Sicurezza dei sistemi e delle reti[1]

Mattia Monga

Dip. di Informatica
Università degli Studi di Milano, Italia
mattia.monga@unimi.it

a.a. 2014/15

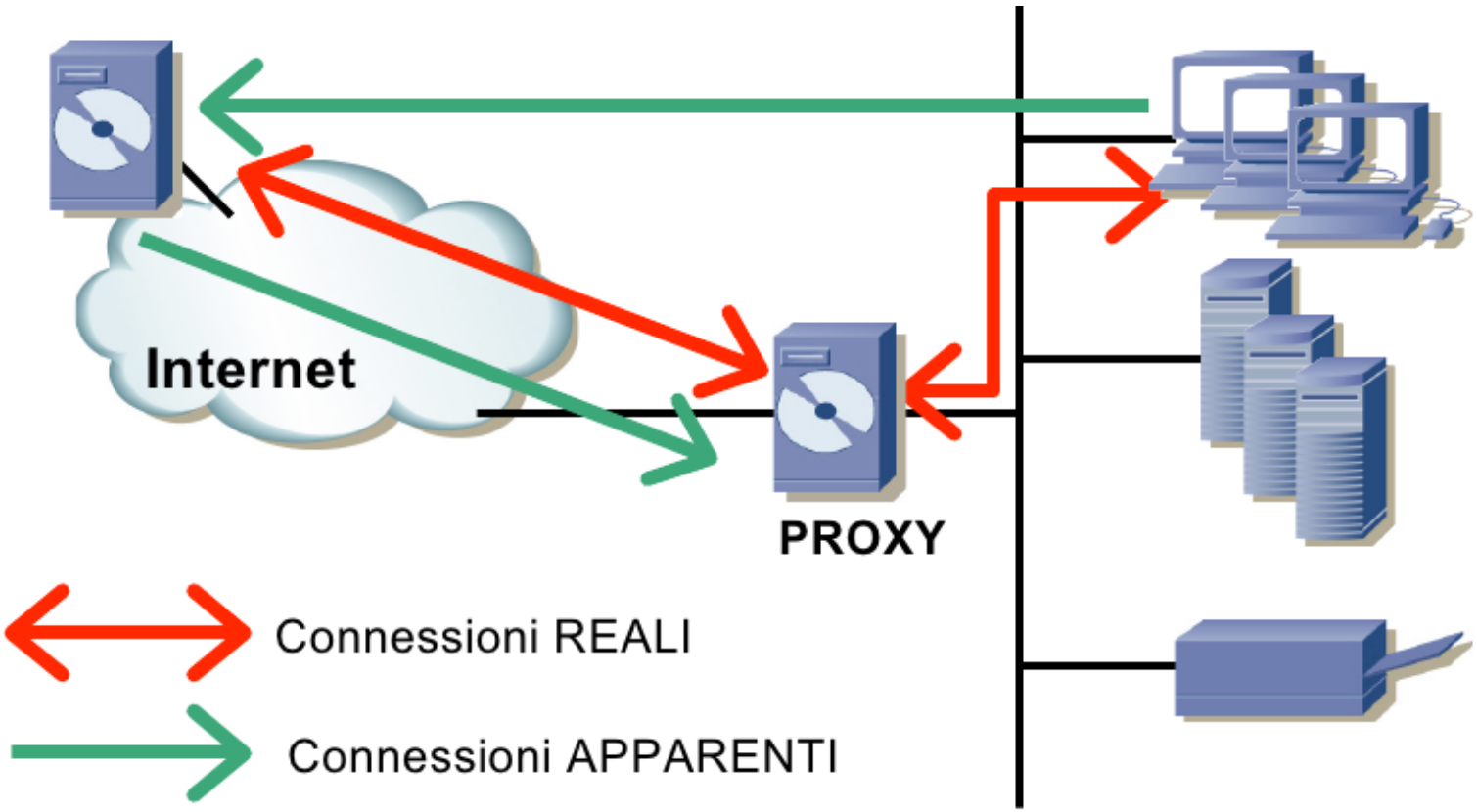
Lezione X: Proxy

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



Proxy

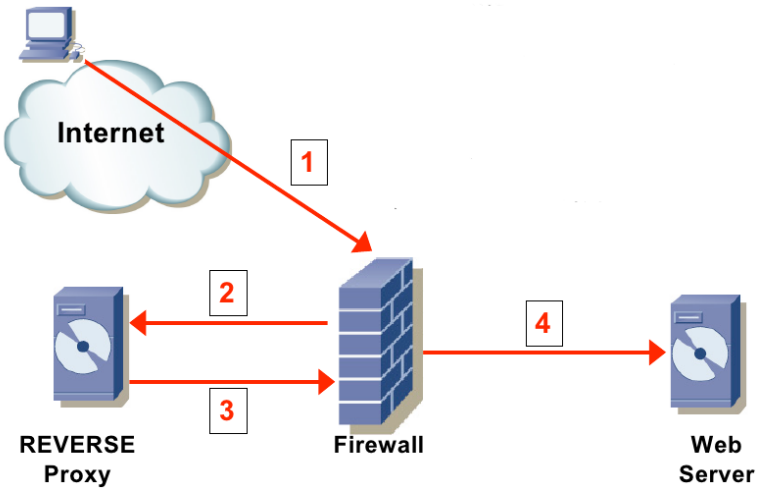
Web Proxy Cache di pagine web.

Anonymizing Proxy Anonimizzazione di connessioni web.

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

Proxy Firewall

Reverse proxy

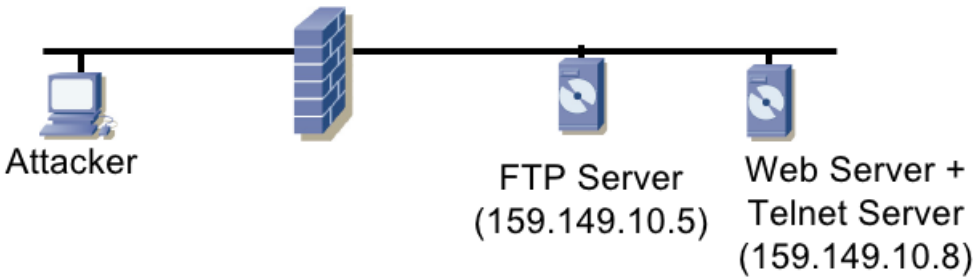


1. Connessione da utente esterno verso il Web Server
2. Redirezione della connessione verso il Reverse Proxy
3. Autenticazione, verifica, filtraggio, ecc...
4. Inoltro verso il Web Server

Proxy firewall

- 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*

Firewall proxy per prevenire FTP bounce



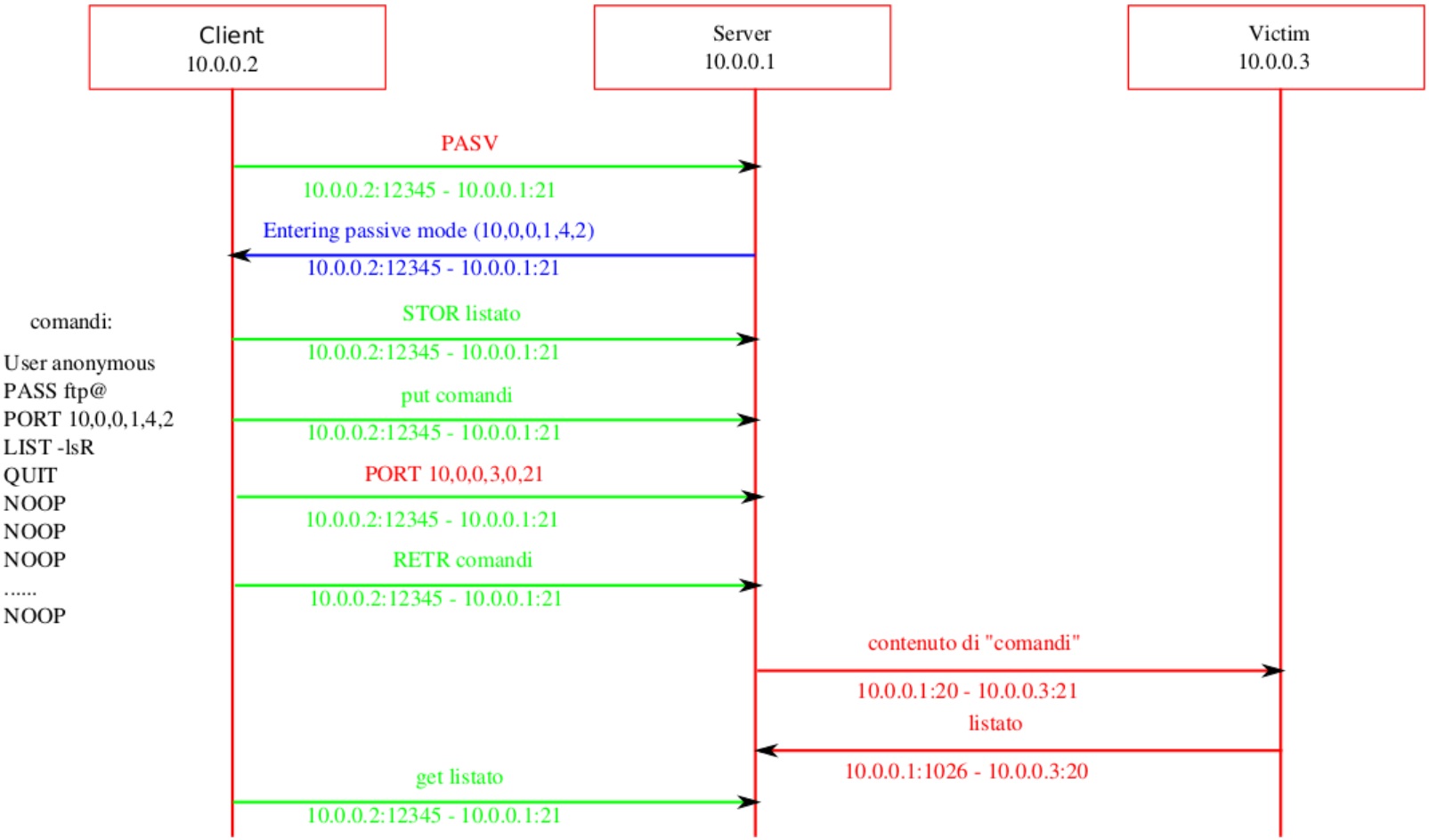
- Il comando PORT di FTP: PORT h1, h2, h3, h4, p1, p2
  - (h1, h2, h3, h4) gli ottetti dell'IP del server
  - $(256 \cdot p1 + p2)$ la porta per la connessione dal server
- PORT 159, 149, 10, 8, 0, 23 (159.149.10.8, porta 23/tcp)
- RETR: apertura di una connessione proveniente dall'FTP server

FTP bounce

Nel caso piú semplice può servire per fare una scansione:

- PORT 159, 149, 10, 8, 0, 23 (159.149.10.8, porta 23/tcp)
- L'attaccante riesce a capire se la porta 23 di 159.149.10.8 accetta connessioni

FTP bounce evoluto



Riassumendo

Un proxy

- firewall stateful che lavorano a livello applicativo
- potenzialmente molto onerosi, ma possono risultare utili quando è possibile prevedere quali applicazioni useranno gli utenti della rete

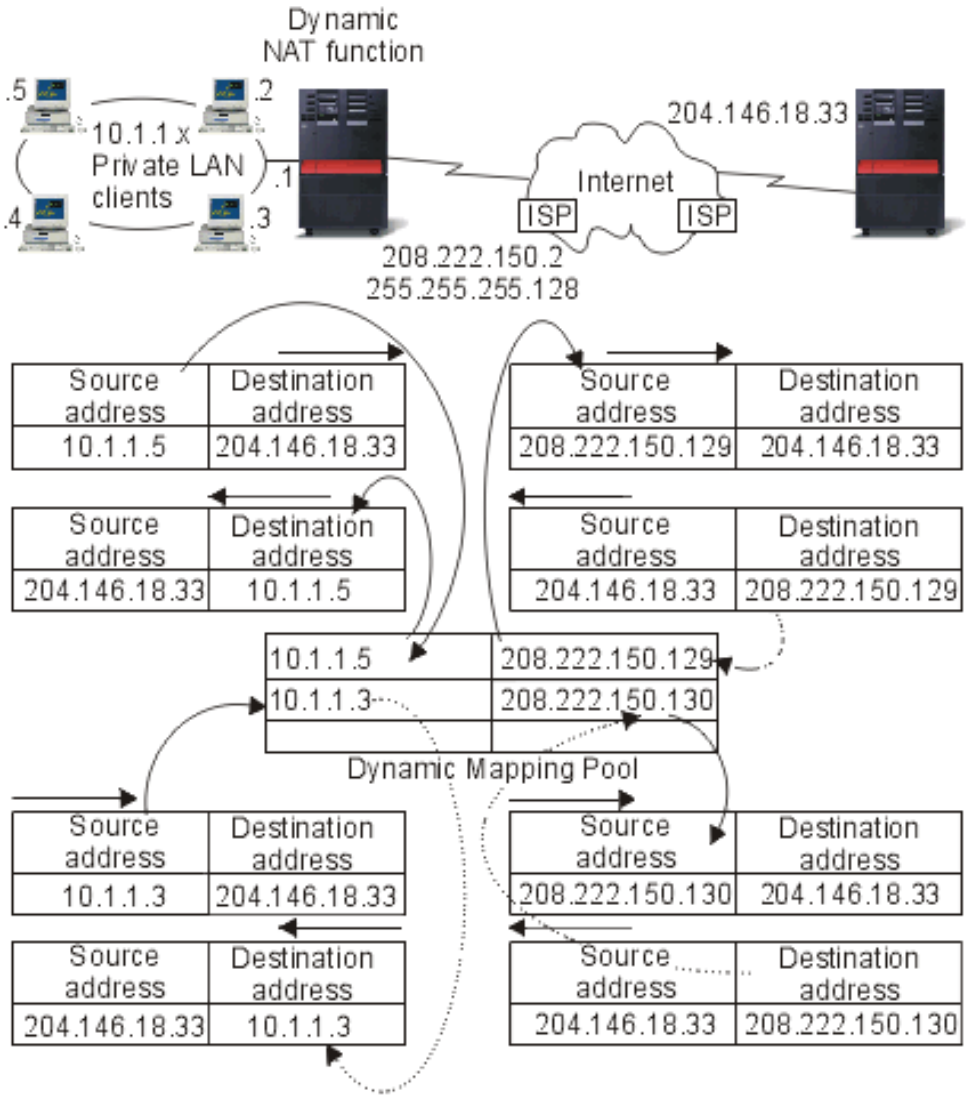
Network Address Translation (NAT) e IP Masquerading

- Consente di manipolare gli indirizzi IP nel passaggio tra le due interfacce di un firewall/router
- Tipicamente viene usato sfruttando le classi di indirizzi IP riservate e non istradabili (10., 172.16-31, e 192.168)
- Maschera gli indirizzi effettivamente utilizzati all'interno della rete

NAT

- Il router modifica gli indirizzi dei pacchetti prima instradarli
- Statico: IP interni mappati staticamente in IP pubblici.
- Dinamico: L'associazione tra IP interno e IP pubblico avviene a run-time

Dynamic NAT

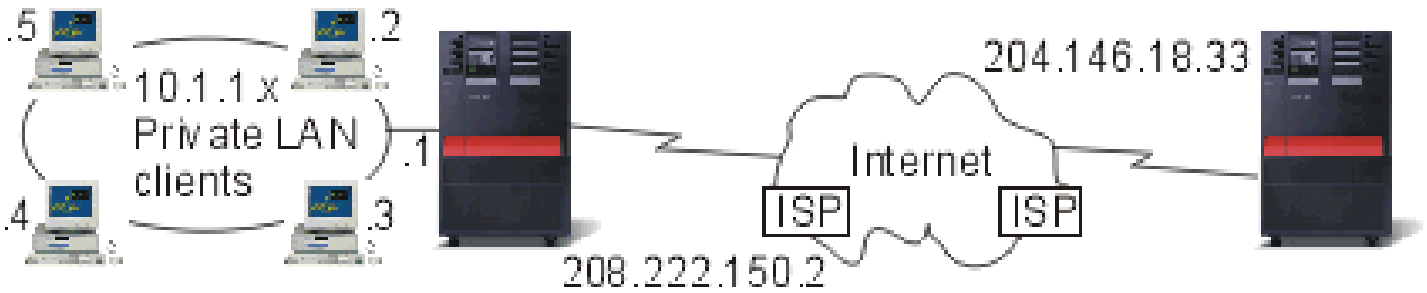

Dynamic
NAT function
.5
.2
10.1.1.x
Private LAN
clients
.1
.4
.3
204.146.18.33
Internet
ISP
ISP
208.222.150.2
255.255.255.128
Source address
Destination address
10.1.1.5
204.146.18.33
Source address
Destination address
208.222.150.129
204.146.18.33
Source address
Destination address
204.146.18.33
10.1.1.5
Source address
Destination address
204.146.18.33
208.222.150.129
10.1.1.5
208.222.150.129
10.1.1.3
208.222.150.130
Dynamic Mapping Pool
Source address
Destination address
10.1.1.3
204.146.18.33
Source address
Destination address
208.222.150.130
204.146.18.33
Source address
Destination address
204.146.18.33
10.1.1.3
Source address
Destination address
204.146.18.33
208.222.150.130

Masquerading

È una forma di NAT capace di lavorare anche ai livelli applicativi.

- Si usa la Port Address Translation: l'associazione avviene modificando la porta sorgente (p.es. ≥ 32536)
- Il masquerading proxy conosce alcuni protocolli e adatta la conversazione alle nuove condizioni (p.es. FTP)

Esempio Masquerading



Masquerade NAT function

Source address	Destination address	SP	DP
10.1.1.5	192.10.1.5	1025	80

Source address	Destination address	SP	DP
208.222.150.2	204.146.18.33	55336	80

Address	10.1.1.5	208.222.150.2
Port	1025	55336

Masquerade mapping table

Source address	Destination address	SP	DP
192.10.1.5	10.1.1.5	80	1025

Source address	Destination address	SP	DP
204.146.18.33	208.222.150.2	80	55336

Riassumendo

NAT e masquerading

- nate piú come tecniche di gestione della rete, che misure di sicurezza
- nascondo la rete interna, garantendo l'irrangiugibilità diretta