ASA 8.4(4): Configurazione NAT di alcune identità non consentita

Sommario

Introduzione

Le appliance ASA (Adaptive Security Appliance) con versione 8.4(4) o successive possono rifiutare alcune configurazioni NAT e visualizzare un messaggio di errore simile al seguente:

```
ERROR: <mapped address range> overlaps with <interface> standby interface
   address
ERROR: NAT Policy is not downloaded
```

Il problema può essere visualizzato anche quando si aggiorna l'ASA alla versione 8.4(4) o successive a partire da una versione precedente. Alcuni comandi NAT non sono più presenti nella configurazione di esecuzione dell'ASA. In questi casi, è consigliabile esaminare i messaggi della console stampati per verificare se sono presenti messaggi nel formato indicato.

Èpossibile notare anche che il traffico di alcune subnet dietro l'ASA potrebbe non passare più attraverso i tunnel VPN (Virtual Private Network) che terminano sull'appliance. Questo documento descrive come risolvere questi problemi.

Operazioni preliminari

Requisiti

Per risolvere il problema è necessario che siano soddisfatte le seguenti condizioni:

- ASA con versione 8.4(4) o successive o aggiornata alla versione 8.4(4) o successive da una versione precedente.
- ASA configurata con un indirizzo IP di standby su almeno una delle interfacce.
- Un NAT è configurato con l'interfaccia sopra indicata come interfaccia mappata.

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione hardware e software:

- ASA con versione 8.4(4) o successive

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Problema

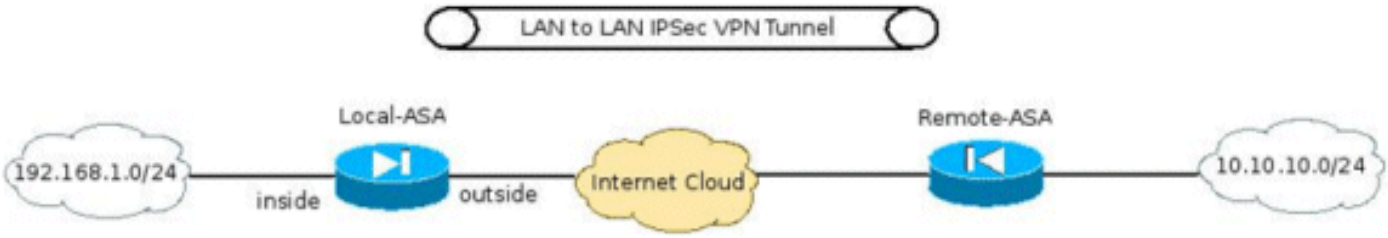
Come suggerisce il messaggio di errore, se l'intervallo di indirizzi mappati in un'istruzione NAT statica include l'indirizzo IP di standby assegnato all'interfaccia mappata, il comando NAT viene rifiutato. Questo comportamento è sempre esistito per il reindirizzamento delle porte statiche, ma è stato introdotto per le istruzioni NAT statiche uno-a-uno e con la versione 8.4(4) come correzione per l'ID bug Cisco CSCtw82147 (solo utenti registrati).

Questo bug è stato risolto perché prima della versione 8.4(4) l'ASA aveva consentito agli utenti di configurare l'indirizzo mappato in una configurazione NAT statica in modo che fosse lo stesso indirizzo IP di standby assegnato all'interfaccia mappata. Ad esempio, esaminare questo frammento di configurazione da un'appliance ASA:

```
ciscoasa(config)# show run int e0/0
!
interface Ethernet0/0
 nameif vm
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config)# show run nat
!
object network obj-10.76.76.160
 nat (tftp,vm) static 192.168.1.2
```

Anche se il comando è accettato, questa configurazione NAT non funzionerà mai in base alla progettazione. Di conseguenza, a partire dalla versione 8.4(4), l'ASA non consente di configurare una regola NAT di questo tipo.

Ne è derivato un altro problema imprevisto. Ad esempio, considerare lo scenario in cui l'utente ha un tunnel VPN che termina sull'appliance ASA e vuole che la subnet "interna" sia in grado di comunicare con la subnet VPN remota.



Tra gli altri comandi richiesti per configurare il tunnel VPN, una delle configurazioni più importanti è verificare che il traffico tra le subnet VPN non ottenga il protocollo NAT. Questa procedura viene implementata con la versione 8.3 e successive utilizzando un comando Manual/Twice NAT in

questo formato:

```
interface Ethernet0/0
 nameif inside
 security-level 0
 ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
object network obj-192.168.1.0
 description Inside subnet
 subnet 192.168.1.0 255.255.255.0
object network obj-10.10.10.0
 description Remote VPN subnet
 subnet 10.10.10.0 255.255.255.0
!
nat (inside,any) source static obj-192.168.1.0 obj-192.168.1.0 destination
   static obj-10.10.10.0 obj-10.10.10.0
!
object network obj-192.168.1.0
 nat (inside,outside) dynamic interface
```

Quando l'ASA è aggiornata alla versione 8.4(4) o successive, questo comando NAT non è presente nella configurazione di esecuzione dell'ASA e questo errore viene stampato sulla console dell'ASA:

```
ERROR: 192.168.1.0-192.168.1.255 overlaps with inside standby interface
   address
ERROR: NAT Policy is not downloaded
```

Di conseguenza, il traffico tra le subnet 192.168.1.0/24 e 10.10.10.0/24 non passerà più attraverso il tunnel VPN.

Soluzione

Esistono due possibili soluzioni per questa condizione:

- Rendere il comando NAT il più specifico possibile prima di eseguire l'aggiornamento a 8.4(4) in modo che l'interfaccia mappata non sia "any" (qualsiasi). Ad esempio, il comando NAT sopra riportato può essere modificato nell'interfaccia tramite la quale è possibile raggiungere la subnet VPN remota (denominata "external" nello scenario precedente):
  ```
  nat (inside,outside) source static obj-192.168.1.0 obj-192.168.1.0 destination
     static obj-10.10.10.0 obj-10.10.10.0
  ```
- Se la soluzione precedente non è disponibile, attenersi alla seguente procedura:Se l'appliance ASA è in esecuzione versione 8.4(4) o successive, rimuovere l'indirizzo IP di standby assegnato all'interfaccia.Applicare il comando NAT.Riapplicare l'indirizzo IP di standby sull'interfaccia.Ad esempio:
  ```
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
  ciscoasa(config-if)# exit
  ciscoasa(config)# nat (inside,any) 1 source static obj-192.168.1.0
     obj-192.168.1.0 destination static obj-10.10.10.0 obj-10.10.10.0
  ciscoasa(config)# interface Ethernet0/0
  ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  ```

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems