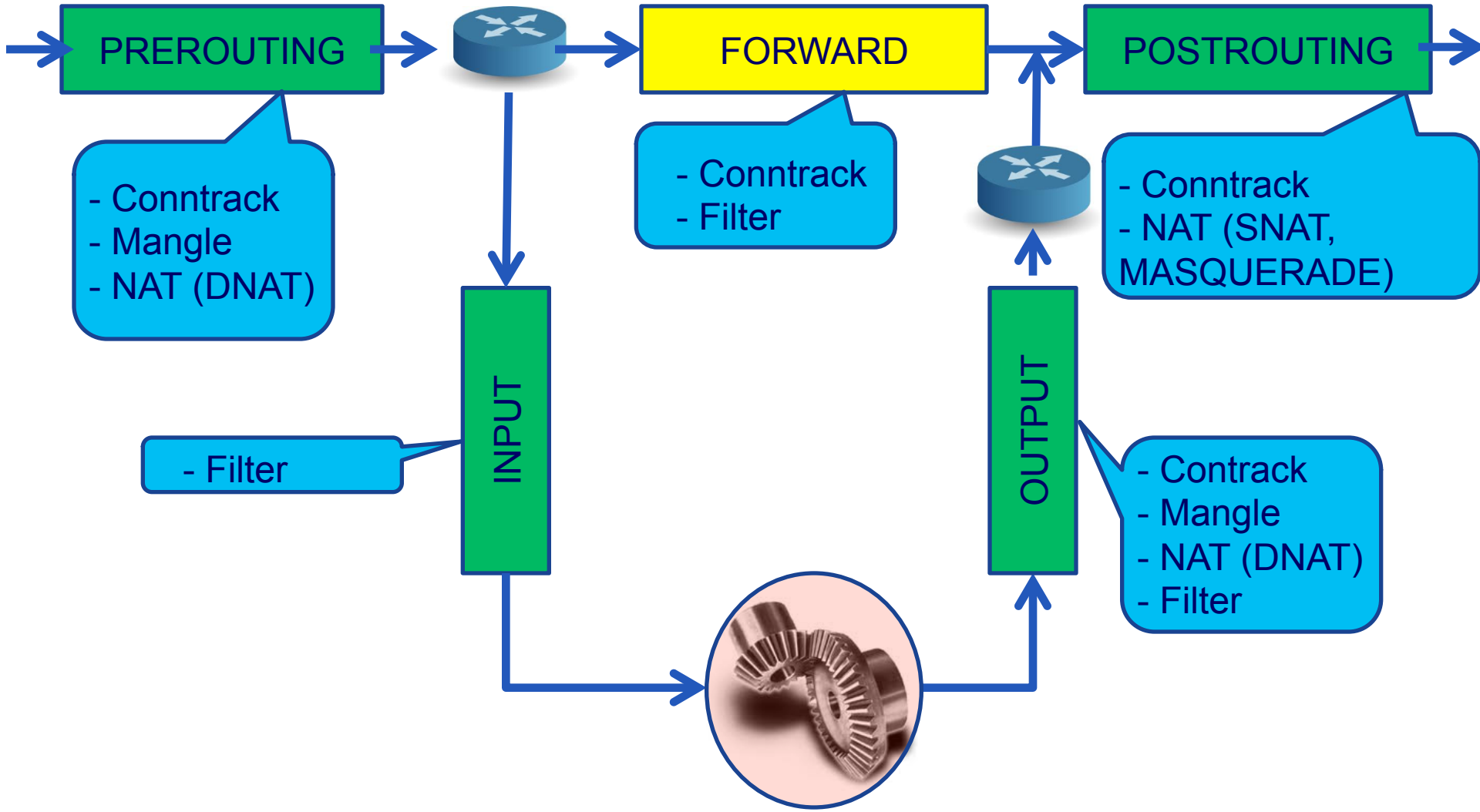
LPIC-2 TRAINING COURSE

Topic 210: IPTABLES

What is iptables?

- Stateful packet inspection
- Filtering packets based on a MAC address, IPv4, IPv6
- Filtering packets based on the value of the flags in the TPC header
- NAT/NAPT support
- System logging of network activities
- Packet manupulation (mangling) like altering TOS/DSCP/ECN bits

Network Package Flow



Processing For Packets

Table Type	Table Function	Chain	Chain Function
Filter	Packet Filtering	FORWARD	Filter packets to servers accessible by another NIC on the firewall
		INPUT	Filter packets destined to the firewall
		OUTPUT	Filter packets orinating from the firewall
Nat	Network Address Translation	PREROUTING	Address translation occurs before routing. Used with NAT of the destination IP address (DNAT)
		POST ROUTING	Address translation occurs after routing. Used with NAT of the source IP address (Source NAT or SNAT)
		OUTPUT	NAT for packets generated by the firewall (rarely used)
Mangle	TCP header modification	PREROUTING OUTPUT	Modification of the TCP packet QoS bits before routing occurs

Targets and Jumps (1/2)

- **ACCEPT**
  - ***iptables*** stops further processing
  - The packet is handed over to the end application or the OS for processing
- **DROP**
  - ***iptables*** stop further processing
  - The packet is blocked
- **LOG**
  - The packet information is sent to the syslog daemon
  - ***iptables*** *continues processing with the next rule in the table*
- **REJECT**
  - Works like the DROP target, but will also return an error message to the host sending the packet

Targets and Jumps (2/2)

- **SNAT**
  - Used to do source network address translation, rewriting the source IP address of the packet
  - The source IP address is user defined:
    `--to-source <address>[:<port>]`
- **DNAT**
  - Used to do destination network address translation, rewriting the destination IP address of the packet
  - The destination IP address is user defined:
    `--to-destination <address>[:<port>]`
- **MASQUERADE**
  - Used to do Source Network Address Translation
  - Source IP address is the same as that used by the firewall's interface
    `[--to-ports <port>]`

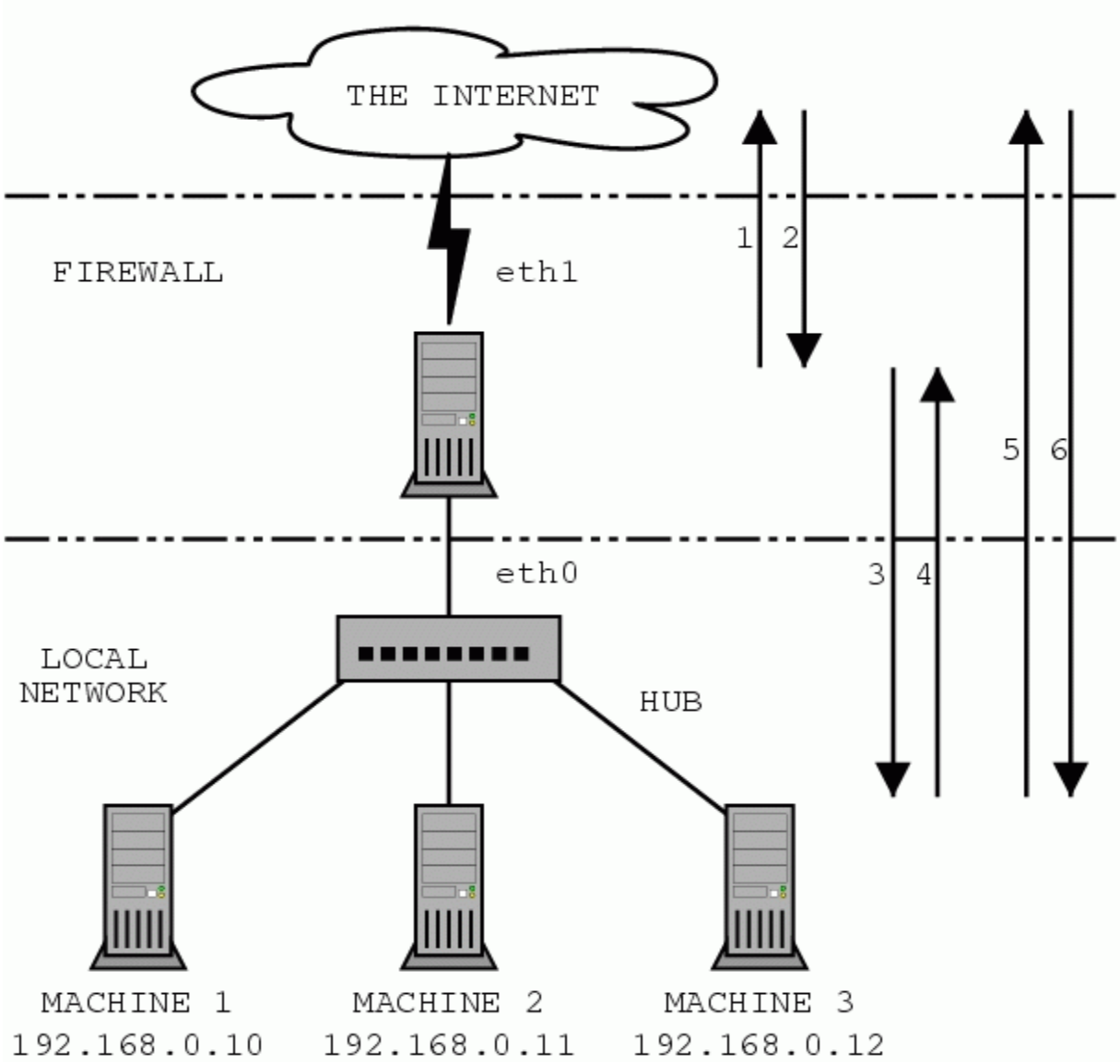
Basic of iptables command

iptables [-t table] command chain [match] [-j target]

- **table**: **nat, mangle, filter**. Default is **filter**
- **command**: **--append, --delete, --replace, --insert, --list, --flush, --policy**
- **chain**: **PREROUTING, INPUT, OUTPUT, FORWARD, POSTROUTING**
- **match**: **--protocol, --src, --src-range, --dst, --dst-range, --sport, --dport, --mac-source,--in-interface, --out-interface, --tcp-flags, --icmp-type, -m**
- **target**:
  - **-j ACCPEPT**
  - **-j DROP**
  - **-j REJECT --reject-with <REJECT-TYPE>**
  - **-j LOG --log-level**
  - **-j SNAT --to-source <IPRANGE/IP:PORTRANGE>**
  - **-j DNAT --to-destination <IPRANGE/IP:PORTRANGE>**
  - **-j MASQUERADE --to-ports <PORTRANGE>**

Example: iptables -t filter --append INPUT --protocol icmp --icmp-type echo-request -j ACCEPT

Network Example



Example commands

- **Allow ping request/reply from/to firewall:**

```
iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A INPUT  -p icmp --icmp-type echo-reply   -j ACCEPT
```

- **Allow both port 80 and 443 for webserver on inside:**

```
iptables -A FORWARD -s 0/0 -i eth1 -d 192.168.0.10 -o eth0 -p
TCP --sport 1024:65535 -m multiport --dport 80,443 -j ACCEPT

iptables -A FORWARD -d 0/0 -o eth1 -s 192.168.0.10 -i eth0 -p
TCP -m state --state ESTABLISHED -j ACCEPT
```

Managing iptables

- **Start/stop/restart iptables**

```
service iptables start|stop|restart|status
```

- **List iptables rules**

```
iptables -L -t <table>
```

- **Flush iptables rules**

```
iptables -F -t <table>
```

- **Save iptables configuration**

```
iptables-save > fw.rules
```

- **Load iptables configuration**

```
iptables-restore < fw.rules
```

Thank You !

BACKUP SLIDES

15 Most Frequently Used iptables Rules

1. Drop all package by default

```
# iptables -P INPUT -j DROP
# iptables -P FORWARD -j DROP
# iptables -P OUTPUT -j DROP
```

2. Block a specific IP Address

```
# iptables -A INPUT -s x.x.x.x -j DROP
```

3. Allow incoming SSH

```
# iptables -A INPUT -i eth0 -p tcp -s x.x.x.x/y --dport 22 -m
> state --state NEW, ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state
> ESTABLISHED -j ACCEPT
```

4. Allow outgoing SSH

```
# iptables -A INPUT -i eth0 -p tcp -d x.x.x.x/y --dport 22 -m
> state --state NEW, ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state
> ESTABLISHED -j ACCEPT
```

15 Most Frequently Used iptables Rules

5. Allow incoming HTTP and HTTPS

```
# iptables -A INPUT -i eth0 -p tcp -m multiport --dport 80,443 -m
> state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp -m multiport --sport 80,443
> -m state --state ESTABLISHED -j ACCEPT
```

6. Allow ping from outside to inside

```
# iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
# iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

7. Allow ping from inside to outside

```
# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

8. Allow loopback access

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
```

9. Allow internal network to external network

```
# iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

15 Most Frequently Used iptables Rules

10. Allow outbound DNS

```
# iptables -A OUTPUT -p udp -o eth0 --dport 53 -j ACCEPT
# iptables -A INPUT -p udp -i eth0 --sport 53 -j ACCEPT
```

11. Port Forwarding (forward all traffics that comes to port 442 to 22)

```
# iptables -A INPUT -i eth0 -p tcp --dport 422 -m state --state
> NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 422 -m state --state
> ESTABLISHED -j ACCEPT
# iptables -t nat -A PREROUTING -p tcp -d x.x.x.x --dport 422 -j
> DNAT --to x.x.x.x:22
```

12. Allow ping from inside to outside

```
# iptables -A OUTPUT -p icmp --icmp-type echo-request -j ACCEPT
# iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

13. Prevent DoS attack on webserver

```
# iptables -A INPUT -p tcp --dport 80 -m limit --limit 25/minute
> --limit-burst 100 -j ACCEPT
```

15 Most Frequently Used iptables Rules

14. Log dropped packets

```
# iptables -N LOGGING
# iptables -A LOGGING -m limit --limit 2/min -j LOG --log -prefix
> “IPTables packet dropped: ” --log-level 7
# iptables -A LOGGING -j DROP
# iptables -A INPUT -j LOGGING
```

15. Load balance incoming web traffic to 3 different IP Addresses

```
# iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state
> -- state NEW -m nth --counter 0 --every 3 --packet 0 -j DNAT
> --to-destination x.x.x.x:80
# iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state
> -- state NEW -m nth --counter 0 --every 3 --packet 1 -j DNAT
> --to-destination y.y.y.y:80
# iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state
> -- state NEW -m nth --counter 0 --every 3 --packet 2 -j DNAT
> --to-destination z.z.z.z:80
```