- **LAN1 e LAN2** devono uscire su Internet con **SNAT (IP 2.2.2.2)**.
- **LAN3 e LAN4** non devono essere sottoposte a NAT e devono essere isolate.
- **H2** deve sempre usare **1.1.1.1** per tutto il traffico (in/out).
- **Server** deve avere il servizio **HTTPS (443) accessibile da Internet**.
- **H1** deve avere il servizio **SSH (22) accessibile da Internet**.
- **LAN3 e LAN4** devono essere **bloccate sia per l'uscita su Internet che per la comunicazione con LAN1/LAN2**.
- **Server** deve rispondere solo su porta **443**.
- **M1 deve avere i servizi HTTP (8080) e HTTPS (4433) mappati sulle porte pubbliche 80 e 443** di R1.
- **M1 deve avere un indirizzo pubblico dedicato per comunicare con la rete aziendale**.
- **Tutto il traffico in entrata da Internet verso la rete aziendale deve essere bloccato**, tranne per i servizi in esecuzione su M1.

1️⃣ Configurazione NAT (Source e Destination NAT)

📌 Source NAT per LAN1 e LAN2

```
iptables -t nat -A POSTROUTING -s 192.168.254.0/24 -o eth0 -j SNAT --to-source 2.2.2.2
iptables -t nat -A POSTROUTING -s 192.168.253.0/24 -o eth0 -j SNAT --to-source 2.2.2.2
```

📌 Evitare il NAT per LAN3 e LAN4

```
iptables -t nat -A POSTROUTING -s 192.168.252.0/24 -o eth0 -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.251.0/24 -o eth0 -j ACCEPT
```

📌 Dedicare IP pubblico 1.1.1.1 per H2

```
iptables -t nat -A PREROUTING -d 1.1.1.1 -j DNAT --to-destination 192.168.255.1
iptables -t nat -A POSTROUTING -s 192.168.255.1 -o eth0 -j SNAT --to-source 1.1.1.1
```

📌 Port Forwarding per Server HTTPS (443)

```
iptables -t nat -A PREROUTING -d 2.2.2.2 -p tcp --dport 443 -j DNAT --to-
destination 192.168.254.100:443
```

📌 Port Forwarding per SSH su H1 (22)

```
iptables -t nat -A PREROUTING -d 2.2.2.2 -p tcp --dport 22 -j DNAT --to-
destination 192.168.253.50:22
```

📌 Port Forwarding per i servizi HTTP e HTTPS di M1

```
iptables -t nat -A PREROUTING -d 2.2.2.2 -p tcp --dport 80 -j DNAT --to-
destination 192.168.252.10:8080
iptables -t nat -A PREROUTING -d 2.2.2.2 -p tcp --dport 443 -j DNAT --to-
destination 192.168.252.10:4433
```

📌 IP pubblico dedicato per M1

```
iptables -t nat -A PREROUTING -d 3.3.3.3 -j DNAT --to-destination
192.168.252.10
iptables -t nat -A POSTROUTING -s 192.168.252.10 -o eth0 -j SNAT --to-source
3.3.3.3
```

2️⃣ Firewalling con `iptables` (filter table)

📌 Bloccare l'uscita su Internet da LAN3 e LAN4

```
iptables -A FORWARD -s 192.168.252.0/24 -o eth0 -j DROP
iptables -A FORWARD -s 192.168.251.0/24 -o eth0 -j DROP
```

📌 Consentire solo il traffico HTTPS per il Server

```
iptables -A FORWARD -d 192.168.254.100 -p tcp --dport 443 -m state --state
NEW,ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 192.168.254.100 -p tcp --sport 443 -m state --state
ESTABLISHED -j ACCEPT
```

📌 Bloccare la comunicazione tra LAN1/LAN2 e LAN3/LAN4

```
iptables -A FORWARD -s 192.168.254.0/24 -d 192.168.252.0/24 -j DROP
iptables -A FORWARD -s 192.168.253.0/24 -d 192.168.252.0/24 -j DROP
iptables -A FORWARD -s 192.168.252.0/24 -d 192.168.254.0/24 -j DROP
iptables -A FORWARD -s 192.168.252.0/24 -d 192.168.253.0/24 -j DROP
```

📌 Bloccare il traffico in entrata da Internet verso la rete aziendale

```
iptables -A INPUT -i eth0 -m state --state NEW -j DROP
```

📌 Consentire solo il traffico necessario verso M1

```
iptables -A INPUT -d 2.2.2.2 -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -d 2.2.2.2 -p tcp --dport 443 -j ACCEPT
```

3️⃣ Verifica della configurazione

```
iptables -t nat -L -v -n
iptables -L -v -n
```

Per verificare il traffico:

```
tcpdump -i eth0 host 3.3.3.3
tcpdump -i eth1 port 4433
```