Autenticazione ASA su un'ASA in standby quando il dispositivo AAA si trova tramite un esempio di configurazione L2L

Sommario

Introduzione

In questo documento viene descritto come risolvere uno scenario in cui l'amministratore non è in grado di autenticarsi a un'appliance ASA (Standby Cisco Adaptive Security Appliance) in una coppia di failover a causa del fatto che il server di autenticazione, autorizzazione e accounting (AAA) si trova su una postazione remota tramite una connessione LAN a LAN (L2L).

Sebbene sia possibile utilizzare il fallback all'autenticazione LOCALE, è preferibile l'autenticazione RADIUS per entrambe le unità.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Failover ASA
- VPN
- NAT (Network Address Translation)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

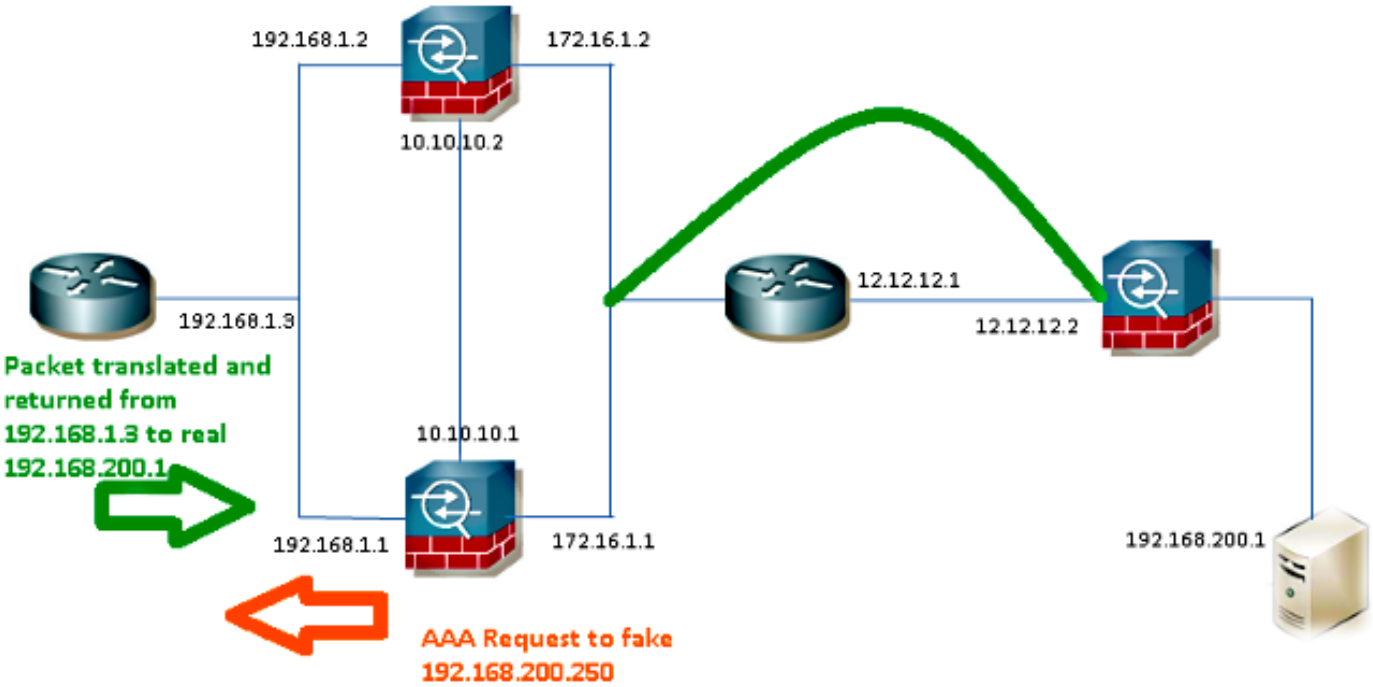
Configurazione

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

Esempio di rete

Il server RADIUS si trova all'esterno della coppia di failover e può essere raggiunto tramite un tunnel L2L fino alla versione 12.12.12.2. Questa è la causa del problema, in quanto l'ASA in standby cerca di raggiungerlo tramite la propria interfaccia esterna, ma in questo punto non è stato costruito alcun tunnel. per funzionare, è necessario inviare la richiesta all'interfaccia attiva in modo che il pacchetto possa passare attraverso la VPN, ma i percorsi vengono replicati dall'unità attiva.

In alternativa, è possibile usare un indirizzo IP falso per il server RADIUS sulle appliance ASA e indirizzarlo all'interno. Pertanto, l'indirizzo IP di origine e di destinazione del pacchetto può essere convertito su un dispositivo interno.



Router1

```
interface FastEthernet0/0
ip address 192.168.1.3 255.255.255.0
no ip redirects
no ip unreachables
```

```
ip nat enable
duplex auto
speed auto

ip access-list extended NAT
permit ip 192.168.1.0 0.0.0.255 host 192.168.200.250

ip nat source list NAT interface FastEthernet0/0 overload
ip nat source static 192.168.200.1 192.168.200.250

ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ASA

```
aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 192.168.200.250
timeout 3
key *****
authentication-port 1812
accounting-port 1813

aaa authentication serial console LOCAL
aaa authentication ssh console RADIUS LOCAL
aaa authentication telnet console RADIUS LOCAL
aaa authentication http console RADIUS LOCAL
aaa authentication enable console RADIUS LOCAL

route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
route inside 192.168.200.250 255.255.255.255 192.168.1.3 1
```

> **Nota:** Nell'esempio è stato usato l'indirizzo IP **192.168.200.250**, ma qualsiasi indirizzo IP inutilizzato funziona.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

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.**

Router

```
Router#   show ip nat nvi tra
Pro Source global Source local Destin local Destin global
udp 192.168.1.3:1025 192.168.1.1:1025 192.168.200.250:1812 192.168.200.1:1812
--- 192.168.200.1 192.168.2.1 --- ---
--- 192.168.200.250 192.168.200.1 --- ---
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.