es3 iptables

Vediamo nel dettaglio cosa richiede il problema e come le regole `iptables` proposte soddisfano i requisiti.

Obiettivo del Problema

1. **Client deve potersi connettere solo via SSH al server.**
2. **Server deve poter ricevere connessioni SSH solo dal client.**

Considerazioni di NAT

- **DNAT su R1**: Il client si connette a R1, che esegue il DNAT per inoltrare la connessione SSH al server.
- **SNAT su R2**: Il server vede la connessione SSH come proveniente da R2, non direttamente dal client.

Regole sul Client

Il client si connette a R1 (192.168.10.254) per stabilire una connessione SSH con il server. Le regole devono permettere questa connessione e le risposte, bloccando tutto il resto eccetto il traffico locale.

Regole `iptables` sul Client

```
iptables -I OUTPUT -d 192.168.10.254 -p tcp --dport 22 -j A
CCEPT
iptables -I INPUT -s 192.168.10.254 -p tcp --sport 22 -m st
ate --state ESTABLISHED -j ACCEPT
iptables -I INPUT -i lo -j ACCEPT
iptables -I OUTPUT -o lo -j ACCEPT
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

Spiegazione delle Regole sul Client

1. **Permetti traffico SSH in uscita verso R1**:

```
iptables -I OUTPUT -d 192.168.10.254 -p tcp --dport 22 -
j ACCEPT
```

Questa regola permette al client di iniziare connessioni SSH verso R1 sulla porta 22.

- `I OUTPUT`: Inserisce una regola nella catena OUTPUT per il traffico in uscita.
- `d 192.168.10.254`: Specifica l'indirizzo di destinazione come 192.168.10.254 (R1).
- `p tcp --dport 22`: Limita la regola al traffico TCP diretto alla porta 22 (SSH).
- `j ACCEPT`: Accetta il traffico che soddisfa i criteri specificati.

2. **Permetti risposte SSH in ingresso da R1**:

```
iptables -I INPUT -s 192.168.10.254 -p tcp --sport 22 -m
state --state ESTABLISHED -j ACCEPT
```

Questa regola permette di accettare i pacchetti di risposta SSH provenienti da R1 se la connessione è già stabilita.

- `I INPUT`: Inserisce una regola nella catena INPUT per il traffico in entrata.
- `s 192.168.10.254`: Specifica l'indirizzo sorgente come 192.168.10.254 (R1).
- `p tcp --sport 22`: Limita la regola al traffico TCP proveniente dalla porta 22.
- `m state --state ESTABLISHED`: Applica la regola solo a connessioni già stabilite.
- `j ACCEPT`: Accetta il traffico che soddisfa i criteri specificati.

3. **Permetti traffico locale in ingresso**:

```
iptables -I INPUT -i lo -j ACCEPT
```

Questa regola permette il traffico che utilizza l'interfaccia di loopback (`lo`).

- `i lo` : Si riferisce all'interfaccia di loopback (`lo`), utilizzata per il traffico locale all'interno del sistema.
- `j ACCEPT`: Accetta il traffico che passa attraverso l'interfaccia di loopback.

4. **Permetti traffico locale in uscita**:

```
iptables -I OUTPUT -o lo -j ACCEPT
```

   Questa regola permette il traffico che utilizza l'interfaccia di loopback (`lo`).

5. **Imposta politica predefinita DROP per INPUT**:

```
iptables -P INPUT DROP
```

   Questa regola imposta la politica predefinita per la catena `INPUT` a DROP, bloccando tutto il traffico in ingresso non esplicitamente permesso.

   - `-P INPUT DROP` : Imposta le politiche predefinite delle catene INPUT su DROP, bloccando tutto il traffico non specificamente permesso da altre regole.

6. **Imposta politica predefinita DROP per OUTPUT**:

```
iptables -P OUTPUT DROP
```

   Questa regola imposta la politica predefinita per la catena `OUTPUT` a DROP, bloccando tutto il traffico in uscita non esplicitamente permesso.

Regole sul Server

Il server riceve connessioni SSH che appaiono provenire da R2 (192.168.20.254) a causa del SNAT. Le regole devono permettere queste connessioni e le risposte, bloccando tutto il resto eccetto il traffico locale.

Regole `iptables` sul Server

```
iptables -I INPUT -s 192.168.20.254 -p tcp --dport 22 -j AC
CEPT
iptables -I OUTPUT -d 192.168.20.254 -p tcp --sport 22 -m s
tate --state ESTABLISHED -j ACCEPT
```

```
iptables -I INPUT -i lo -j ACCEPT
iptables -I OUTPUT -o lo -j ACCEPT
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

Spiegazione delle Regole sul Server

1. **Permetti traffico SSH in ingresso da R2**:

   ```
   iptables -I INPUT -s 192.168.20.254 -p tcp --dport 22 -j ACCEPT
   ```

   Questa regola permette al server di accettare connessioni SSH provenienti da R2 sulla porta 22.

   - `I INPUT`: Inserisce una regola nella catena INPUT per il traffico in entrata.
   - `s 192.168.20.254`: Specifica l'indirizzo sorgente come 192.168.20.254 (R2).
   - `p tcp --dport 22`: Limita la regola al traffico TCP diretto alla porta 22 (SSH).
   - `j ACCEPT`: Accetta il traffico che soddisfa i criteri specificati.

   NB: Il problema richiede che il server debba solo poter ricevere connessioni SSH dal client, ma a causa del NAT, il client sarà visto dal server come proveniente da R2. Di conseguenza, le regole devono riflettere questa realtà falsata.

2. **Permetti risposte SSH in uscita verso R2**:

   ```
   iptables -I OUTPUT -d 192.168.20.254 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
   ```

   Questa regola permette di inviare pacchetti di risposta SSH verso R2 se la connessione è già stabilita.

   - `I OUTPUT`: Inserisce una regola nella catena OUTPUT per il traffico in uscita.

- `d 192.168.20.254`: Specifica l'indirizzo di destinazione come 192.168.20.254 (R2).
- `p tcp --sport 22`: Limita la regola al traffico TCP proveniente dalla porta 22.
- `m state --state ESTABLISHED`: Applica la regola solo a connessioni già stabilite.
- `j ACCEPT`: Accetta il traffico che soddisfa i criteri specificati.

3. **Permetti traffico locale in ingresso**:

```
iptables -I INPUT -i lo -j ACCEPT
```

Questa regola permette il traffico che utilizza l'interfaccia di loopback (`lo`).

- `i lo` e `o lo`: Si riferiscono all'interfaccia di loopback (`lo`), utilizzata per il traffico locale all'interno del sistema.
- `j ACCEPT`: Accetta il traffico che passa attraverso l'interfaccia di loopback.

4. **Permetti traffico locale in uscita**:

```
iptables -I OUTPUT -o lo -j ACCEPT
```

Questa regola permette il traffico che utilizza l'interfaccia di loopback (`lo`).

5. **Imposta politica predefinita DROP per INPUT**:

```
iptables -P INPUT DROP
```

Questa regola imposta la politica predefinita per la catena `INPUT` a DROP, bloccando tutto il traffico in ingresso non esplicitamente permesso.

6. **Imposta politica predefinita DROP per OUTPUT**:

```
iptables -P OUTPUT DROP
```

Questa regola imposta la politica predefinita per la catena `OUTPUT` a DROP, bloccando tutto il traffico in uscita non esplicitamente permesso.

- `-P INPUT DROP` e `-P OUTPUT DROP`: Imposta le politiche predefinite delle catene INPUT e OUTPUT su DROP, bloccando tutto il traffico non specificamente permesso da altre regole.

Riepilogo

Le regole `iptables` configurate sul client e sul server assicurano che:

- **Il client** può iniziare connessioni SSH solo verso R1 e ricevere risposte da R1.
- **Il server** può accettare connessioni SSH solo da R2 e inviare risposte a R2.
- Tutto il traffico non locale è bloccato, garantendo che il client possa solo connettersi al server tramite SSH e il server possa solo ricevere connessioni SSH dal client.

In questo modo, anche se il NAT cambia l'apparenza della sorgente e della destinazione del traffico, le regole imposte realizzano il vincolo richiesto: consentire solo connessioni SSH specifiche e bloccare tutto il resto.