



Sicurezza delle
reti

Monga

Proxy

NAT

Sicurezza delle reti¹

Mattia Monga

Dip. di Informatica e Comunicazione
Università degli Studi di Milano, Italia

mattia.monga@unimi.it

a.a. 2010/11

¹ © 2011 M. Monga. Creative Commons Attribuzione-Condividi allo stesso modo 2.5 Italia License.
<http://creativecommons.org/licenses/by-sa/2.5/it/>. Materiale derivato da © 2010 M. Cremonini.



Sicurezza delle
reti

Monga

Proxy

NAT

Lezione IX: Sicurezza perimetrale



Proxy

Un **proxy** è un componente che media le comunicazioni tra altri due componenti che rimangono inconsapevoli della sua presenza.

- Un proxy disaccoppia la comunicazione tra due componenti rendendola indiretta
- Un proxy agisce sia da client (rispetto al server originale) che da server (rispetto al client originale)

Proxy

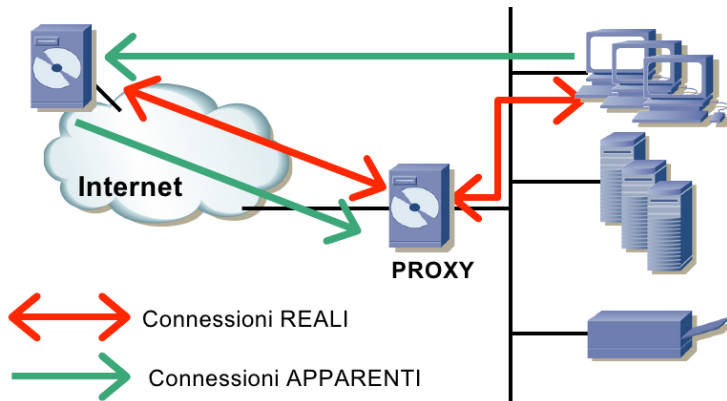


Sicurezza delle reti

Monga

Proxy

NAT





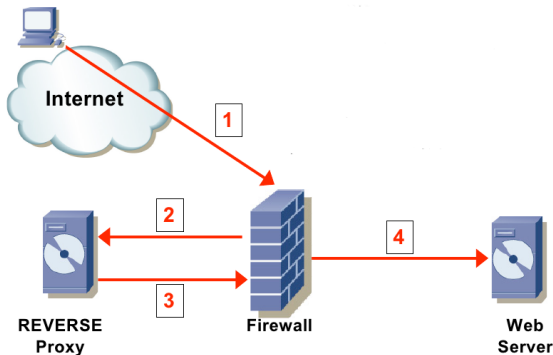
Web Proxy Cache di pagine web.

Anonymizing Proxy Anonimizzazione di connessioni web.

Reverse Proxy Gestiscono l'accesso da utenti esterni a risorse interne.

Proxy Firewall Mediano connessioni applicative e gestiscono aspetti di sicurezza dei protocolli.

Reverse proxy



- 1 Connessione da utente esterno verso il Web Server
- 2 Redirezione della connessione verso il Reverse Proxy
- 3 Autenticazione, verifica, filtraggio, ecc...
- 4 Inoltro verso il Web Server

Sicurezza delle
reti

Monga

Proxy

NAT

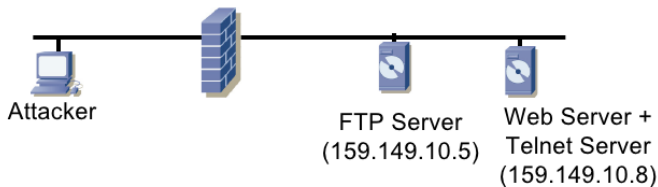


- Può essere usato per analizzare i dati delle applicazioni perché opera a livello applicativo
- Performance potenzialmente molto critiche
- Analogo ad un firewall stateful, ma lavora a livello del protocollo applicativo
- A volte plug-in dei firewall: *protocol decoding*



Esempio di firewall proxy

FTP-bounce attack



- Il comando PORT di FTP: `PORT h1, h2, h3, h4, p1, p2`
 - (h1, h2, h3, h4) rappresentano gli ottetti dell'indirizzo IP del server FTP
 - $(256 \cdot p1 + p2)$ restituisce la porta sulla quale il client riceverà la connessione dal server
- `PORT 159, 149, 10, 8, 0, 23` (159.149.10.8, porta 23/tcp)
- `RETR`: apertura di una connessione proveniente dall'FTP server

Un proxy firewall con conoscenza del protocollo FTP potrebbe

Sicurezza delle
reti

Monga

Proxy

NAT



Spesso chiamato anche IP Masquerading

- Consente di manipolare gli indirizzi IP nel passaggio tra le due interfacce di un firewall/router
- Tipicamente viene usato per sfruttare le classi di indirizzi IP riservate e non istradabili (10., 172.16-31, e 192.168)
- Il NAT non è propriamente una soluzione per la sicurezza della rete aziendale, ma una tecnica di gestione della rete
- Fornisce un beneficio rilevante: maschera gli indirizzi effettivamente utilizzati all'interno della rete

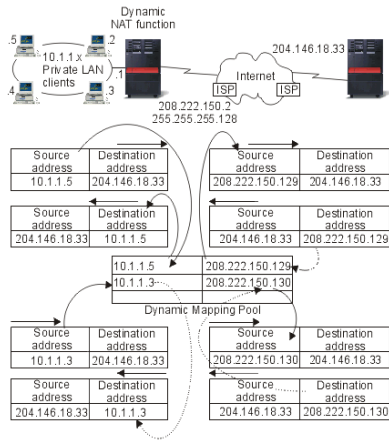


Tipologie di NAT

Terminologia IBM

- **Statico** Indirizzi IP interni vengono mappati staticamente in indirizzi IP pubblici. L'associazione è predefinita e fissa
- **Dinamico** L'associazione tra indirizzo IP interno e indirizzo IP pubblico avviene dinamicamente a run-time
- **PAT (Port Address Translation)** L'associazione tra avviene modificando la porta sorgente

Dinamico



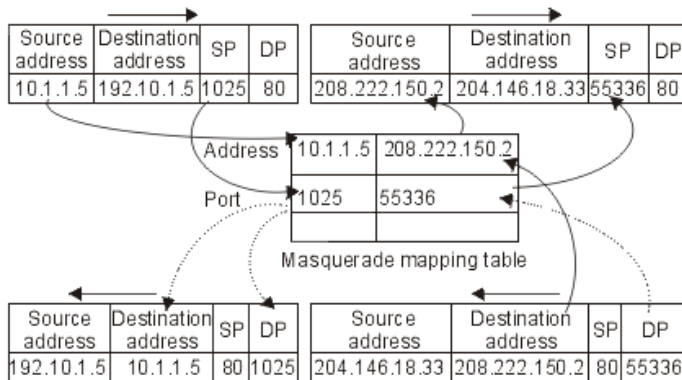
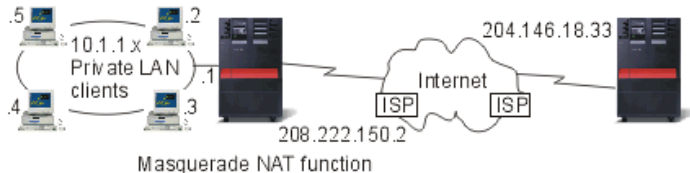
Sicurezza delle reti

Monga

Proxy

NAT

Esempio Masquerading



Sicurezza delle reti

Monga

Proxy

NAT