VM APPLICATIF :

```
# RESET ALL RULES
iptables -F
iptables -X


# Allow loopback (local)
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Allow established and related connections
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT


# SSH ACCESS
iptables -A INPUT -p tcp --dport 22 -s 192.168.10.0/27 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -d 192.168.10.0/27 -j ACCEPT

# HTTP / HTTPS ACCESS (from all internal VLANs)
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 192.168.10.0/27 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 192.168.20.0/25 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 192.168.11.0/28 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 192.168.21.0/27 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 10.0.3.2/30 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 192.168.12.0/28 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 -s 192.168.22.0/27 -j ACCEPT



# Allow outgoing web traffic
iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -j ACCEPT

# Allow all outgoing traffic via ens18 (for updates, external connections)
iptables -A OUTPUT -o ens18 -j ACCEPT

# Allow established inbound traffic coming back from Internet (responses)
iptables -A INPUT -i ens18 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT


# MYSQL DATABASE (accessible only from VM réseau)
iptables -A INPUT -p tcp --dport 3306 -s 10.0.1.2 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 3306 -d 10.0.1.2 -j ACCEPT

# LOGS TO OPENOBSERVE (VM Réseau)
iptables -A OUTPUT -p tcp -d 10.0.1.2 --dport 5080 -j ACCEPT
iptables -A OUTPUT -p tcp -d 10.0.1.2 --dport 443 -j ACCEPT
```

```
# DNS + DHCP CLIENT
# DNS requests to VM réseau
iptables -A OUTPUT -p udp --dport 53 -d 10.0.1.2 -j ACCEPT
iptables -A INPUT  -p udp --sport 53 -s 10.0.1.2 -j ACCEPT


# DHCP (client)
iptables -A OUTPUT -p udp --dport 67:68 -j ACCEPT
iptables -A INPUT  -p udp --sport 67:68 -j ACCEPT


# DEFAULT POLICIES (set at the end)
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

iptables-save
```

VM-RESEAU :

```
# RESET ALL RULES
iptables -F
iptables -X

# Allow loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Allow established and related
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# SSH (Admin access)
iptables -A INPUT -p tcp --dport 22 -s 192.168.10.0/27 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -d 192.168.10.0/27 -j ACCEPT

# DNS SERVER (UDP & TCP)
iptables -A INPUT -p udp --dport 53 -s 192.168.10.0/27 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -s 192.168.20.0/25 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -s 192.168.11.0/28 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -s 192.168.21.0/27 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -s 192.168.12.0/28 -j ACCEPT
iptables -A INPUT -p udp --dport 53 -s 192.168.22.0/27 -j ACCEPT
iptables -A INPUT -p tcp --dport 53 -m conntrack --ctstate NEW -j ACCEPT

# DHCP SERVER (UDP 67,68)
```

```
iptables -A INPUT -p udp --dport 67:68 -j ACCEPT
iptables -A OUTPUT -p udp --sport 67:68 -j ACCEPT

# MONITORING (OpenObserve / Web interface)
iptables -A INPUT -p tcp --dport 5080 -s 192.168.10.0/27 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 192.168.10.0/27 -j ACCEPT
iptables -A INPUT -p tcp --dport 5080 -s 192.168.20.0/25 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 192.168.20.0/25 -j ACCEPT
iptables -A INPUT -p tcp --dport 5080 -s 192.168.11.0/28 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 192.168.11.0/28 -j ACCEPT
iptables -A INPUT -p tcp --dport 5080 -s 192.168.21.0/27 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 192.168.21.0/27 -j ACCEPT
iptables -A INPUT -p tcp --dport 5080 -s 192.168.12.0/28 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 192.168.12.0/28 -j ACCEPT
iptables -A INPUT -p tcp --dport 5080 -s 192.168.22.0/27 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 192.168.22.0/27 -j ACCEPT

iptables -A INPUT -p tcp --dport 5080 -s 10.0.1.3/29  -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -s 10.0.1.3/29 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -s 10.0.1.3/29 -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443,5080 -s 10.0.1.3 -j ACCEPT

iptables -A INPUT -p tcp --dport 9100 -s 10.0.1.3 -j ACCEPT



# Outgoing web & updates
iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
iptables -A OUTPUT -o ens18 -j ACCEPT

# Default policies
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

# Save configuration
iptables-save > /etc/iptables/rules.v4
```