ASA 8.3: Definizione e risoluzione dei problemi di connettività tramite Cisco Security Appliance

Sommario

Introduzione

La configurazione iniziale di una appliance Cisco Adaptive Security (ASA) prevede una policy di sicurezza predefinita che consente a tutti gli utenti interni di uscire e a nessuno dall'esterno di accedere. Se il sito richiede un criterio di protezione diverso, è possibile consentire agli utenti esterni di connettersi al server Web tramite l'appliance ASA.

Una volta stabilita la connettività di base tramite Cisco ASA, è possibile apportare modifiche alla configurazione del firewall. Verificare che le modifiche apportate alla configurazione dell'appliance ASA siano conformi ai criteri di sicurezza del sito.

Per ulteriori informazioni, fare riferimento al documento PIX/ASA: Stabilire e risolvere i problemi di connettività con Cisco Security Appliance per la stessa configurazione sull'appliance Cisco ASA con le versioni 8.2 e precedenti.

Prerequisiti

Requisiti

In questo documento si presume che alcune configurazioni di base siano già state completate sull'appliance Cisco ASA. Per esempi su una configurazione ASA iniziale, consultare i seguenti documenti:

- ASA 8.3(x): Connessione di una singola rete interna a Internet
- Configurazione del client PPPoE su un'appliance Cisco Adaptive Security (ASA)

Componenti usati

Per questo documento, è stata usata una Cisco Adaptive Security Appliance (ASA) con versione 8.3 e successive.

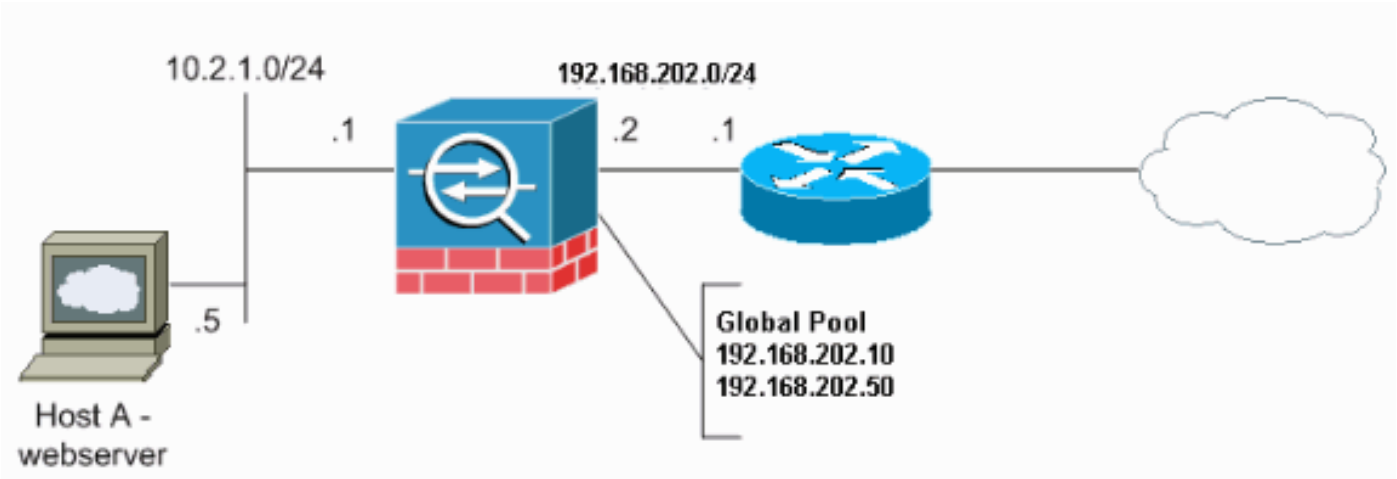
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Convenzioni

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

Come funziona la connettività tramite l'ASA

In questa rete, l'host A è il server Web con indirizzo interno 10.2.1.5. Al server Web viene assegnato un indirizzo esterno (tradotto) 192.168.202.5. Per accedere al server Web, gli utenti Internet devono puntare a 192.168.202.5. La voce DNS per il server Web deve essere tale indirizzo. Non sono consentite altre connessioni da Internet.



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

Configurazione della connettività con Cisco ASA

Per configurare la connettività tramite l'appliance ASA, completare la procedura seguente:

1. Creare un oggetto di rete che definisca la subnet interna e un altro oggetto di rete per l'intervallo del pool IP. Configurare NAT utilizzando i seguenti oggetti di rete:

```
object network inside-net
subnet 0.0.0.0 0.0.0.0
```

```
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. Assegnare un indirizzo statico tradotto per l'host interno a cui gli utenti Internet hanno accesso.

```
object network obj-10.2.1.5
  host 10.2.1.5
  nat (inside,outside) static 192.168.202.5
```

3. Usare il comando **access-list** per permettere agli utenti esterni di usare Cisco ASA. Utilizzare sempre l'indirizzo tradotto nel comando **access-list**.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
  access-group 101 in interface outside
```

Consenti traffico broadcast ARP

L'accessorio di sicurezza collega la stessa rete alle relative interfacce interne ed esterne. Poiché il firewall non è un hop indirizzato, è possibile introdurre facilmente un firewall trasparente in una rete esistente. Il reindirizzamento IP non è necessario. Il traffico IPv4 può passare attraverso il firewall trasparente automaticamente da un'interfaccia con sicurezza superiore a un'interfaccia con sicurezza inferiore, senza elenco degli accessi. I protocolli ARP (Address Resolution Protocol) sono consentiti attraverso il firewall trasparente in entrambe le direzioni senza un elenco degli accessi. Il traffico ARP può essere controllato mediante ispezione ARP. Per il traffico di layer 3 che passa da un'interfaccia di sicurezza bassa a una di sicurezza alta, è necessario un elenco degli accessi esteso.

Nota: l'appliance di sicurezza in modalità trasparente non passa pacchetti Cisco Discovery Protocol (CDP), pacchetti IPv6 o pacchetti che non hanno un EtherType valido maggiore o uguale a 0x600. Ad esempio, non è possibile passare pacchetti IS-IS. Viene fatta un'eccezione per le BDPU (Bridge Protocol Data Unit), che sono supportate.

Indirizzi MAC consentiti

Questi indirizzi MAC di destinazione sono consentiti attraverso il firewall trasparente. Gli indirizzi MAC non presenti in questo elenco vengono eliminati:

- VERO indirizzo MAC di destinazione broadcast uguale a FFFF.FFFF.FFFF
- Indirizzi MAC multicast IPv4 da 0100.5E00.0000 a 0100.5EFE.FFFF
- Indirizzi MAC multicast IPv6 da 333.0000.000 a 3333.FFFF.FFFF
- Indirizzo multicast BPDU uguale a 0100.0CCC.CCCD
- Indirizzi MAC multicast AppleTalk da 0900.0700.0000 a 0900.07FF.FFFF

Traffico non autorizzato in modalità router

In modalità router, alcuni tipi di traffico non possono passare attraverso l'appliance di sicurezza anche se sono consentiti nell'elenco degli accessi. Il firewall trasparente, tuttavia, può consentire

quasi tutto il traffico attraverso l'utilizzo di un elenco degli accessi esteso (per il traffico IP) o di un elenco degli accessi EtherType (per il traffico non IP).

Ad esempio, è possibile stabilire le adiacenze del protocollo di routing tramite un firewall trasparente. È possibile consentire il traffico OSPF (Open Shortest Path First), RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) o BGP (Border Gateway Protocol) tramite in base a un elenco di accessi esteso. Analogamente, protocolli quali HSRP (Hot Standby Router Protocol) o VRRP (Virtual Router Redundancy Protocol) possono passare attraverso l'appliance di sicurezza.

Il traffico non IP (ad esempio, AppleTalk, IPX, BPDU e MPLS) può essere configurato in modo da passare attraverso un elenco degli accessi EtherType.

Per le funzionalità non supportate direttamente sul firewall trasparente, è possibile consentire il passaggio del traffico in modo che i router a monte e a valle possano supportarne la funzionalità. Ad esempio, utilizzando un elenco degli accessi esteso, è possibile consentire il traffico DHCP (Dynamic Host Configuration Protocol) (anziché la funzionalità di inoltro DHCP non supportata) o il traffico multicast, come quello creato da IP/TV.

Risoluzione dei problemi di connettività

Se gli utenti Internet non possono accedere al sito Web, attenersi alla seguente procedura:

1. Verificare di aver immesso correttamente gli indirizzi di configurazione:Indirizzo esterno validoCorreggi indirizzo internoIndirizzo tradotto DNS esterno
2. Verificare la presenza di errori nell'interfaccia esterna.Cisco Security Appliance è preconfigurata per il rilevamento automatico della velocità e delle impostazioni duplex su un'interfaccia. Tuttavia, esistono diverse situazioni che possono ostacolare il completamento del processo di negoziazione automatica. Il risultato sono una mancata corrispondenza della velocità o del duplex (e un problema di prestazioni). Per le infrastrutture di rete mission-critical, Cisco codifica manualmente la velocità e il duplex su ciascuna interfaccia, in modo che non ci siano possibilità di errore. Questi dispositivi generalmente non si spostano. Pertanto, se le si configura correttamente, non è necessario modificarle.**Esempio:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex full
   asa(config-if)#speed 100
   asa(config-if)#exit
   ```

   In alcune situazioni, l'hardcode delle impostazioni di velocità e duplex porta alla generazione di errori. Pertanto, è necessario configurare l'interfaccia sull'impostazione predefinita della modalità di rilevamento automatico, come mostrato nell'esempio:**Esempio:**
   ```
   asa(config)#interface ethernet 0/0
   asa(config-if)#duplex auto
   asa(config-if)#speed auto
   asa(config-if)#exit
   ```

3. Se il traffico non invia né riceve dati tramite l'interfaccia dell'ASA o il router headend, provare a cancellare le statistiche ARP.
   ```
   asa#clear arp
   ```

4. Per verificare che la traduzione statica sia abilitata, utilizzare i comandi **show run object** e

show run static.Esempio:

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

In questo scenario, l'indirizzo IP esterno viene utilizzato come indirizzo IP mappato per il server Web.

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. Verificare che il percorso predefinito sul server Web punti all'interfaccia interna dell'ASA.
6. Controllare la tabella di traduzione utilizzando il comando show xlate per verificare se la traduzione è stata creata.
7. Usare il comando logging buffered per controllare i file di log e verificare se sono presenti richieste di negazione. (Cercare l'indirizzo tradotto e vedere se si vedono eventuali rifiuti.)
8. Utilizzare il comando capture:

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

Nota: questo comando genera una quantità significativa di output. Può causare il blocco o il ricaricamento di un router in caso di carichi di traffico elevati.

9. Se i pacchetti arrivano all'appliance ASA, verificare che il percorso tra l'appliance e il server Web sia corretto. Controllare i comandi route nella configurazione ASA.
10. Verificare se il proxy ARP è disattivato. Usare il comando show running-config system in ASA 8.3.In questo caso, il comando **sysopt noproxyarp outside** disabilita il protocollo ARP proxy:

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

Per riabilitare il proxy ARP, immettere questo comando in modalità di configurazione globale:

```
ciscoasa(config)#no sysopt noproxyarp outside
```

Quando un host invia traffico IP a un altro dispositivo sulla stessa rete Ethernet, l'host deve conoscere l'indirizzo MAC del dispositivo. ARP è un protocollo di layer 2 che risolve un indirizzo IP in un indirizzo MAC. Un host invia una richiesta ARP e chiede "Chi è questo indirizzo IP?". Il dispositivo che possiede l'indirizzo IP risponde: "Io possiedo quell'indirizzo IP; ecco il mio indirizzo MAC."La funzionalità ARP proxy consente all'appliance di sicurezza

di rispondere a una richiesta ARP per conto degli host sottostanti. A tale scopo, risponde alle richieste ARP per gli indirizzi statici mappati di tali host. L'appliance di sicurezza risponde alla richiesta con il proprio indirizzo MAC, quindi inoltra i pacchetti IP all'host interno appropriato.Ad esempio, nel diagramma di questo documento, quando viene effettuata una richiesta ARP per l'indirizzo IP globale del server Web, 192.168.202.5, l'appliance di sicurezza risponde con il proprio indirizzo MAC. Se il comando ARP proxy non è abilitato, gli host sulla rete esterna dell'appliance di sicurezza non potranno raggiungere il server Web inviando una richiesta ARP all'indirizzo 192.168.202.5. Per ulteriori informazioni sul comando **sysopt,** consultare la guida di riferimento del comando.

11. Se tutto sembra essere corretto e gli utenti non possono ancora accedere al server Web, aprire una richiesta di assistenza in Cisco Technical Support.

Messaggio di errore - %ASA-4-407001:

Alcuni host non sono in grado di connettersi a Internet e viene visualizzato il `messaggio di errore - %ASA-4-407001: Nega traffico per nome_interfaccia:indirizzo_interno dell'host locale.` Messaggio di errore `Numero massimo di licenze superato` ricevuto nel syslog. Come viene risolto questo errore?

Questo messaggio di errore viene visualizzato quando il numero di utenti supera il limite di utenti della licenza utilizzata. Per risolvere il problema, aggiornare la licenza a un numero maggiore di utenti. Può essere una licenza per 50, 100 o per un numero illimitato di utenti, in base alle esigenze.

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Avvisi sui prodotti per la sicurezza (comprese le appliance Cisco Adaptive Security (ASA))
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems