisire il traffico in modo bidirezionale. Il comando capture definito per

l'interfaccia esterna non fa riferimento all'indirizzo IP del server di posta interno perché il firewall esegue un NAT su tale indirizzo IP del server di posta. Di conseguenza, non è possibile stabilire una corrispondenza con l'indirizzo IP del server. Nell'esempio seguente viene invece utilizzata la parola **any** (qualsiasi) per indicare che tutti gli indirizzi IP possibili soddisferebbero questa condizione.

Dopo aver configurato le clip, tentare di stabilire nuovamente la connessione e procedere alla visualizzazione delle clip con il comando **show capture <nome_acquisizione>**. Nell'esempio, è possibile vedere che l'host esterno è stato in grado di connettersi al server di posta, come dimostra l'handshake TCP a tre vie mostrato nelle clip:

```
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

3 packets captured

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

ASA# show capture capout

3 packets captured

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

Server di posta nella rete interna

Packet-Tracer

Di seguito è riportato un esempio di output del comando packet tracer:

```
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
```

Server di posta nella rete esterna

Packet-Tracer

Di seguito è riportato un esempio di output del comando packet tracer:

```
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
```

Informazioni correlate

- Messaggi syslog Cisco serie ASA
- Esempio di acquisizione di pacchetti ASA con CLI e configurazione ASDM
- Cisco ASA Series CLI Configuration Guide, 9.0 - Configuring Network Object NAT

- Documentazione e supporto tecnico - Cisco Systems