Esempio di connessione di tre reti interne ad ASA versione 9.1(x) con configurazione Internet

Sommario

Introduzione

In questo documento viene spiegato come configurare Cisco Adaptive Security Appliance (ASA) versione 9.1(5) per l'utilizzo con tre reti interne. Per semplicità, sui router vengono usati percorsi statici.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stata usata la versione 9.1(5) di Cisco Adaptive Security Appliance (ASA).

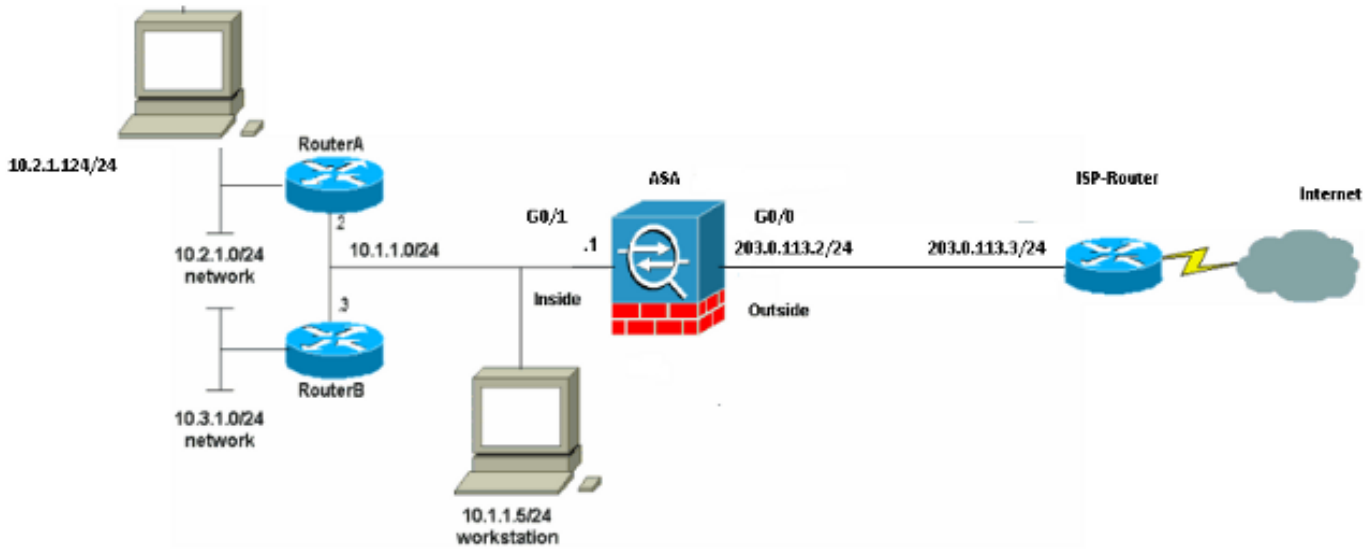
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

Esempio di rete



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

Configurazione ASA 9.1

Nel documento vengono usate queste configurazioni. se il dispositivo Cisco restituisce i risultati di un comando **write terminal**, è possibile usare Output Interpreter (solo utenti registrati) per visualizzare i potenziali errori e correggerli.

Configurazioni

- Configurazione router A
- Configurazione router B
- Configurazione di ASA revisione 9.1 e successive

Configurazione router 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#
```

Configurazione router 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#
```

Configurazione di ASA revisione 9.1 e successive

```
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
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Provare ad accedere a un sito Web tramite HTTP con un browser Web. In questo esempio viene usato un sito ospitato all'indirizzo 198.51.100.100. Se la connessione ha esito positivo, questo output può essere visualizzato sulla CLI di ASA.

Connessione

```
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
```

L'ASA è un firewall con stato e il traffico di ritorno dal server Web può attraversare nuovamente il

firewall perché corrisponde a una ***connessione*** nella tabella delle connessioni del firewall. Il traffico che corrisponde a una connessione già esistente viene autorizzato attraverso il firewall e non viene bloccato da un ACL di interfaccia.

Nell'output precedente, il client sull'interfaccia interna ha stabilito una connessione con l'host 198.51.100.100 dall'interfaccia esterna. Questa connessione viene effettuata con il protocollo TCP ed è rimasta inattiva per sei secondi. I flag di connessione indicano lo stato corrente della connessione. Per ulteriori informazioni sui flag di connessione, consultare Flag di connessione TCP ASA.

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)
```

Il firewall ASA genera syslog durante il normale funzionamento. L'intervallo dei syslog è espresso in dettaglio in base alla configurazione di registrazione. L'output mostra due syslog visualizzati al livello sei, o livello 'informativo'.

In questo esempio vengono generati due syslog. Il primo è un messaggio di registro che indica che il firewall ha creato una traduzione, in particolare una traduzione TCP dinamica (PAT). Indica l'indirizzo IP e la porta di origine, nonché l'indirizzo IP e la porta convertiti, quando il traffico attraversa le interfacce interna ed esterna.

Il secondo syslog indica che il firewall ha creato una connessione nella relativa tabella di connessione per il traffico specifico tra il client e il server. Se il firewall è stato configurato per bloccare questo 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. Viene invece registrato un motivo per cui la connessione viene negata o un'indicazione relativa al fattore che ha impedito la creazione della connessione.

Traduzioni 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
```

Nell'ambito di questa configurazione, PAT è configurato in modo da convertire gli indirizzi IP degli host interni in indirizzi instradabili su Internet. Per confermare la creazione di queste traduzioni, è possibile controllare la tabella delle traduzioni NAT (xlate). Il comando **show xlate,** se 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 precedente mostra che è attualmente presente una traduzione per questo host tra le interfacce interna ed esterna. L'indirizzo IP e la porta dell'host interno vengono convertiti nell'indirizzo 203.0.113.2 per ciascuna configurazione. I contrassegni elencati, o i, indicano che la traduzione è **dinamica** e una **cartina delle porte**. Per ulteriori

informazioni sulle diverse configurazioni NAT, vedere Informazioni su NAT.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

L'appliance ASA fornisce diversi strumenti per risolvere i problemi di connettività. Se il problema persiste dopo aver verificato la configurazione e verificato l'output elencato in precedenza, questi strumenti e tecniche possono aiutare a determinare la causa dell'errore di connettività.

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
```

La funzionalità di traccia 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 5-tuple per simulare il traffico. Nell'esempio precedente, il packet tracer viene usato per simulare un tentativo di connessione che soddisfa i seguenti criteri:

- Il pacchetto simulato arriva all'**interno**.
- Il protocollo utilizzato è **TCP**.
- L'indirizzo IP del client simulato è **10.2.1.124**.
- Il client invia il traffico proveniente dalla porta **1234**.
- Il traffico è destinato a un server all'indirizzo IP **198.51.100.100**.
- Il traffico è destinato al porto **80**.

Nel comando non è stata menzionata alcuna interfaccia **esterna**. 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 dall'interfaccia. Per ulteriori informazioni su packet tracer, vedere Analisi dei pacchetti con Packet Tracer.

Acquisisci

```
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>
```

Il firewall ASA può acquisire il traffico in entrata o in uscita dalle interfacce. Questa funzionalità di acquisizione è fantastica perché può dimostrare in modo definitivo se il traffico arriva a un firewall o se ne esce. Nell'esempio precedente è stata mostrata la configurazione di due clip denominate **capin** e **capout** rispettivamente sulle interfacce interna ed esterna. I comandi di acquisizione hanno utilizzato la parola chiave **match**, che consente di essere specifici sul traffico da acquisire.

Per il capin di acquisizione, è stato indicato che si desidera far corrispondere il traffico visualizzato sull'interfaccia interna (in entrata o in uscita) che corrisponde all'**host tcp 10.2.1.124 host 198.51.100.100**. In altre parole, si desidera acquisire tutto il traffico TCP inviato dall'**host 10.2.1.124** all'**host 198.51.100.100** 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 client interno perché il firewall esegue PAT su tale indirizzo IP del client. Di conseguenza, non è possibile **stabilire una corrispondenza** con l'indirizzo IP di quel client. Nell'esempio viene invece utilizzato **any** per indicare che tutti gli indirizzi IP possibili soddisferanno la condizione.

Dopo aver configurato le clip, tentare di stabilire nuovamente la connessione e continuare a visualizzarle con il comando **show capture *<nome_acquisizione>***. In questo esempio, è possibile notare che il client è stato in grado di connettersi al server come evidenziato dall'handshake TCP a 3 vie rilevato nelle acquisizioni.