Configurazioni avanzate di VPN per Network analysis-as-a-service

Nicola Bena

Ottobre 2018

MoonCloud

- Framework per la valutazione ed il monitoraggio continuo di servizi cloud
- valutazione continuata che proprietà siano rispettate nel servizio cloud (*non solo proprietà di sicurezza*)
- per l'utente finale MoonCloud è un servizio offerto via cloud
  - inserisce informazioni sul target
  - MoonCloud effettua valutazione
  - mostra risultati

Non solo cloud

Obiettivo: estendere MoonCloud per poter analizzare infrastrutture IP *classiche* (reti aziendali)

- mantenendo intatto il modello as-a-service di MoonCloud
- MoonCloud non può semplicemente fare richieste verso una rete target, c'è almeno un firewall
- soluzione: utilizzare una VPN tra MoonCloud e la rete target

Soluzione

La soluzione VPN deve:

- essere flessibile
- ligthweight per il cliente: non deve configurare niente nella propria rete

Soluzione:

- device Linux portato nella rete target che fa da VPN client
- in MoonCloud i VPN server
- OpenVPN per il collegamento VPN
- nftables (successore di iptables) per risolvere problemi di configurazione

Sfida 1 – NAT al contrario

- IP sorgente dei pacchetti MoonCloud $\rightarrow$ rete target appartiene alla rete MoonCloud

NAT al contrario: tutti i pacchetti provenienti dalla VPN vengono immessi nella rete target usando come IP sorgente quello del client VPN

- stesso NET ID della rete target
- quindi le risposte tornano direttamente ad esso
- realizzato con nftables

Sfida 1 – NAT al contrario

- IP sorgente dei pacchetti MoonCloud $\rightarrow$ rete target appartiene alla rete MoonCloud
- la rete target deve inviare le risposte al VPN client, ma senza rotte configurate le invierebbe al proprio default gateway

NAT al contrario: tutti i pacchetti provenienti dalla VPN vengono immessi nella rete target usando come IP sorgente quello del client VPN

- stesso NET ID della rete target
- quindi le risposte tornano direttamente ad esso
- realizzato con nftables

Sfida 2 – IP mapping

"*Ogni rete connessa alla VPN deve stare in reti IP diverse*"[1]

- si vuole che un server gestisca più client, quindi reti, possibili

IP mapping: *mappare* ogni rete target in una nuova rete garantita univoca perché scelta da MoonCloud

- tutta MoonCloud conosce solo indirizzi mappati quindi unici

[1] `https://openvpn.net`

Sfida 2 – IP mapping

"*Ogni rete connessa alla VPN deve stare in reti IP diverse*"[1]

- si vuole che un server gestisca più client, quindi reti, possibili
- ma reti target hanno IP privati

IP mapping: *mappare* ogni rete target in una nuova rete garantita univoca perché scelta da MoonCloud

- tutta MoonCloud conosce solo indirizzi mappati quindi unici

[1] `https://openvpn.net`

Sfida 2 – IP mapping

"*Ogni rete connessa alla VPN deve stare in reti IP diverse*"[1]

- si vuole che un server gestisca più client, quindi reti, possibili
- ma reti target hanno IP privati
- quindi ci saranno conflitti

IP mapping: *mappare* ogni rete target in una nuova rete garantita univoca perché scelta da MoonCloud

- tutta MoonCloud conosce solo indirizzi mappati quindi unici

[1] `https://openvpn.net`

Sfida 2 – IP mapping (2)

- Lato client si utilizza nftables sul VPN client
  - pacchetti MoonCloud $\rightarrow$ client: modifica IP mappato $\rightarrow$ IP originale (e poi invia a target)
  - pacchetti client $\rightarrow$ MoonCloud: modifica IP originale $\rightarrow$ IP mappato
- Lato server
  - quando si registra un nuovo client si *mappano* le sue reti su reti nuove
  - trasparente per l'utente
    - inserisce come target l'IP originale
    - MoonCloud si occupa di mapparlo

MoonCloud_VPN

Microservizio integrato in MoonCloud per gestire la soluzione VPN

- creare file di configurazione per OpenVPN
  - e trasferimento via SSH ai server
- gestire i certificati di client e server
  - creare
  - revocare mediante CRL
- gestire IP mapping
  - file di configurazione per nftables
  - assegnare nuove reti ai client
  - dato un IP originale ritornare quello mappato