iptables?

```
#!/bin/bash

iptables -F     # Flush out the rules
iptables -X     # Delete all custom chains

# Setting up custom IP chains

# Application server only access ?? AP server ?? CRM
iptables -N SERVER-ONLY
iptables -A SERVER-ONLY -s 192.168.1.3 -j ACCEPT
iptables -A SERVER-ONLY -j DROP

# Administrator level access ???
iptables -N ADMIN-LEVEL
iptables -A ADMIN-LEVEL -s 192.168.1.0/255.255.255.0 -j ACCEPT
iptables -A ADMIN-LEVEL -j DROP

# User level access (add external phone users, extensions) ????
iptables -N USER-LEVEL
# auto-extensions
iptables -A USER-LEVEL -s 99.99.99.91 -j ACCEPT # auto-extension-1001
iptables -A USER-LEVEL -s 99.99.99.92 -j ACCEPT # auto-extension-1002
iptables -A USER-LEVEL -s 99.99.99.93 -j ACCEPT # auto-extension-1003
iptables -A USER-LEVEL -j ADMIN-LEVEL

# Trunk level access (add additional SIP trunks here) ???
iptables -N TRUNK-LEVEL
iptables -A TRUNK-LEVEL -s 88.88.88.88 -j ACCEPT
iptables -A TRUNK-LEVEL -j USER-LEVEL

# Basic rules
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow ports
iptables -A INPUT -p icmp --icmp-type 8 -j USER-LEVEL       # allow ping (optional)
iptables -A INPUT -p tcp --dport 22 -j ADMIN-LEVEL          # ssh
iptables -A INPUT -p tcp --dport 80 -j ADMIN-LEVEL          # freepbx http interface
iptables -A INPUT -p tcp --dport 5060 -j TRUNK-LEVEL        # sip
iptables -A INPUT -p udp --dport 5060 -j TRUNK-LEVEL        # sip
iptables -A INPUT -p udp --dport 10000:20000 -j USER-LEVEL  # rtp range
iptables -A INPUT -p tcp --dport 50080 -j SERVER-ONLY       # server scripts

# Set default actions
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

```
# Save configuration
service iptables save
```