



# Sicurezza dei sistemi e delle reti<sup>1</sup>

Mattia Monga

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

a.a. 2014/15

<sup>1</sup>© 2011-15 M. Monga. Creative Commons Attribuzione — Condividi allo stesso modo 4.0 Internazionale. <http://creativecommons.org/licenses/by-sa/4.0/deed.it>. Derivato con permesso da © 2010 M. Cremonini.



# Lezione X: Proxy

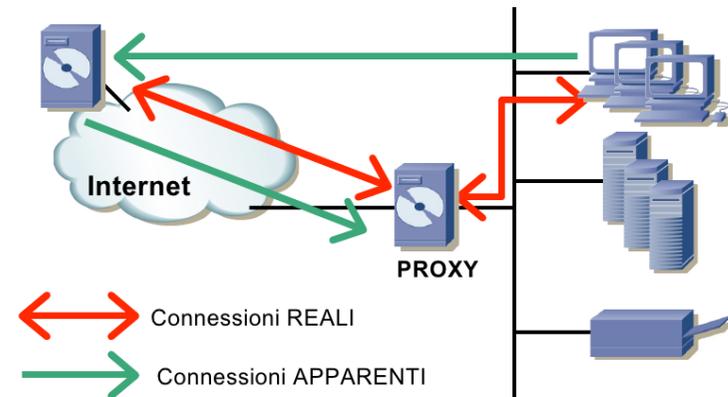
## Proxy



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



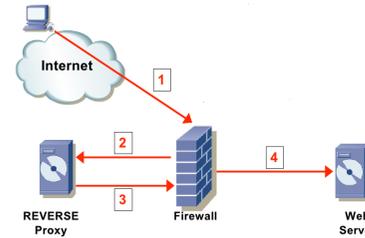


Web Proxy Cache di pagine web.

Anonymizing Proxy Anonimizzazione di connessioni web.

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

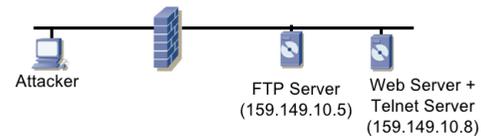
Proxy Firewall



- 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



- 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*



- 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



Sicurezza delle reti  
Monga  
Proxy  
NAT/Masquerading

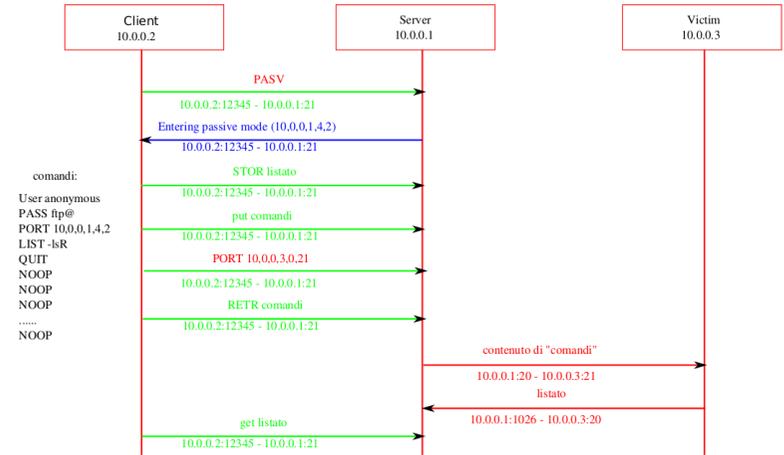
Nel caso piú semplice può servire per fare una scansione:

- 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



Sicurezza delle reti  
Monga  
Proxy  
NAT/Masquerading



# Riassumendo



Sicurezza delle reti  
Monga  
Proxy  
NAT/Masquerading

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



Sicurezza delle reti  
Monga  
Proxy  
NAT/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



Sicurezza delle reti  
Monga  
Proxy  
NAT/Masquerading

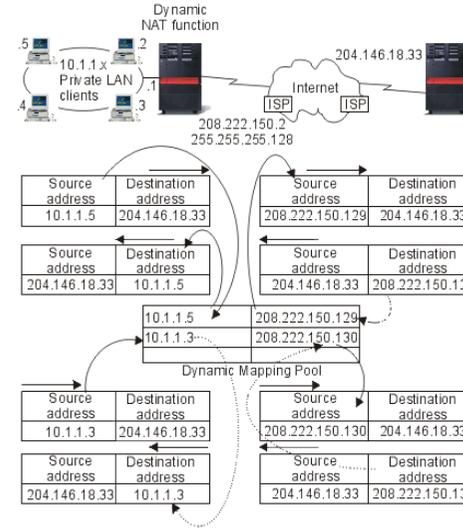
- Il router modifica gli indirizzi dei pacchetti prima instradarli
- Statico: IP interni mappati staticamente in IP pubblici.
- Dinamico: L'associazione tra IP interno e IP pubblico avviene a run-time

188

# Dynamic NAT



Sicurezza delle reti  
Monga  
Proxy  
NAT/Masquerading



189

# Masquerading



Sicurezza delle reti  
Monga  
Proxy  
NAT/Masquerading

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

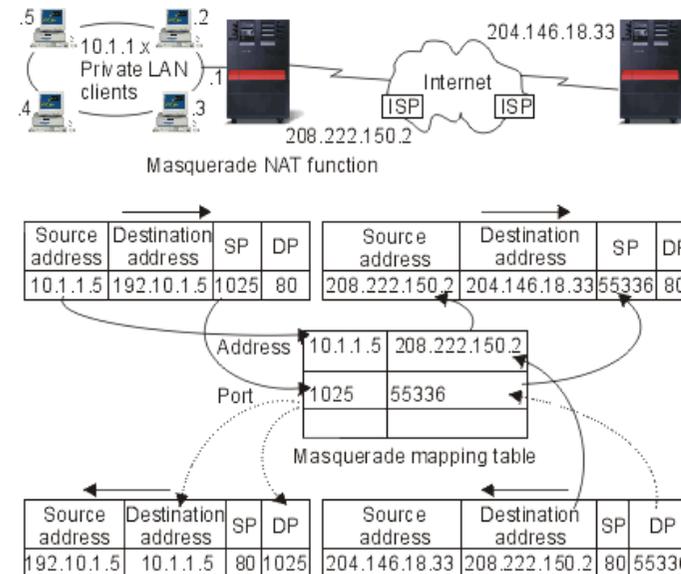
- Si usa la Port Address Translation: l'associazione avviene modificando la porta sorgente (p.es.  $\geq 32536$ )
- Il masquerading proxy conosce alcuni protocolli e adatta la conversazione alle nuove condizioni (p.es. FTP)

190

# Esempio Masquerading



Sicurezza delle reti  
Monga  
Proxy  
NAT/Masquerading



191



Sicurezza delle  
reti

**Monga**

Proxy

**NAT/Masque-  
rading**

## NAT e masquerading

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