Bloccare gli indirizzi IP con nginx

nginx è un web server potente e flessibile, ampiamente utilizzato per servire contenuti web ad alte prestazioni. Uno dei suoi molteplici utilizzi è la capacità di gestire l'accesso al server in base agli indirizzi IP. Bloccare o consentire l'accesso a determinati IP può essere utile per vari motivi, come la sicurezza, la gestione del traffico o la limitazione dell'accesso a utenti specifici. In questo articolo, vedremo come configurare nginx per bloccare l'accesso a determinati indirizzi IP.

Per bloccare l'accesso a specifici indirizzi IP, devi utilizzare la direttiva `deny` all'interno del blocco del server o del location che vuoi proteggere. Ad esempio, per bloccare l'accesso a un sito web intero da un IP specifico, aggiungi quanto segue nel blocco `server`:

```
server {
    listen 80;
    server_name miosito.com www.miosito.com;

    # Blocca l'accesso a specifici indirizzi IP
    deny 192.168.1.1;
    deny 203.0.113.0/24;

    # Permetti l'accesso a tutti gli altri
    allow all;

    location / {
        # Configurazioni aggiuntive
        try_files $uri $uri/ =404;
    }
}
```

In questo esempio, l'indirizzo IP `192.168.1.1` e l'intervallo di IP `203.0.113.0/24` saranno bloccati dall'accesso al sito. La direttiva `allow all` garantisce che tutti gli altri indirizzi IP non specificati siano autorizzati.

Se vuoi bloccare l'accesso solo a una specifica pagina o directory, puoi farlo all'interno di un blocco `location`:

```
server {
    listen 80;
    server_name miosito.com www.miosito.com;

    location /admin {
        # Blocca l'accesso a specifici indirizzi IP
        deny 192.168.1.1;
        deny 203.0.113.0/24;

        # Permetti l'accesso a tutti gli altri
        allow all;

        # Configurazioni aggiuntive per /admin
        try_files $uri $uri/ =404;
    }
}
```

In questo caso, solo l'accesso alla directory `/admin` è limitato agli indirizzi IP specificati.

Conclusioni

Bloccare l'accesso a determinati indirizzi IP con nginx è un'operazione semplice ma potente per la gestione del traffico e la sicurezza del tuo server web. Utilizzando le direttive `deny` e `allow`, puoi facilmente controllare chi ha accesso alle risorse del tuo sito web. Ricorda di testare sempre le configurazioni su un ambiente di staging prima di applicarle in produzione per evitare interruzioni non pianificate.