Università degli Studi di Verona
Corso di Laurea Magistrale in Informatica

Laboratorio di Sicurezza delle Reti

Firewall con linux: netfilter ed iptables

Andrea Zwirner


andrea@linkspirit.it


@AndreaZwirner

Netfilter

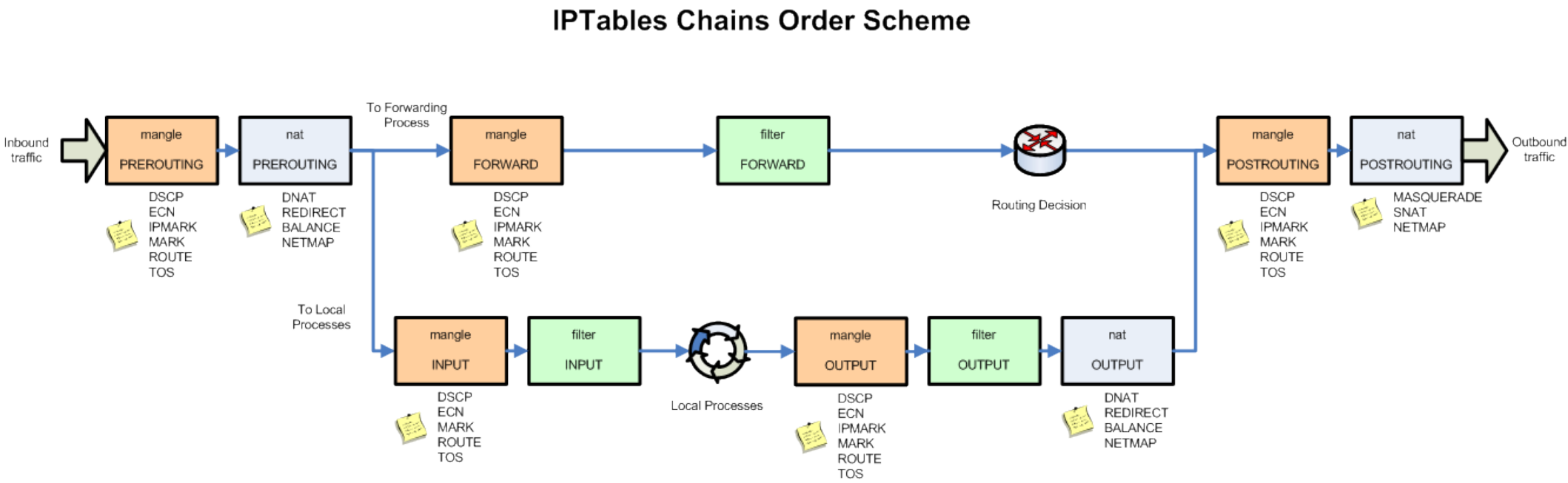
- Strumento di filtraggio disponibile nel kernel Linux
  - ipchains (kernel 2.2)
  - iptables (kernel 2.4 e successivi)

- Funzionalità
  - Filtraggio stateless e statefull
  - Manipolazione di pacchetti
  - Address and port translation (NAT, DNAT, SNAT, etc)
  - QoS e policy-based routing con tc ed iproute2
  - Filtering a layer 7 (L7-filter)

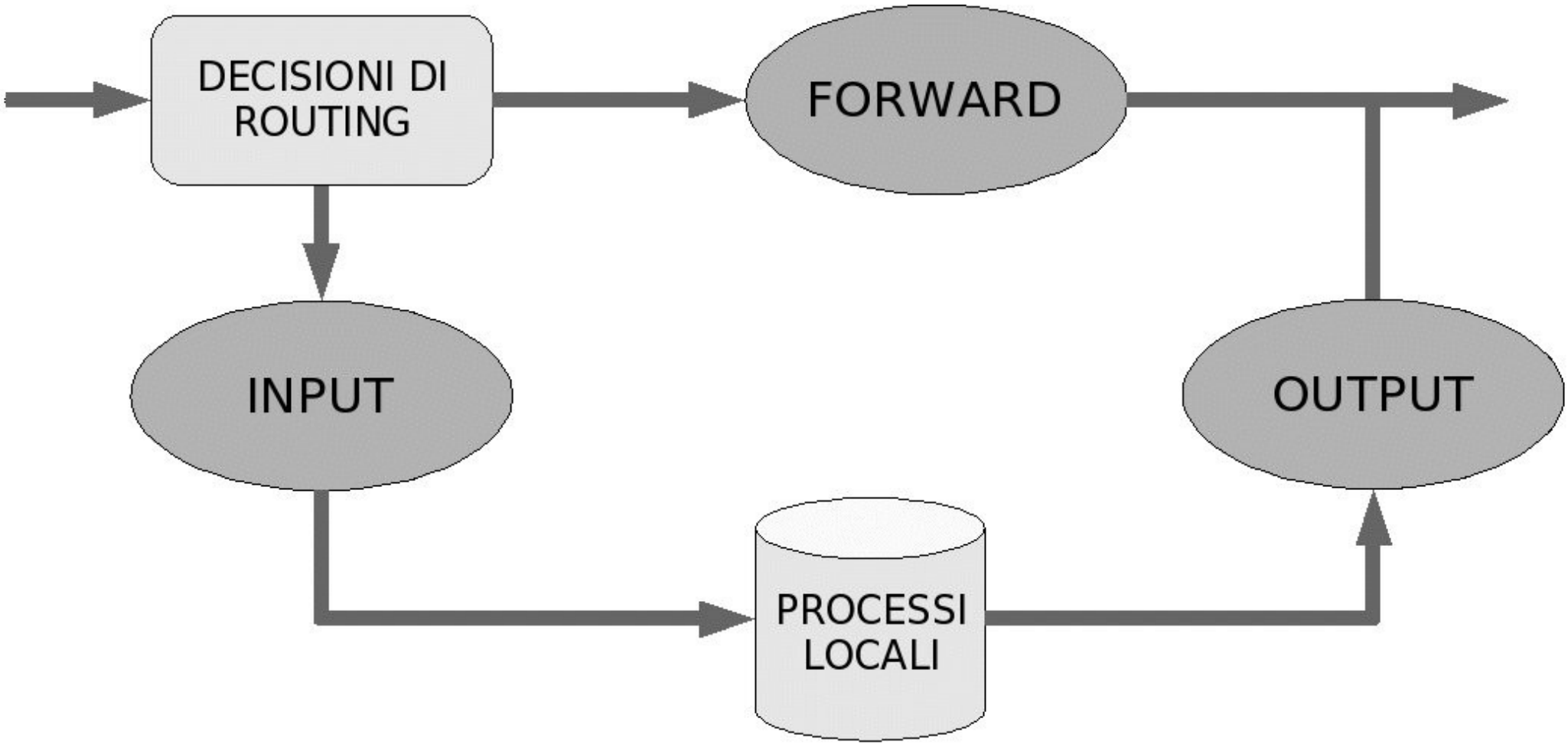
La struttura di Netfilter

- Basata su tabelle
- Le tabelle sono suddivise in catene
- Le catene sono composte da regole

Linux Iptables Firewall Schema



Particolare: la tabella di filtraggio



La tabella filter

- Effettua il filtraggio del traffico
- INPUT
  - Pacchetti in ingresso, destinati all'host locale (userspace)
- FORWARD
  - Pacchetti in transito, non destinati all'host locale
- OUTPUT
  - Pacchetti in uscita, generati dall'host locale

La tabella nat

- Permette di effettuare attività di NAT (D/S-NAT, redirezione porte, etc)
- PREROUTING
  - Pacchetti in transito prima della decisione di routing
- POSTROUTING
  - Pacchetti in transito dopo della decisione di routing
- OUTPUT / INPUT (ker 2.6.34)
  - Pacchetti in uscita / entrata

La tabella mangle

- Permette di alterare i pacchetti in transito (QoS) nelle fasi di:
  - PREROUTING
  - INPUT
  - FORWARD
  - OUTPUT
  - POSTROUTING
- To mangle: rovinare, storpiare, fare scempio
- Non dev'essere usata per il filtraggio

Applicazione delle regole da parte di Netfilter

- Per ogni pacchetto in transito in una catena
- Le regole della catena vengono scorse in ordine di inserimento
- Alla prima corrispondenza
  - Viene eseguita l'azione definita (*target*) per la regola
  - Il controllo torna alla tabella (non per LOG)
- In assenza di corrispondenze, viene applicata la regola di default (*default policy*)

Visualizzazione delle tabelle

iptables [-t tabella] -n [-v] [--line-numbers] -L [<CATENA>]

- tabella: filter (default), nat, mangle
- CATENA: INPUT, OUTPUT, FORWARD, etc

- Esempio: iptables -nL INPUT

Svuotamento delle catene

iptables -F <CATENA>

- Esempio: iptables -F INPUT

Impostazione della policy di default

iptables -P <CATENA> <AZIONE>

- CATENA: INPUT, OUTPUT, FORWARD
- AZIONE (target)
  - ACCEPT accetta il pacchetto
  - DROP scarta il pacchetto

Esempio 1

Impostazione di default policy

Impostare a DROP la default policy della catena di INPUT

Definizione di regole: aggiunta

- Aggiunta (accodamento) di una regola ad una catena

iptables -A <CATENA> [opzioni] -j AZIONE

- AZIONE
  - ACCEPT
  - DROP
  - QUEUE manda il pacchetto in user-space
  - RETURN termina l'attraversamento della catena
  - LOG logga il pacchetto (--log-prefix)

Definizione di regole: gestione

- Rimozione di una regola da una catena

  iptables -D <CATENA> [opzioni] -j AZIONE

- Inserimento/Sostituzione/Rimozione della ***k***-esima regola

Inserimento:	iptables	-I	***k*** [...]
Sostituzione:	iptables	-R	***k*** [...]
Rimozione:	iptables	-D	***k***

Definizione di regole: opzioni

Opzioni

- --protocol, -p <protocollo>
- --syn Si tratta di pacchetto SYN
- --source, -s <indirizzo>[/<maschera>]
- --destination, -d <indirizzo>[/<maschera>]
- --source-port, --sport <porta>[:<porta>]
- --destination-port, --dport <porta>[:<porta>]
- --in-interface, -i <interfaccia>
- --out-interface, -o <interfaccia>

- Operatore not: “!” – attenzione a spaziarlo

Esempio 2

Come evitare di chiudersi fuori

Impostare permesso di accesso da proprio IP

Impostare a DROP la default policy della catena di INPUT

Esercizio 1

Proteggere il firewall

Impedire accesso SSH al proprio firewall da parte degli altri

Impedire che gli altri possano utilizzare il proprio firewall come gateway (per raggiungere target)

Cercate di evitare di chiudervi fuori :-)

Estensioni per il matching

-m <match> [--match-options]

- Moduli che estendono le capacità di matching
- Ogni modulo ha le proprie specifiche opzioni aggiuntive

Tipologie di indirizzi

-m addrtype --src-type <TIPO>, --dst-type <TIPO>

- Basati sulle tabelle di routing

- Tipi di indirizzi:
  - UNSPEC — non specificato (e.g. 0.0.0.0)
  - LOCAL, PROHIBIT
  - UNICAST, BROADCAST
  - …

Commenti

-m comment -- comment “questa regola non serve a nulla”

Limiti

-m limit --limit <quantità>/second /minute /hour /day

- Un pacchetto corrisponde fintanto che il numero di pacchetti che corrispondono alla regola spera il limite
- L'opzione --limit-burst indica il numero massimo d pacchetti da lasciar passare prima di attivare il matching

MAC address

-m mac --mac-source XX:XX:XX:XX:XX:XX

MAC address

-m mac --mac-source XX:XX:XX:XX:XX:XX

A chi viene in mente qualcosa?

MAC address

-m mac --mac-source XX:XX:XX:XX:XX:XX

Italians: spaghetti, pizza, mandolino, ARP spoofing!

Scenario d'attacco

- L'attaccante avvelena la tabella ARP del client sostituendo il MAC del gateway con il proprio
- Il client inizia ad inviare all'attaccante le comunicazioni per target
- L'attaccante le inoltra al gateway (includendovi il proprio MAC address), affinché questo le inoltri a sua volta a target
- Il traffico di ritorno passa quindi di nuovo nelle mani dell'attaccante

Esercizio 2

ARP spoofing mitigation (dei poveri)

Implementare un sistema lato firewall che

impedisca agli altri host di rete di

intercettare il proprio traffico con il firewall

Mitigare non è risolvere

- In questo caso per mitigare gli effetti dell'ARP spoofing generiamo un DOS

- La perdita in disponibilità di servizio sembra comunque un costo trascurabile in cambio del beneficio in confidenzialità ed integrità

Ispezione degli stati

-m state --state <STATO>

- STATI
  - NEW

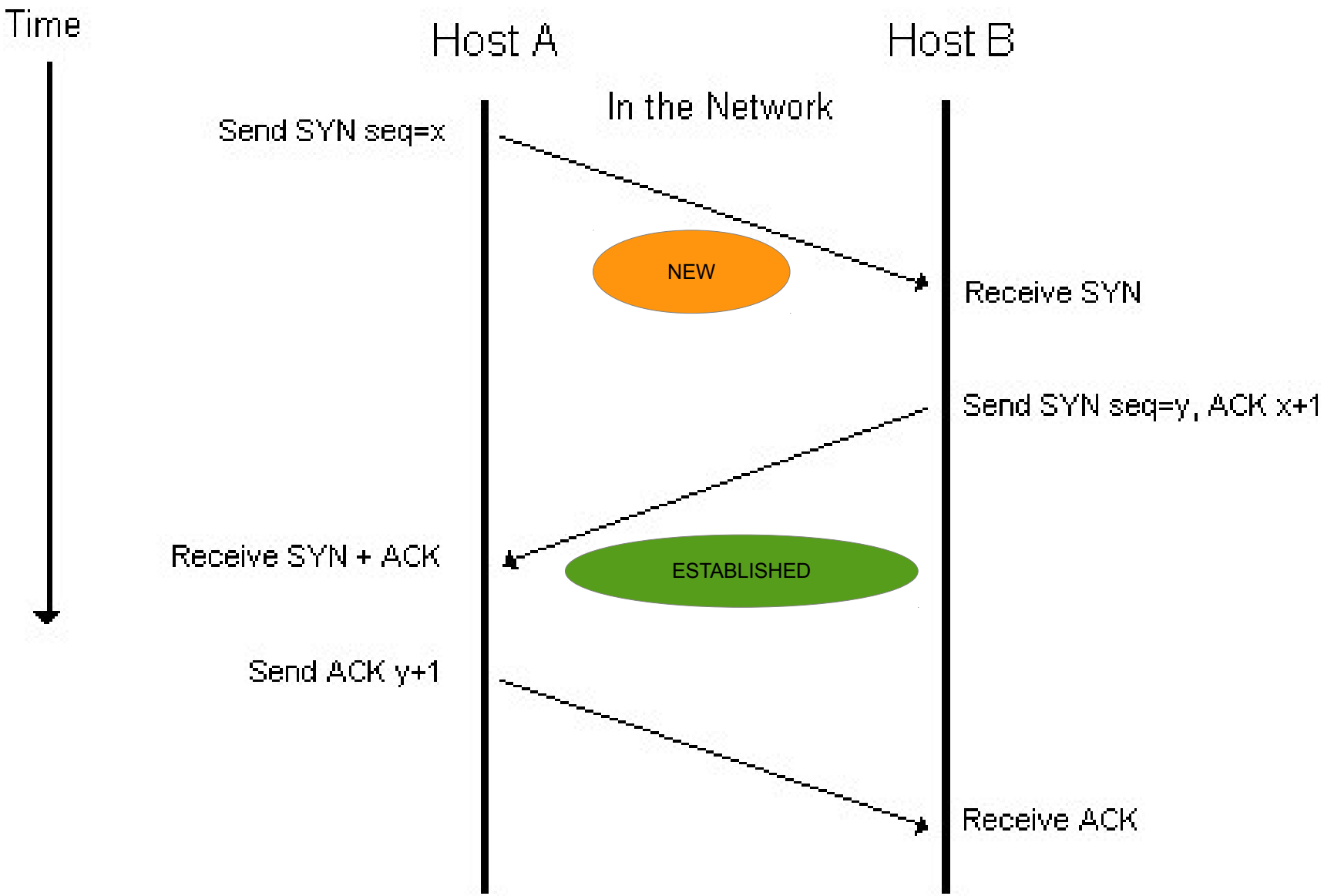
    Pacchetto SYN dell'handshaking di connessione o primo pacchetto di connessione stateless.

    La connessione non ha ancora visto pacchetti in entrambe le direzioni

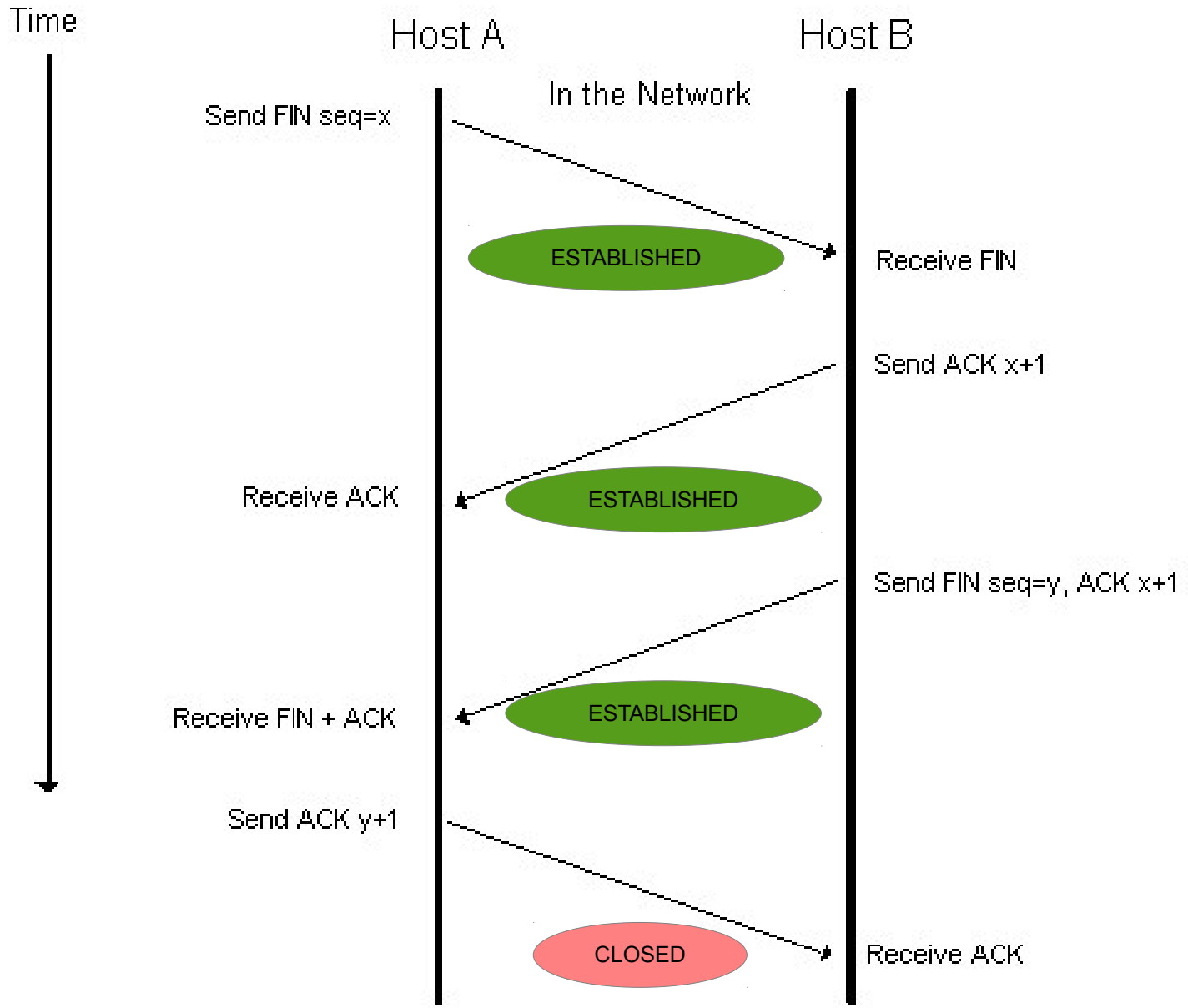
  - ESTABLISHED

    Pacchetto appartenente ad una connessione attiva (dal primo pacchetto del secondo interlocutore)

Handshake a 3 vie ed ispezione degli stati



Handshake a 4 vie ed ispezione degli stati



Ispezione degli stati

-m state --state <STATO>

- STATI
  - RELATED

    Pacchetti non facenti parte di una connessione, ma ad essa collegati (e.g. FTP data transfer, ICMP error, etc)

  - INVALID

    Nessuno degli altri.

    Non necessariamente malevolo: errori di rete, il sistema sta finendo le risorse per il tracciamento degli stati, etc

Esercizio 3

Correzione del problema riscontrato nell'Esempio 2

Impostare a DROP la default policy della catena di INPUT

facendo in modo da non chiudersi fuori e che le risposte

alle richieste inviate possano raggiungere il firewall

Filtraggio a layer 7

- Richiede modulo aggiuntivo *L7-filter*

-m layer7 --l7proto <protocollo>

- I protocolli sono quelli che ci si può aspettare (http, ftp, telnet, etc) a cui si aggiungono
  - unset: pacchetti iniziali per cui non è ancora stata rilevato il protocollo
  - unknown: protocollo sconosciuto

Università degli Studi di Verona
Corso di Laurea Magistrale in Informatica

Laboratorio di Sicurezza delle Reti

Firewall con linux: netfilter ed iptables

Andrea Zwirner


andrea@linkspirit.it


@AndreaZwirner