es 2 iptables

Andiamo passo passo per capire cosa bisogna fare nel dettaglio.

Scenario e Obiettivi

Hai due router, R1 e R2, e un server. Vuoi:

1. Rimuovere dal server una regola di routing di default che instrada tutto il traffico attraverso R2.
2. Configurare R2 in modo che il traffico SSH in arrivo tramite la VPN e diretto al server venga mascherato (NAT).

Passo 1: Rimozione della Regola di Routing dal Server

La prima cosa da fare è rimuovere dal server la regola di routing di default che instrada tutto il traffico attraverso R2. Attualmente, questa regola è configurata per instradare il traffico tramite l'indirizzo IP 192.168.20.254 (R2).

▼ come si determina IP del gateway che il server usa come default?

Per determinare l'IP del gateway che il server utilizza come default, si può eseguire una serie di comandi e passaggi sul server stesso.

1. Verifica della Route di Default Attuale

Sul server, esegui il seguente comando per visualizzare la route di default attuale:

```
ip route
```

Oppure:

```
route -n
```

Questi comandi ti mostreranno le rotte di rete attualmente configurate. Cerca una riga che inizi con `default` o `0.0.0.0` (che indica la route di default). Dovrebbe apparire qualcosa del genere:

```
default via 192.168.20.254 dev eth0
```

Oppure:

```
0.0.0.0         192.168.20.254  0.0.0.0         UG    0
0        0 eth0
```

In entrambi i casi, `192.168.20.254` è l'IP del gateway di default.

2. Conferma dell'IP del Gateway R2

Per confermare che l'IP `192.168.20.254` corrisponde effettivamente a R2, puoi eseguire un ping o un traceroute verso quell'IP:

```
ping 192.168.20.254
```

Oppure:

```
traceroute 192.168.20.254
```

Se R2 risponde ai ping o il traceroute mostra che `192.168.20.254` è raggiungibile come primo hop, allora puoi essere sicuro che `192.168.20.254` è l'IP di R2.

3. Verifica delle Configurazioni di Rete

Puoi anche verificare le configurazioni di rete del server, come il file `/etc/network/interfaces` (su sistemi Debian/Ubuntu) o `/etc/sysconfig/network-scripts/ifcfg-<interface>` (su sistemi Red Hat/CentOS), per vedere se l'IP di default è specificato lì.

Esempio per Debian/Ubuntu:

```
cat /etc/network/interfaces
```

Potresti vedere qualcosa del genere:

```
auto eth0
iface eth0 inet static
    address 192.168.20.10
    netmask 255.255.255.0
    gateway 192.168.20.254
```

Riepilogo dei Passi

1. **Controllo delle rotte attuali**:

   ```
   ip route
   ```

   Oppure:

   ```
   route -n
   ```

2. **Ping o traceroute per conferma**:

   ```
   ping 192.168.20.254
   ```

   Oppure:

   ```
   traceroute 192.168.20.254
   ```

3. **Verifica delle configurazioni di rete**:

   ```
   cat /etc/network/interfaces
   ```

   Oppure:

   ```
   cat /etc/sysconfig/network-scripts/ifcfg-<interface>
   ```

Seguendo questi passaggi, sarai in grado di identificare con certezza l'IP del gateway utilizzato come default dal server.

Comando per Rimuovere la Regola di Routing

Sul server, esegui il seguente comando:

```
ip route del default via 192.168.20.254
```

Spiegazione

- `ip route del default`: Questo comando indica di eliminare la rotta di default.

- `via 192.168.20.254`: Specifica l'indirizzo del gateway (R2) tramite cui la rotta di default è attualmente impostata.

Dettagli del Comando

- `ip`: Questo è il comando principale utilizzato per configurare e mostrare le tabelle di routing, le interfacce di rete, i dispositivi e i tunnel IP.
- `route`: Specifica che stiamo lavorando con le tabelle di routing.
- `del`: Indica che vogliamo eliminare una specifica route.
- `default`: Si riferisce alla route di default. La route di default è utilizzata per instradare il traffico verso destinazioni non coperte da altre rotte specifiche. In altre parole, se un pacchetto non trova una route specifica nella tabella di routing, verrà instradato tramite la route di default.
- `via 192.168.20.254`: Specifica che la route di default da eliminare è quella che instrada il traffico attraverso l'indirizzo IP 192.168.20.254, che è l'IP del gateway.

Passo 2: Configurazione del NAT su R2

Ora, devi configurare R2 per mascherare (NAT) il traffico SSH in arrivo attraverso la VPN e diretto al server, impostando l'indirizzo sorgente come 192.168.20.254.

Comando per Configurare il NAT su R2

Sul router R2, esegui il seguente comando `iptables`:

```
iptables -t nat -I POSTROUTING -s 192.168.10.0/24 -d 192.16
8.20.0/24 -j SNAT --to-source 192.168.20.254
```

▼ come trovare gli IP delle reti sorgente e destinazione?

Per determinare che gli indirizzi sorgente e destinazione sono `192.168.10.0/24` e `192.168.20.0/24`, devi esaminare la configurazione di rete del server e dei router coinvolti (R1 e R2). Di seguito è riportata una guida dettagliata per identificare e verificare questi indirizzi:

Passaggio 1: Verifica delle Interfacce di Rete sul Server

Utilizzando `ip addr`

Esegui il seguente comando sul server per visualizzare le informazioni sulle interfacce di rete e gli indirizzi IP configurati:

```
ip addr
```

Questo comando mostrerà un output simile a questo:

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdis
c pfifo_fast state UP qlen 1000
    inet 192.168.20.1/24 brd 192.168.20.255 scope global
eth0
    ...
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdis
c pfifo_fast state UP qlen 1000
    inet 192.168.10.1/24 brd 192.168.10.255 scope global
eth1
    ...
```

In questo esempio, puoi vedere che l'interfaccia `eth0` è configurata con un indirizzo IP nella rete `192.168.20.0/24` e l'interfaccia `eth1` è configurata con un indirizzo IP nella rete `192.168.10.0/24`.

Passaggio 2: Verifica della Tabella di Routing sul Server Utilizzando `ip route`

Esegui il seguente comando per visualizzare la tabella di routing del server:

```
ip route
```

Questo comando mostrerà un output simile a questo:

```
default via 192.168.20.254 dev eth0
192.168.10.0/24 dev eth1 proto kernel scope link src 19
2.168.10.1
192.168.20.0/24 dev eth0 proto kernel scope link src 19
2.168.20.1
```

Questo output mostra che il traffico verso la rete `192.168.10.0/24` viene instradato tramite l'interfaccia `eth1` e il traffico verso la rete `192.168.20.0/24` viene instradato tramite l'interfaccia `eth0`.

Passaggio 3: Verifica delle Configurazioni di Rete sui Router (R1 e R2)

Se hai accesso ai router, puoi eseguire comandi simili per verificare le configurazioni delle loro interfacce di rete e delle tabelle di routing.

Accesso a R1 e R2

Per accedere alla console dei router, puoi utilizzare SSH o accedere fisicamente ai dispositivi. Una volta connesso, puoi eseguire comandi come `ip addr` e `ip route` (se il router utilizza un sistema operativo basato su Linux) per visualizzare le configurazioni.

Esempio di Comando su un Router

Esegui il seguente comando per visualizzare le interfacce di rete su un router basato su Linux:

```
ip addr
```

E il seguente comando per visualizzare la tabella di routing:

```
ip route
```

Passaggio 4: Verifica del Traffico SSH Attraverso la VPN

Per confermare che il traffico SSH in arrivo attraverso la VPN è diretto al server, puoi controllare le regole di firewall e NAT sui router. Ad esempio, se hai configurato una regola di NAT per mascherare il traffico SSH, dovresti vedere qualcosa di simile a questa regola `iptables` su R2:

```
iptables -t nat -I POSTROUTING -s 192.168.10.0/24 -d 19
2.168.20.0/24 -j SNAT --to-source 192.168.20.254
```

Riepilogo dei Passaggi

1. **Verifica delle Interfacce di Rete sul Server**:

```
ip addr
```

2. **Verifica della Tabella di Routing sul Server**:

```
ip route
```

3. **Verifica delle Configurazioni di Rete sui Router**:
   - Accesso ai router tramite console.
   - Utilizzo di comandi simili a quelli usati sul server per visualizzare le configurazioni di rete.
4. **Verifica delle Regole di NAT**:
   - Controllo delle regole di firewall e NAT sui router per confermare il traffico SSH.

Seguendo questi passaggi, sarai in grado di identificare e verificare che le reti sorgente e destinazione sono `192.168.10.0/24` e `192.168.20.0/24`.

Spiegazione

- `iptables`: Strumento per configurare le tabelle del firewall di Linux.
- `t nat`: Specifica che la regola è per la tabella NAT.
- `I POSTROUTING`: Inserisce la regola nella catena `POSTROUTING`, che è utilizzata per manipolare i pacchetti dopo che sono stati instradati.
- `s 192.168.10.0/24`: La regola si applica ai pacchetti con indirizzo sorgente nella rete 192.168.10.0/24.
- `d 192.168.20.0/24`: La regola si applica ai pacchetti con indirizzo di destinazione nella rete 192.168.20.0/24.
- `j SNAT`: Indica che si sta facendo Source NAT, ovvero si sta cambiando l'indirizzo sorgente dei pacchetti.
- `-to-source 192.168.20.254`: Specifica il nuovo indirizzo sorgente da usare per i pacchetti NAT-tati.

Effetti delle Modifiche

- **Rimozione della Regola di Routing sul Server**: Ora il server non utilizzerà più R2 come gateway di default. Questo potrebbe significare che il server userà un'altra route di default o un altro gateway se configurato.
- **NAT su R2**: Tutto il traffico SSH proveniente dalla rete 192.168.10.0/24 e diretto alla rete 192.168.20.0/24 avrà l'indirizzo sorgente modificato in 192.168.20.254. Questo mascheramento può essere utile per una serie di motivi, come semplificare le regole del firewall sul server o evitare problemi di routing.

Considerazioni Finali

1. **Persistenza delle Regole**: Le modifiche effettuate con `ip route` e `iptables` non sono persistenti e andranno perse al riavvio. Per renderle persistenti, devi aggiungere i comandi ai file di configurazione appropriati del sistema operativo.
2. **Backup delle Configurazioni**: Prima di apportare modifiche, è sempre una buona pratica fare un backup delle configurazioni correnti, nel caso sia necessario ripristinarle.

Ecco come puoi salvare le regole di iptables su R2:

```
# Salvare le regole attuali in un file
iptables-save > /etc/iptables/rules.v4
```

E ripristinarle al boot (esempio per sistemi basati su Debian/Ubuntu):

```
# Installare iptables-persistent
apt-get install iptables-persistent

# Salvare le regole
netfilter-persistent save
```

Con queste istruzioni dettagliate, dovresti essere in grado di rimuovere la regola di routing di default dal server e configurare correttamente il NAT su R2.