Gestione del firewall sulle VPS Debian/Ubuntu

Christian Cantinelli - 2026-05-29 - Server Virtuali/Cloud

Per motivi di sicurezza, tutte le VPS Debian e Ubuntu vengono fornite con un firewall software basato su **iptables** già configurato e attivo.

Configurazione predefinita

Al momento dell'attivazione:

- Tutte le connessioni in ingresso sono bloccate.
- È consentito il traffico relativo a connessioni già stabilite.
- È consentito il traffico locale (lo).
- È aperta esclusivamente la porta **SSH indicata nell'email di attivazione del servizio.**

La configurazione del firewall è memorizzata nel file:

```
/etc/iptables/rules.v4
```

Dopo aver apportato modifiche al file, è necessario riavviare il servizio per applicarle:

```
systemctl restart netfilter-persistent
```

Oppure:

```
service netfilter-persistent restart
```

Apertura delle porte HTTP e HTTPS (80 e 443)

Per pubblicare un sito web, aggiungere le seguenti regole prima della regola finale di REJECT:

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
```

Esempio:

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT

-A INPUT -j REJECT --reject-with icmp-host-prohibited
```

Limitare l'accesso SSH ad un singolo indirizzo IP

Supponiamo che la porta SSH assegnata sia la 22 e che si desideri consentire l'accesso esclusivamente dall'IP 203.0.113.10.

Note

Attenzione: le VPS vengono fornite con una **porta SSH personalizzata**, diversa dalla porta standard 22.

La porta SSH corretta viene indicata nella **mail di attivazione del servizio**. Leggere attentamente la mail

prima di modificare le regole del firewall o tentare l’accesso SSH.

Sostituire la regola esistente:

```
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

con:

```
-A INPUT -p tcp -s 203.0.113.10 -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

In questo modo solo l'indirizzo IP specificato potrà collegarsi via SSH.

Chiudere completamente l'accesso SSH

Per bloccare completamente l'accesso SSH è sufficiente commentare o rimuovere la regola relativa alla porta SSH:

```
# -A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```

oppure eliminarla completamente dal file.

Warning

Attenzione: prima di chiudere la porta SSH assicurarsi di avere un metodo alternativo per accedere alla VPS (da vcloud) altrimenti non sarà più possibile amministrare il server da remoto.

Verifica della configurazione

Dopo aver modificato il file e riavviato il servizio, è possibile verificare le regole attive con:

```
iptables -L -n -v
```

Questo comando mostrerà tutte le regole attualmente caricate nel firewall, insieme ai contatori di traffico e alle porte autorizzate.