Corso MIUR C2

Modulo 8

Firewall

Ing. Giampaolo Mancini
Ing. Fabio De Vito

Sommario

- Concetto di firewalling
- Funzionalità di un firewall
  - Filtro sui pacchetti in ingresso
  - Filtro sui pacchetti in uscita
  - Filtro sui pacchetti in transito
  - Traduzione di pacchetti (NAT)
  - Redirezione di indirizzi (PAT)

Firewalling

- Il firewall è un insieme di regole che gestiscono il comportamento di una macchina rispetto ai pacchetti che transitano sulle sue interfacce
- Generalmente per firewall si intende il blocco in ingresso dei pacchetti indesiderati o ritenuti dannosi
- In realtà il firewall è un filtro che permette di gestire in modo differenziato i pacchetti

Firewalling

- I firewall possono contenere regole molto generali o molto complesse
- Si può filtrare basandosi su dati molto dettagliati
  - Indirizzi sorgente/destinazione
    - Indirizzi singoli o intere reti
  - Porte sorgente/destinazione
    - Singoli o elenco di porte
  - Indirizzo MAC
    - Solo per i pacchetti in ingresso

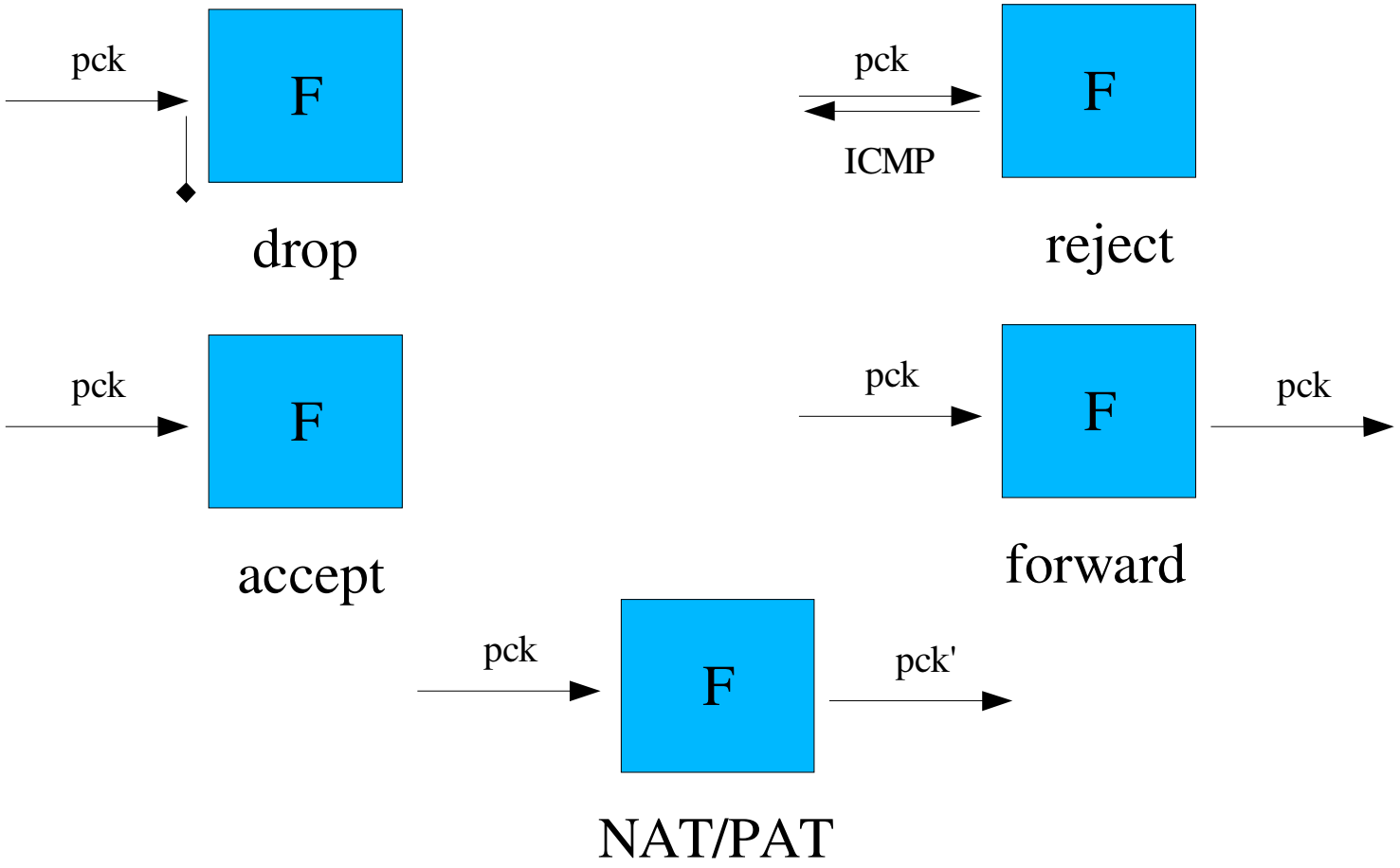
Firewalling

- Protocollo di trasporto
  - TCP, UDP, ICMP, frammenti
  - Nel caso di TCP si possono discriminare i vari flag nell'header (SYN, ACK, etc)
  - Nel caso di ICMP si possono specificare i diversi tipi di messaggi
  - Nel caso di pacchetti frammentati, solo per il primo può essere determinato il tipo di protocollo
- Interfaccia di ricezione/trasmissione del pacchetto
  - Ethernet, PPP, etc

Firewalling

- Si può decidere cosa fare del pacchetto
  - Accettare (accept)
  - Rifiutare (reject) e rispondere con un messaggio di errore
  - Scartare (drop) e non dare segnalazione
  - Tenere traccia del pacchetto (log)
  - Mascherare l'indirizzo sorgente del pacchetto (nat)
  - Redirigere un pacchetto in ingresso verso una macchina con indirizzo privato (pat)

Firewalling



Firewalling

- I firewall devono essere posizionati in modo da essere presenti su tutti i punti di accesso ad un host o a una sottorete
  - In generale è preferibile avere un unico punto di accesso, in modo da poter meglio controllare il traffico
  - È possibile ridondare la protezione includendo, oltre che il firewall sul punto di accesso alla rete, anche un firewall per ogni singola macchina

Firewall: filtro

- La funzionalità di filtro consente di controllare i pacchetti che attraversano il nodo
  - Destinati al nodo, generati dal nodo o solo in transito
- Combinando opportunamente le regole, si possono ottenere comportamenti molto complessi e si possono abilitare servizi specifici per ogni singola macchina

Firewall: filtro

- Bisogna porre particolare attenzione nella configurazione dei filtri
- Bloccare indiscriminatamente la ricezione o il transito di un servizio può compromettere il buon funzionamento di una rete
- Esempio: blocco del transito dei pacchetti UDP
  - Si rischia di bloccare le richieste DNS a server esterni
    - Soluzione: aprire esclusivamente la porta 53 o inserire un server DNS sulla stessa macchina che ospita il firewall

Firewall: filtro

- Esempio: blocco dei pacchetti icmp
  - Non vengono inviate risposte in caso di mancato accesso e le applicazioni che tentano di attraversare il firewall rimangono in attesa fino allo scadere dei timeout, senza sapere il perchè
  - La macchina non risponde alle richieste di ping e di traceroute
    - Più sicurezza ma la macchina non risponde neanche all'amministratore di rete

Filtro: ingresso

- I filtri in ingresso riguardano tutti i pacchetti in arrivo sulle interfacce della macchina
- Questi filtri sono solitamente utilizzati per:
  - Bloccare pacchetti indesiderati
    - Esempio: connessione a porte non autorizzate
  - Limitare il traffico in ingresso
    - Esempio: limitare il numero di ping ai quali rispondere in un dato tempo, evitare la scansione delle porte

Filtro: ingresso

- Impedire l'accesso all'amministrazione remota della macchina che ospita il firewall da determinate macchine

Filtro: uscita

- Il filtro in uscita opera sui pacchetti generati dalla macchina che ospita il firewall
- Questo tipo di filtro si occupa di:
  - Bloccare l'uscita di pacchetti dalla macchina
    - Esempio: impedire che la macchina effettui connessioni su determinate porte o richieste di ping o traceroute
  - Limitare il traffico
    - Esempio: evitare che la macchina generi port scanning

Filtro: inoltro

- Consente di creare delle regole che gestiscono i pacchetti in transito attraverso il nodo
- Si usa per macchine che facciano da punto di accesso ad una rete
- Consente di:
  - Isolare intere reti
    - Esempio: bloccando tutto il traffico in ingresso su una interfaccia

Filtro: inoltro

- Bloccare comunicazioni TCP se iniziate da determinate macchine
  - Esempio: solo le macchine di una rete possono accedere ai servizi di un server
- Limitare il traffico di un certo tipo in transito attraverso il nodo
  - Esempio: evitare che le macchine a valle generino traffico di tipo UDP
  - Attenzione alla gestione del DNS

Filtro: inoltro

- Naturalmente, assicurarsi che il nodo di transito abbia il forwarding dei pacchetti IP attivato
- Se esistono più di due interfacce, occorre particolare attenzione nella scrittura delle regole di inoltro
  - Possono essere necessarie regole differenziate per ogni coppia <interfaccia di ingresso, interfaccia di uscita> e per diversi servizi

Gestione delle regole

- Le regole vengono lette nell'ordine in cui sono scritte
- Non appena si trova il match per il pacchetto, non si scende oltre nella catena
- Per questo è necessario seguire alcuni criteri di base nella stesura delle regole

Gestione delle regole

- Sono possibili due approcci:
  - Tipo router:
    - Lascia passare tutto il traffico che non viene bloccato esplicitamente
  - Tipo macchina:
    - Blocca tutto il traffico che non è stato abilitato nelle regole
    - Approccio più conservativo, tipico delle macchine server (ad esempio è inutile aprire tutte le porte su un web server)

Gestione delle regole

- Un buon approccio (dal punto di vista della sicurezza) è iniziare con le regole che prevedono il rifiuto del pacchetto
  - In questo caso, se dovesse verificarsi un conflitto fra due regole, una che lascia passare il traffico e l'altra che lo blocca, il servizio non funziona ma si diminuisce l'esposizione al rischio (il pacchetto viene scartato)

Gestione delle regole

- Esempio:
  - Blocca i pacchetti UDP
  - Consenti l'accesso alla porta 23
  - Fai passare i pacchetti UDP
- In questo caso i pacchetti UDP vengono scartati
- Se si fossero invertite le regole 1 e 3 i pacchetti sarebbero passati indisturbati

Gestione delle regole

- È sempre meglio iniziare dalle regole più dettagliate
  - In questo modo si evita che il pacchetto soddisfi più regole e che la meno generale mascheri la più dettagliata
  - Esempio:
    - Regola 1 -> bloccare tutto il traffico ICMP
    - Regola 2 -> limitare il numero di risposte a ping
    - In questo caso la seconda regola è inutile, perchè i pacchetti ping sono pacchetti ICMP

Gestione delle regole

- In questo caso la macchina non risponderà mai ai ping

– Esempio:

- Regola 1 -> limitare il numero di risposte a ping
- Regola 2 -> bloccare tutto il traffico ICMP
- In questo caso la macchina risponderà in modo limitato ai ping e bloccherà tutto il resto del traffico ICMP in arrivo/transito

Gestione delle regole

- Tenere sempre conto delle caratteristiche dei vari servizi (protocolli, porte, etc)
  - Esempi:
    - Chiudere il passaggio a tutto il traffico UDP blocca il funzionamento del DNS
    - Bloccare tutti i pacchetti ICMP rende difficoltosa la diagnostica -> meglio chiuderne solo alcuni e limitare gli altri

Gestione delle regole

- Per le connessioni TCP, è meglio bloccare solo il pacchetto SYN e non tutti i pacchetti; il risultato è identico perchè in entrambi i casi la connessione non parte, ma in questo modo si evita di chiudere connessioni già aperte al momento della modifica della regola
- Se si sta lavorando in ssh alla modifica di un firewall remoto, chiudere improvvisamente il passaggio a tutti i pacchetti TCP non consente ulteriori modifiche in quanto si blocca anche la sessione attraverso la quale stiamo lavorando...

Gestione delle regole

- Esiste la possibilità di tenere un log del passaggio di determinati pacchetti
  - In generale è utile salvare le informazioni su un pacchetto prima di scartarlo, in modo da poter tentare di capire chi lo ha generato
  - Da utilizzare per esempio per i pacchetti ICMP

Firewall: NAT/PAT

- Tramite un firewall opportunamente configurato è possibile ottenere i servizi
  - NAT (network address translation)
    - Serve a mascherare alla rete esterna gli indirizzi della rete interna che hanno generato il pacchetto
    - Si usa sempre per dare l'accesso ad internet a macchine con indirizzamento privato
    - Dal punto di vista della rete, è come se tutto il traffico aggregato fosse generato dal nodo che contiene il NAT

Firewall: NAT/PAT

- PAT (port address translation)
  - Serve a redirigere il traffico che giunge al firewall dalla rete esterna verso una determinata macchina all'interno della rete privata
  - Ad esempio: una connessione arriva alla macchina che contiene il firewall, sulla porta 80; il firewall gira tale richiesta ad una macchina interna alla rete su una determinata porta
  - Se non si usasse questo meccanismo, la macchina con indirizzo privato non sarebbe raggiungibile dall'esterno

Firewall: NAT/PAT

- Richiedendo l'attraversamento del nodo, è necessario che l'inoltro dei pacchetti sia abilitato e le tabelle di routing correttamente istruite
- Le operazioni di NAT/PAT si svolgono
  - NAT: dopo il routing
  - PAT: prima del routing

NAT

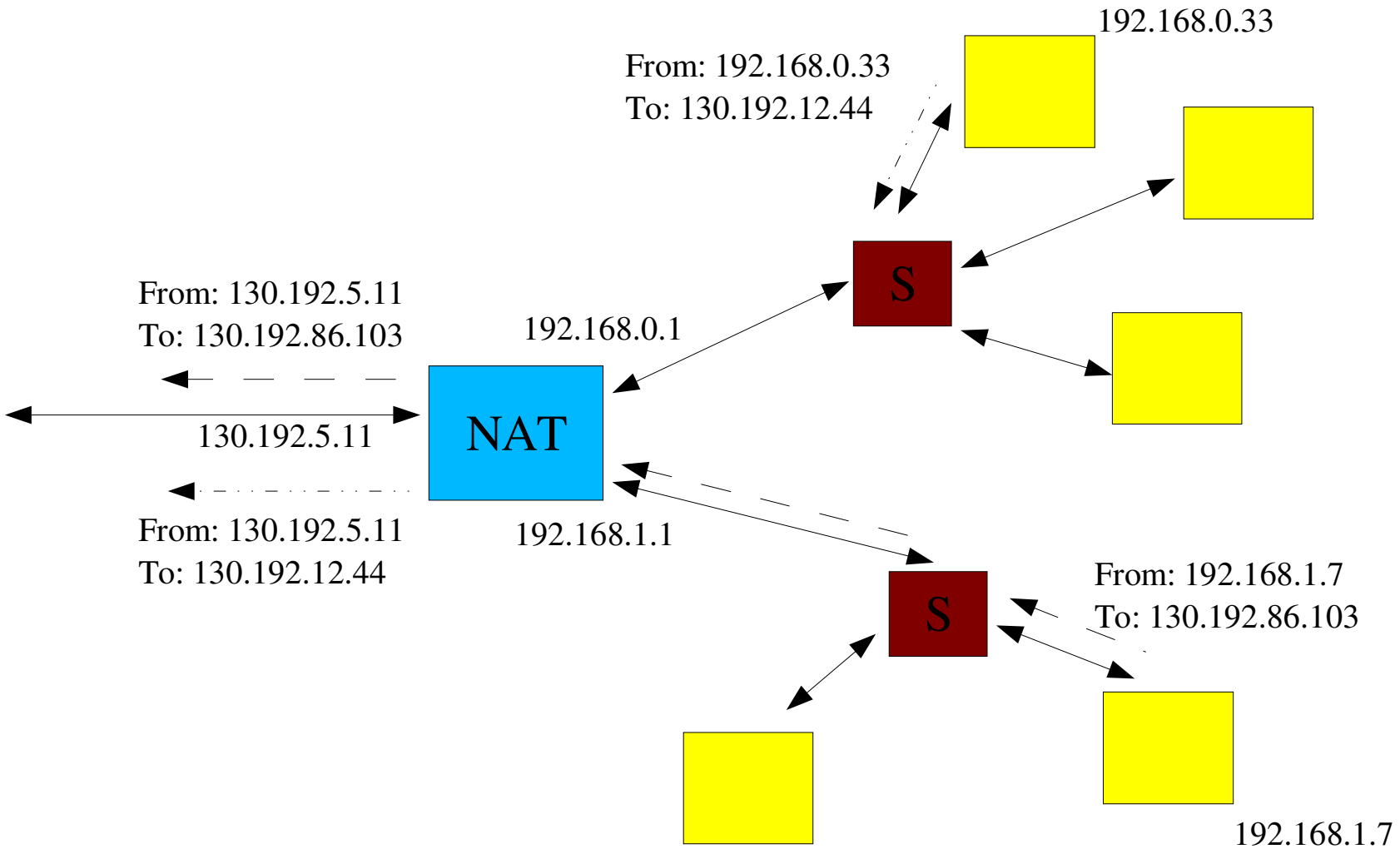
- Il NAT funziona sostituendo, all'interno del nodo che contiene il firewall, l'indirizzo sorgente
  - Può essere effettuato dopo l'instradamento (postrouting) in quanto tale operazione richiede la sola conoscenza della destinazione
  - Funziona mascherando alla rete esterna l'indirizzamento della rete privata
    - Solo la macchina che fa da NAT è direttamente visibile dalla rete mondiale

NAT

- Per l'accesso dall'esterno ad una macchina posizionata a valle di un NAT, è necessario accedere prima all'unica macchina visibile da internet, in quento questo calcolatore è l'unico che riesce a vedere sia la rete mondiale che quella privata; da qui è possibile poi accedere alle risorse interne
- Perdendo di generalità, si possono utilizzare i servizi di PAT


POLITECNICO - DI - TORINO
1859 - 1906

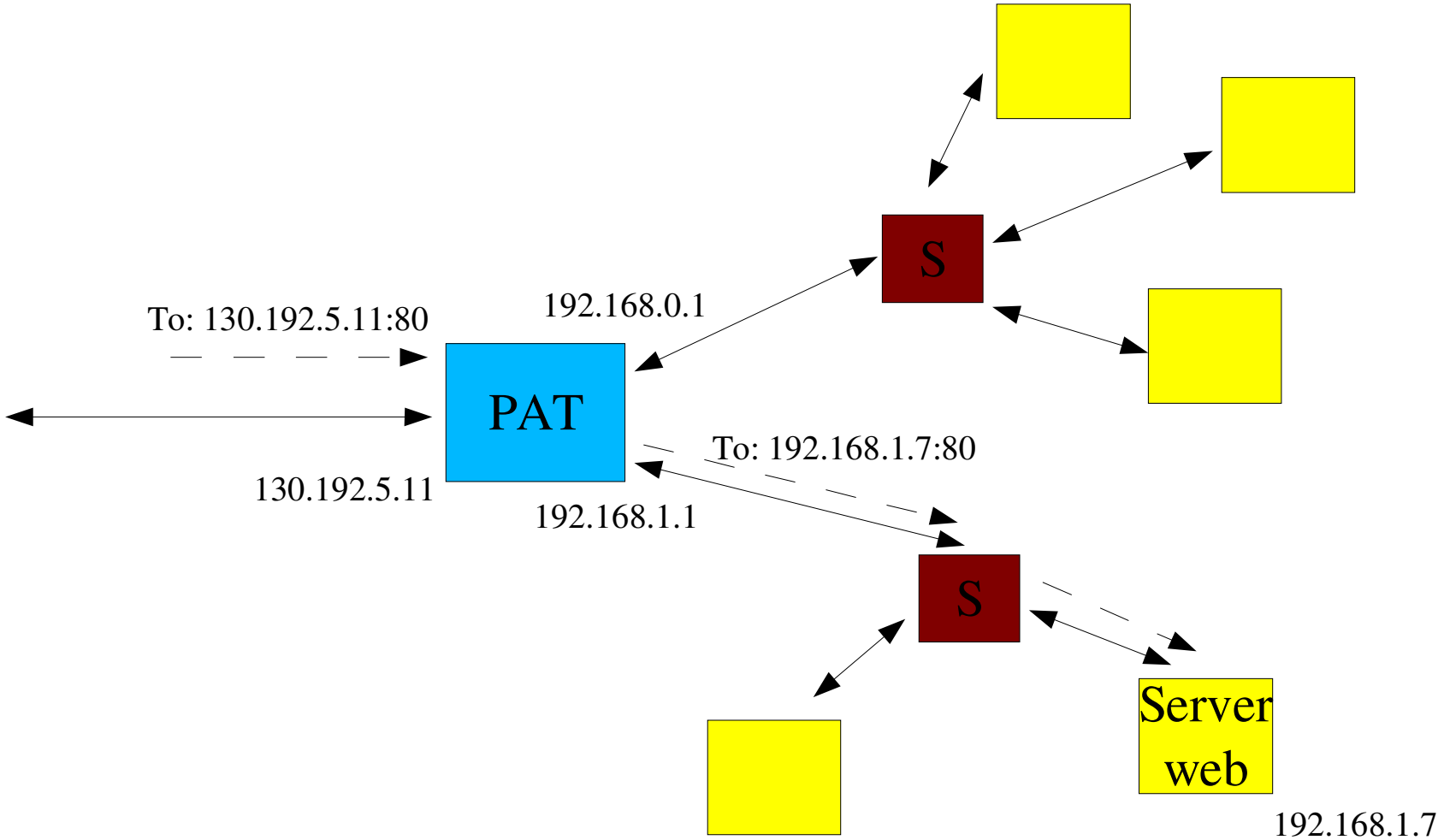
NAT


192.168.0.33
From: 192.168.0.33
To: 130.192.12.44
S
From: 130.192.5.11
To: 130.192.86.103
192.168.0.1
NAT
130.192.5.11
From: 130.192.5.11
To: 130.192.12.44
192.168.1.1
S
From: 192.168.1.7
To: 130.192.86.103
192.168.1.7

PAT

- Il PAT funziona in modo duale al NAT
- Consente di raggiungere un server interno alla rete con indirizzamento privato
  - L'operazione di cambio della destinzione deve essere fatta appena il pacchetto raggiunge il nodo che contiene il PAT
  - Infatti, è necessario modificare la destinazione e poi scegliere l'interfaccia di uscita (prerouting)

PAT


S
192.168.0.1
To: 130.192.5.11:80
PAT
130.192.5.11
To: 192.168.1.7:80
192.168.1.1
S
Server web
192.168.1.7