Esempio di configurazione di ASA 8.4(x): connessione di una singola rete interna a Internet

Sommario

Introduzione

Questo documento descrive come configurare Cisco Adaptive Security Appliance (ASA) con la versione 8.4(1) per l'utilizzo su una singola rete interna.

Per ulteriori informazioni, fare riferimento al documento PIX/ASA: Esempio di connessione di una singola rete interna con configurazione Internet per la stessa configurazione sull'appliance ASA con la versione 8.2 e precedenti.

Prerequisiti

Requisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sull'appliance ASA con versione 8.4(1).

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.

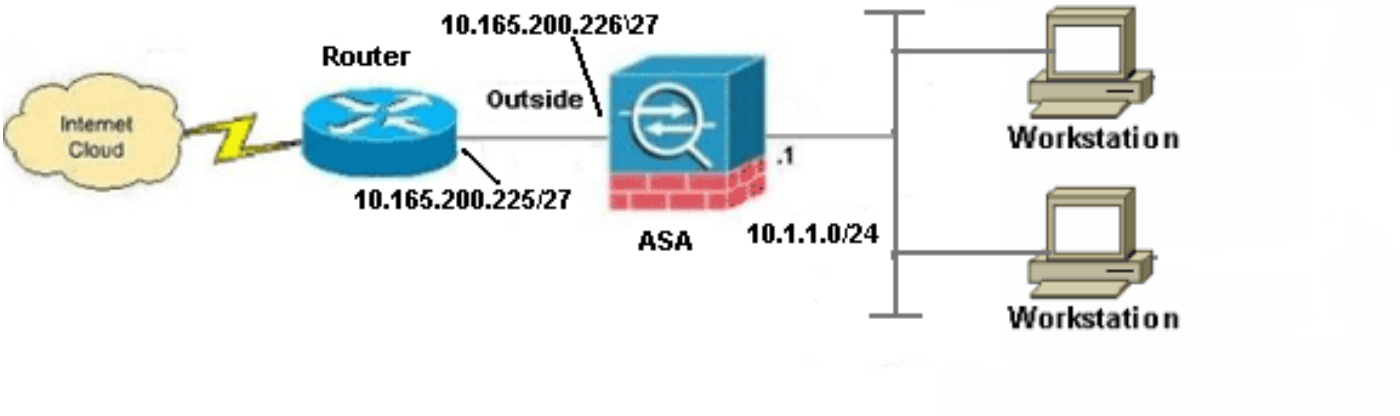
Configurazione

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 questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione 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 8.4

Nel documento vengono usate queste configurazioni:

- Configurazione router
- Configurazione di ASA 8.4 e versioni successive

Configurazione router

```
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
```

Configurazione di ASA 8.4 e versioni successive

```
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
```

> **Nota:** Per ulteriori informazioni sulla configurazione di Network Address Translation (NAT) e Port Address Translation (PAT) sull'appliance ASA versione 8.4, consultare le informazioni su NAT.
>
> Per ulteriori informazioni sulla configurazione degli elenchi degli accessi sull'appliance ASA versione 8.4, fare riferimento alle informazioni sugli elenchi degli accessi.

Verifica

Provare ad accedere a un sito Web tramite HTTP con un browser Web. Questo esempio usa un sito ospitato alla versione 198.51.100.100. Se la connessione ha esito positivo, questo output può essere visualizzato sulla CLI dell'ASA:

Connessione

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
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 preesistente può passare attraverso il firewall senza essere 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 | in 10.1.1.154

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

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:10.1.1.154/58799 (10.165.200.226/58799)
```

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 (Xlate)

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 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:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 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 delle traduzioni, è possibile controllare la tabella xlate (translation). 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 10.165.200.226 per ciascuna configurazione. I flag elencati, r i , indicano che la traduzione è **dinamica** e una **mappa di porta**. Ulteriori informazioni sulle diverse configurazioni NAT sono disponibili qui: Informazioni su NAT.

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 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 10.1.1.154 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
```

La funzionalità **packet tracer** sull'appliance ASA consente di specificare un pacchetto *simulato* e di verificare tutti i vari passaggi, controlli e 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 **10.1.1.154**.
- 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 Traccia dei pacchetti con Packet Tracer.

Acquisisci

```
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

3 packets captured

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



ASA# show capture capout

3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 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 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 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 10.1.1.154 host 198.51.100.100**. In altre parole, si desidera acquisire il traffico TCP inviato dall'**host 10.1.1.154** 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 nuovamente di stabilire una 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.

Informazioni correlate

- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems