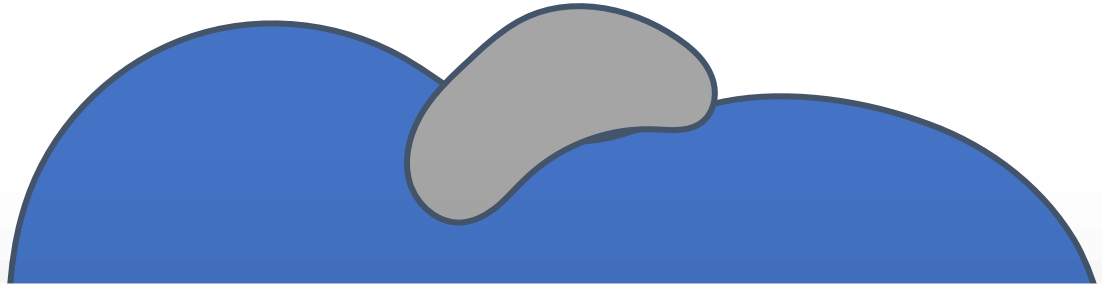
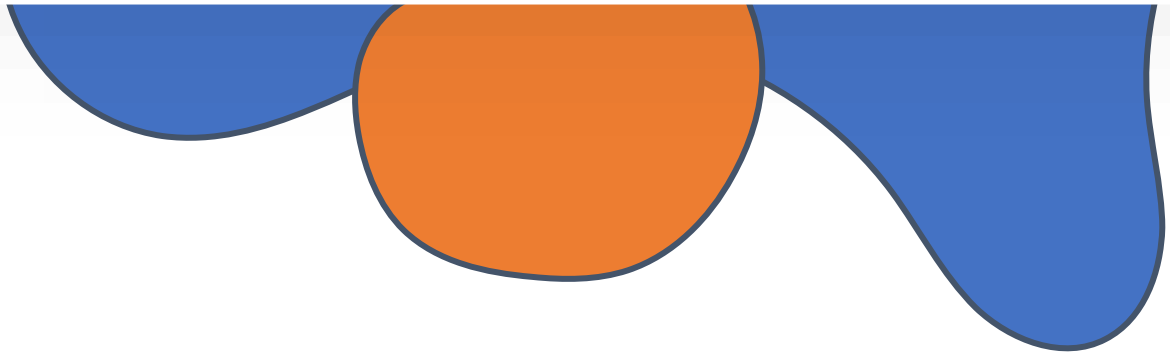

KODEKLOUD

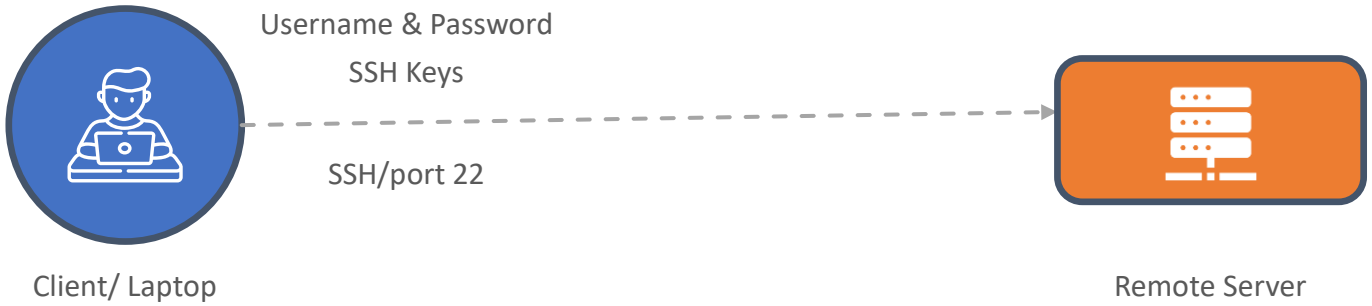


# IP Tables

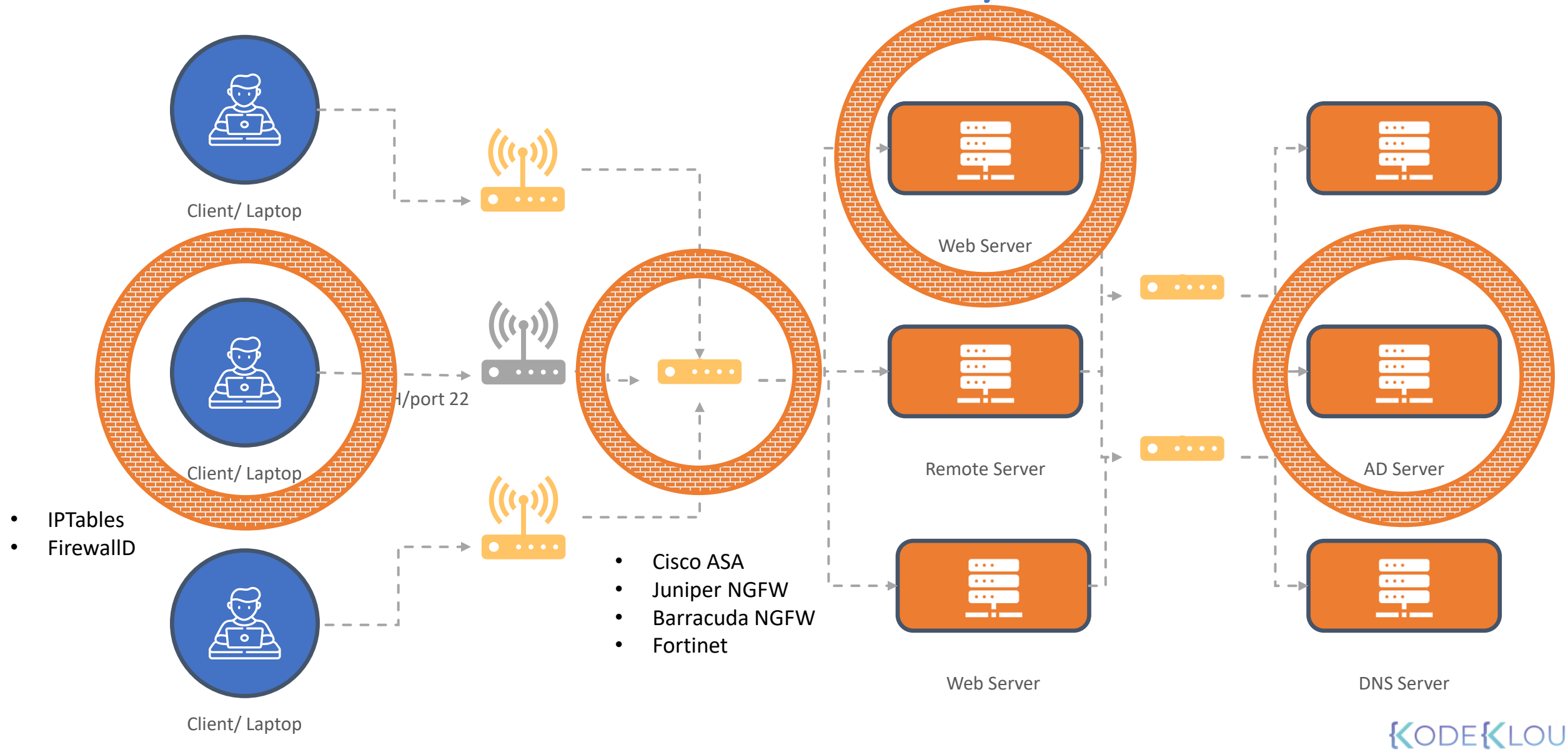
The Linux Basics Course



# Network Security



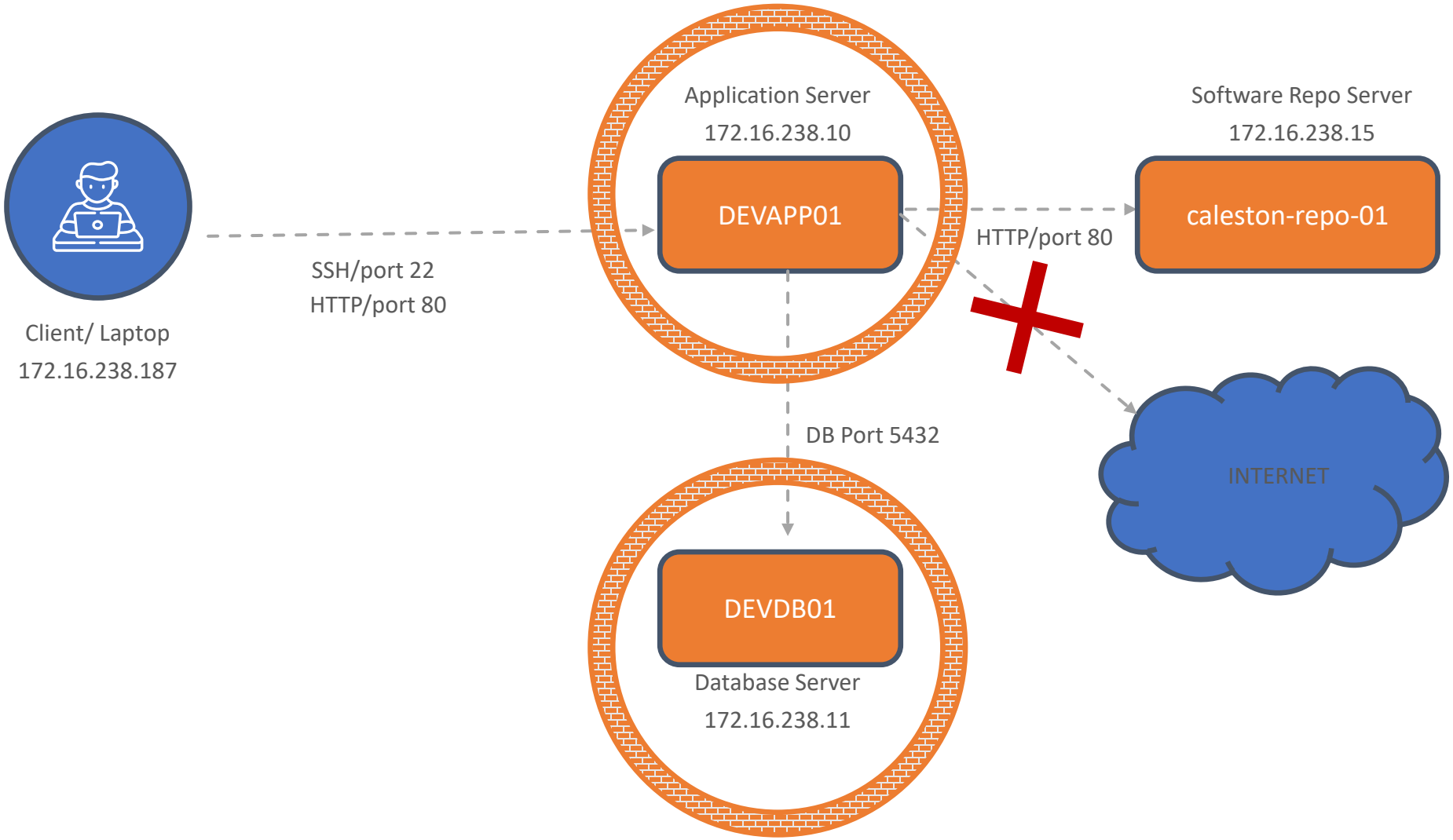
# Network Security



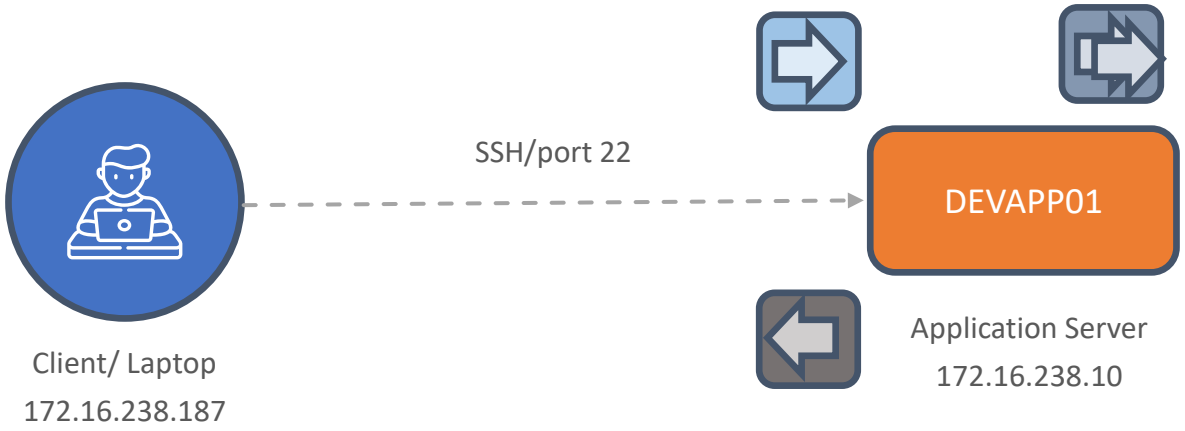

- IPTables
- FirewallD

- Cisco ASA
- Juniper NGFW
- Barracuda NGFW
- Fortinet

# IPTABLES



# IPTABLES




```
[bob@devapp01 ~]$ sudo apt install iptables
```

```
[bob@devapp01 ~]$ sudo iptables -L
```

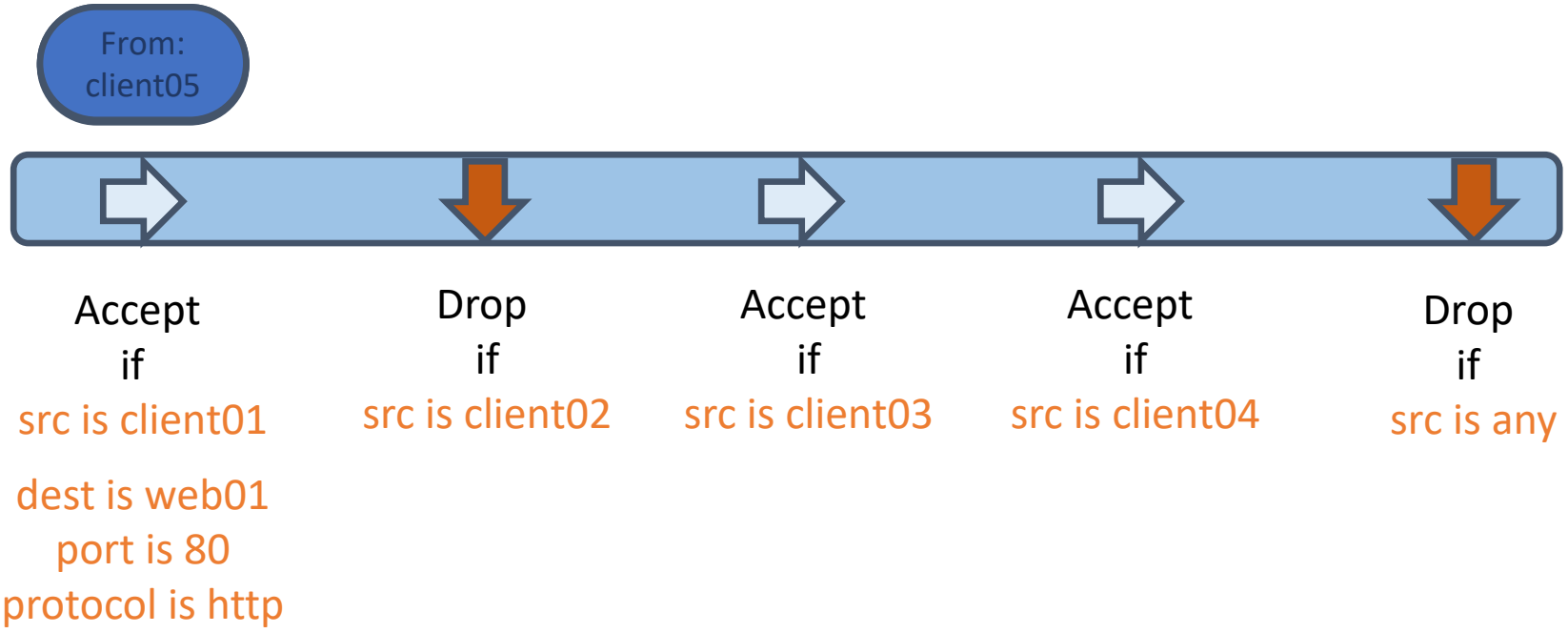
```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

# IPTABLES

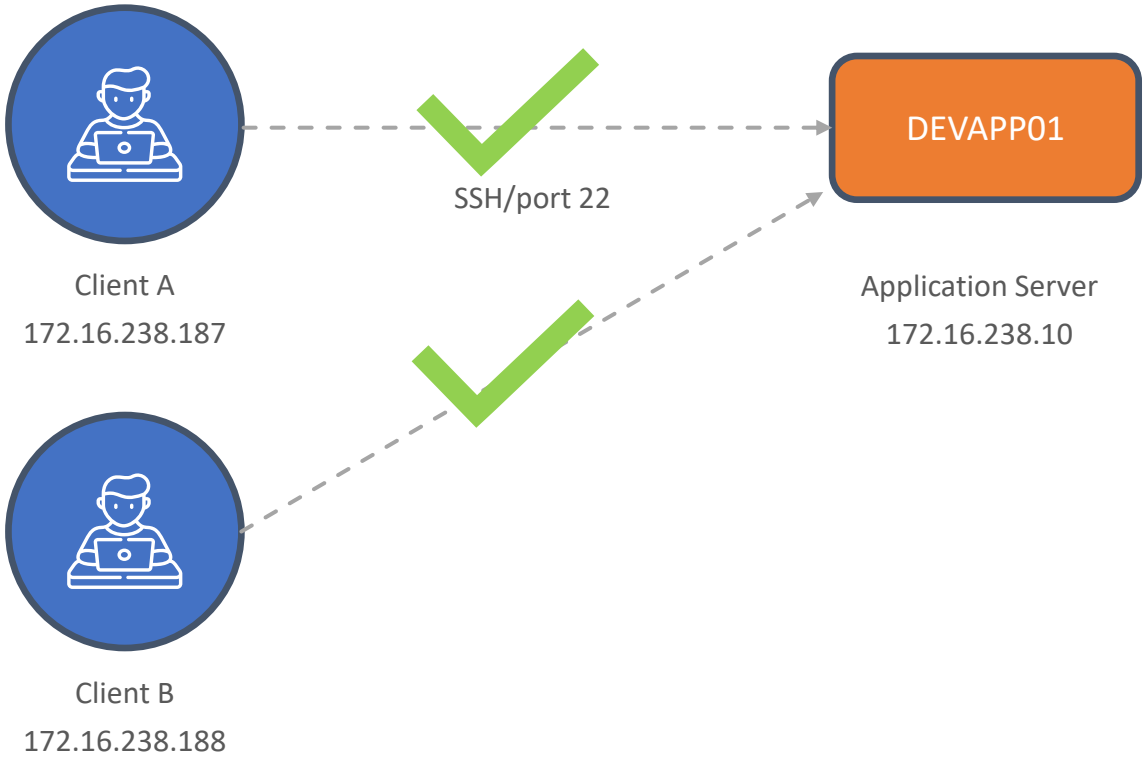
# IPTABLES



# IPTABLES

```
[bob@devapp01 ~]$ iptables -A INPUT -p tcp -s 172.16.238.187 --dport 22 -j ACCEPT
```

```
[bob@devapp01 ~]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  172.16.238.187       anywhere            tcp dpt:ssh
```




| Option | Description |
|---|---|
| -A | Add Rule |
| -p | Protocol |
| -s | Source |
| -d | Destination |
| --dport | Destination port |
| -j | Action to take |

# IPTABLES

```
[bob@devapp01 ~]$ iptables -A INPUT -p tcp --dport 22 -j DROP
```

```
[bob@devapp01 ~]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  172.16.238.187       anywhere             tcp dpt:ssh --▸ 1
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh --▸ 2

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

| Option | Description |
|---|---|
| -A | Add Rule |
| -p | Protocol |
| -s | Source |
| -d | Destination |
| --dport | Destination port |
| -j | Action to take |


Client B
172.16.238.188

Application Server
172.16.238.10

KODEKLOUD

# IPTABLES

```
[bob@devapp01 ~]$ iptables -L

Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  -- 172.16.238.187        anywhere            tcp dpt:ssh  --> 1
DROP       tcp  --  anywhere             anywhere            tcp dpt:ssh  --> 2

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

| Rule # | Description |
|---|---|
| 1 | Allow SSH from caleston-lp10 |
| 2 | Drop SSH from anywhere |

# IPTABLES

| Source/ Destination | Action |
|---|---|
| devdb01 | Allow outgoing connection to port 5432 |
| caleston-repo-01 | Allow outgoing connection to port 80 |
| Internet | Drop all outgoing connections, port 80/443 (HTTP/HTTPS) |
| caleston-lp10 | Allow incoming on port 80 |

```
[bob@devapp01 ~]$ iptables -A OUTPUT -p tcp -d 172.16.238.11 --dport 5432 -j ACCEPT
```

```
[bob@devapp01 ~]$ iptables -A  OUTPUT  -p tcp -d 172.16.238.15 --dport 80 -j ACCEPT
```

```
[bob@devapp01 ~]$ iptables -A OUTPUT -p tcp --dport 443 -j DROP
[bob@devapp01 ~]$ iptables -A OUTPUT -p tcp --dport 80 -j DROP
```

```
[bob@devapp01 ~]$ iptables -A INPUT -p tcp -s 172.16.238.187 --dport 80 -j ACCEPT
```

# IPTABLES

```
[bob@devapp01 ~]$ iptables -L
```

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  172.16.238.187       anywhere             tcp dpt:ssh          ---> 1
DROP       tcp  --  anywhere             anywhere             tcp dpt:ssh          ---> 2
ACCEPT     tcp  --  172.16.238.187       anywhere             tcp dpt:http         ---> 3

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             devdb01              tcp dpt:postgresql   ---> 1
ACCEPT     tcp  --  anywhere             172.16.238.15        tcp dpt:http         ---> 2
DROP       tcp  --  anywhere             anywhere             tcp dpt:http         ---> 3
DROP       tcp  --  anywhere             anywhere             tcp dpt:https        ---> 4
```

# IPTABLES


```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             devdb01              tcp dpt:postgresql    --▸ 1
ACCEPT     tcp  --  anywhere             172.16.238.15        tcp dpt:http          --▸ 2
DROP       tcp  --  anywhere             anywhere             tcp dpt:http          --▸ 3
DROP       tcp  --  anywhere             anywhere             tcp dpt:https         --▸ 4
```

```
[bob@devapp01 ~]$ iptables -I OUTPUT -p tcp -d 172.16.238.100 --dport 443 -j ACCEPT
```

# IPTABLES

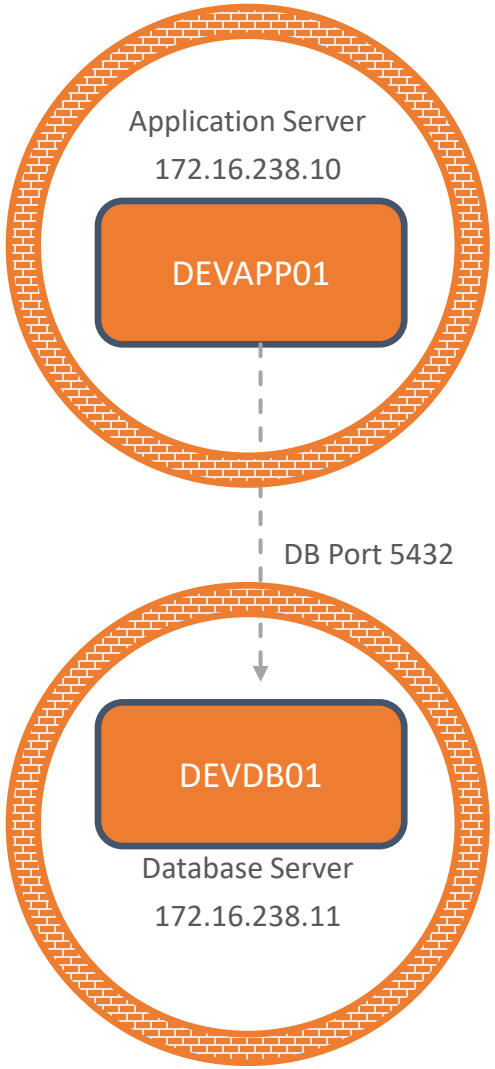

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             caleston-hq          tcp dpt:https          --> 1
ACCEPT     tcp  --  anywhere             devdb01              tcp dpt:postgresql     --> 2
ACCEPT     tcp  --  anywhere             172.16.238.15        tcp dpt:http           --> 3
DROP       tcp  --  anywhere             anywhere             tcp dpt:http           --> 4
DROP       tcp  --  anywhere             anywhere             tcp dpt:https          --> 5
```

# IPTABLES

```
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             caleston-hq          tcp dpt:https          --> 1
ACCEPT     tcp  --  anywhere             devdb01              tcp dpt:postgresql     --> 2
ACCEPT     tcp  --  anywhere             172.16.238.15        tcp dpt:http           --> 3
DROP       tcp  --  anywhere             anywhere             tcp dpt:http           --> 4
DROP       tcp  --  anywhere             anywhere             tcp dpt:https          --> 5
```

```
[bob@devapp01 ~]$ iptables -D OUTPUT 5
```

# IPTABLES




```
[bob@devdb01 ~]$ iptables -A INPUT -p tcp -s 172.16.238.10 --dport 5432 -j ACCEPT
```

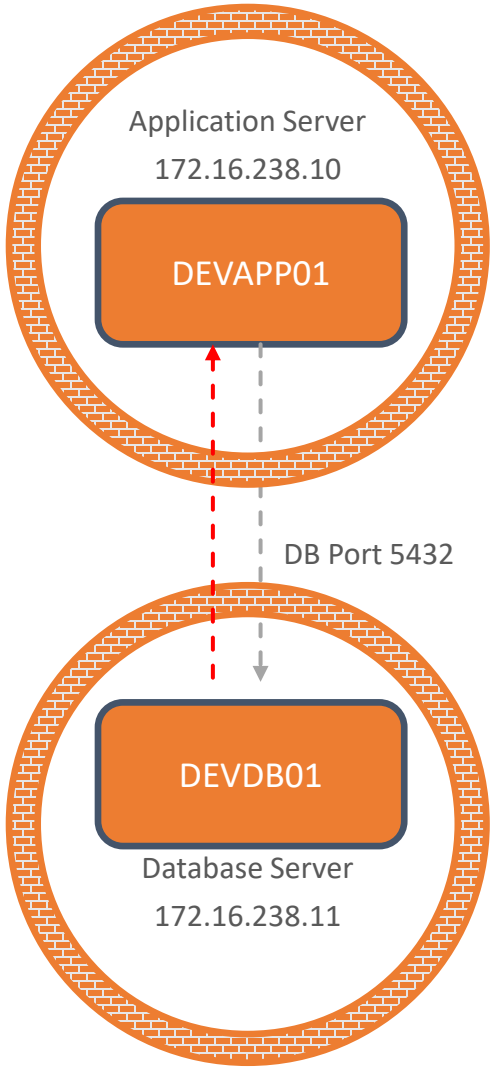
```
[bob@devdb01 ~]$ iptables -A  INPUT  -p tcp --dport 5432 -j DROP
```

```
[bob@devdb01 ~]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  172.16.238.10        anywhere             tcp dpt:5432
DROP       tcp  --  anywhere             anywhere             tcp dpt:5432

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

# IPTABLES




```
[bob@devapp01 ~]$ iptables -A OUTPUT -p tcp -d 172.16.238.11 --dport 5432 -j ACCEPT
```

```
[bob@devdb01 ~]$ iptables -A INPUT -p tcp -s 172.16.238.10 --dport 5432 -j ACCEPT
```

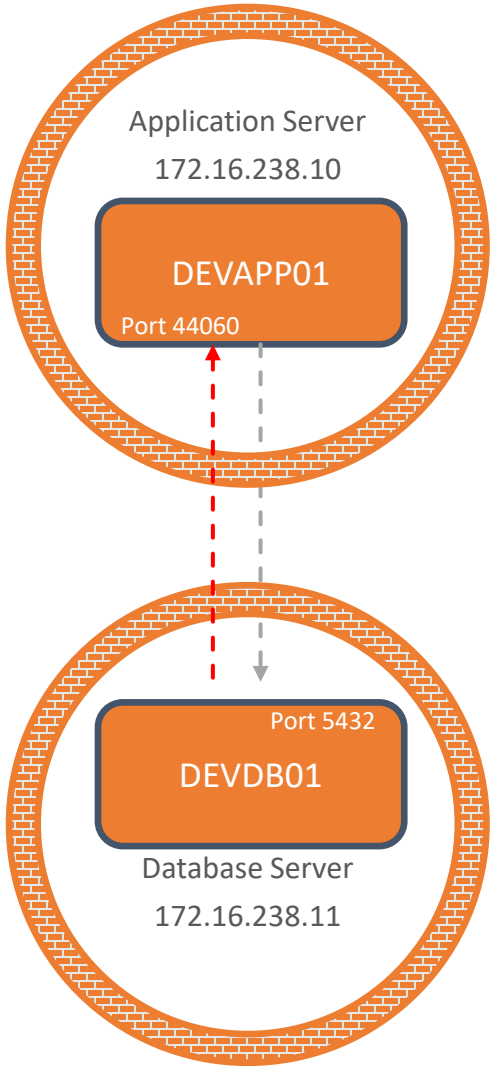
```
[bob@devdb01 ~]$ iptables -A  INPUT  -p tcp --dport 5432 -j DROP
```

```
[bob@devdb01 ~]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  172.16.238.10        anywhere            tcp dpt:5432
DROP       tcp  --  anywhere             anywhere            tcp dpt:5432

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

# IPTABLES



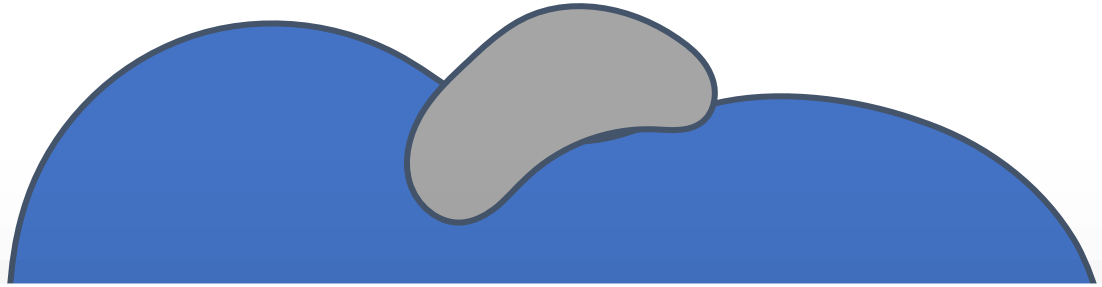

```
[bob@devdb01 ~]$ netstat -an | grep 5432
tcp        0      0 172.16.238.10:44060     172.16.238.11:5432      ESTABLISHED
```

```
[bob@devapp01 ~]$ iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  172.16.238.187       anywhere            tcp dpt:ssh
DROP       tcp  --  anywhere             anywhere            tcp dpt:ssh
ACCEPT     tcp  --  172.16.238.187       anywhere            tcp dpt:http
```

Ephemeral Port Range
32768 - 60999

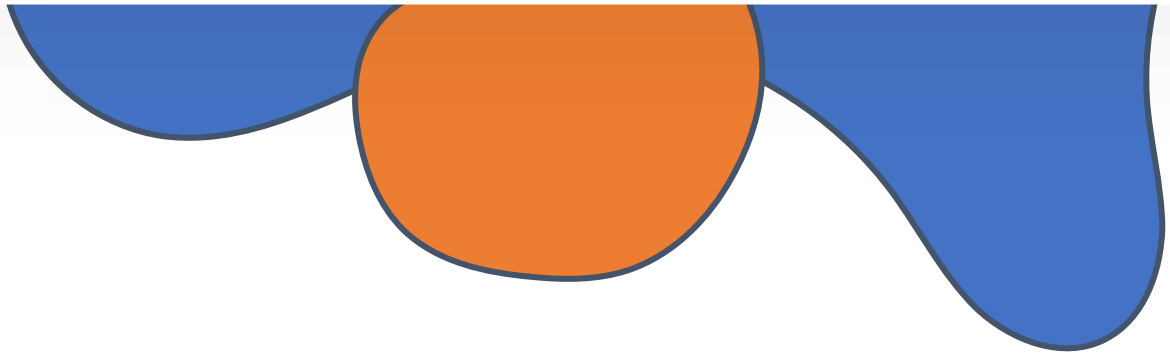
KODEKLOUD


KODEKLOUD



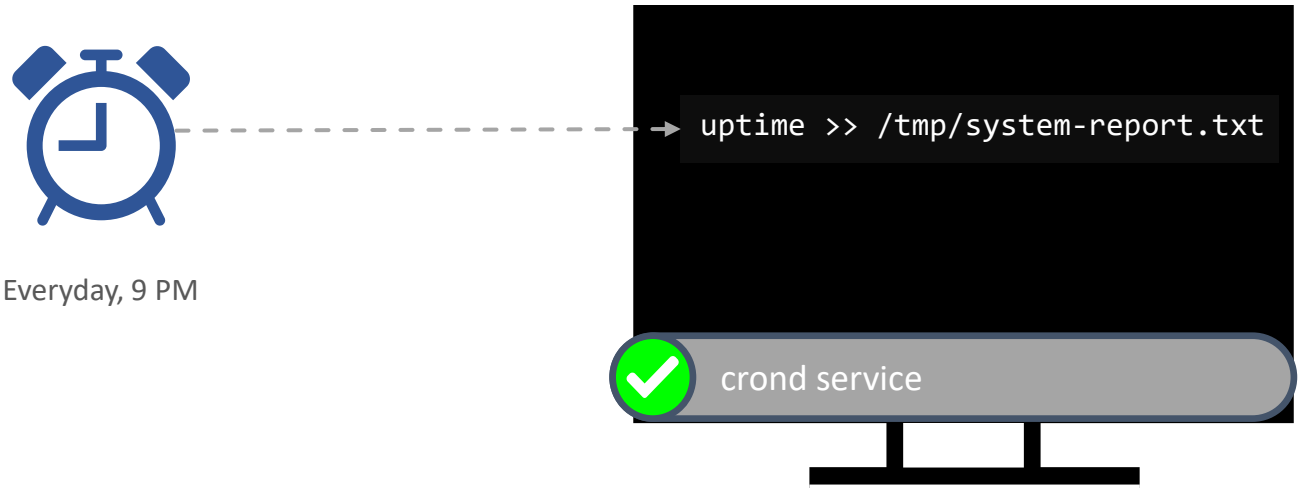
# Cron Jobs

The Linux Basics Course



# CRON

```
[michael@caleston-lp01 ~]$ uptime >> /tmp/system-report.txt
```



# CRON

```
[michael@caleston-lp01 ~]$ crontab -e
```

```
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
  0 21 *   *   *    uptime >> /tmp/system-report.txt
```

# CRON

9 PM Day Every Month Any weekday Monday

```
 00        21       *        *          *
minute    hour     day     month     weekday
```

```
0 21 * * * uptime >> /tmp/system-report.txt
```

| Requirement | Minute | Hour | Day | Month | Weekday |
|---|---|---|---|---|---|
| February 19th, 08:10 AM, Only if it's a Monday | 10 | 8 | 19 | 2 | 1 |
| February 19th, 08:10 AM, any weekday | 10 | 8 | 19 | 2 | * |
| 19th of every month at 08:10 AM, any weekday | 10 | 8 | 19 | * | * |
| Every day of every month at 08:10 AM, any weekday | 10 | 8 | * | * | * |
| Every day of every month at 10 minutes past every hour or any weekday | 10 | * | * | * | * |
| Every day of every month at every minute past every hour or any weekday | * | * | * | * | * |
| Every day of every month at every other minute past every hour or any weekday. eg: 08:02, 08:04, 08:06… 09:02, 09:04, 09:06 | */2 | * | * | * | * |
| Every day of every month at every other minute past every other hour or any weekday. eg: 08:02, 08:04, 08:06… 10:02, 10:04, 10:06… 12:02, 12:04, 12:06 | */2 | */2 | * | * | * |

# CRON

```
[michael@caleston-lp01 ~]$ crontab -l
```

```
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
0 21 * * * uptime >> /tmp/system-report.txt
```

```
[michael@caleston-lp01 ~]$ cat /tmp/system-report.txt
```

```
21:00:00 up 20:15,  1 user,  load average: 0.47, 0.50, 0.52
```

```
[michael@caleston-lp01 ~]$ tail /var/log/syslog
```

```
Jul 22 21:00:01 caleston-lp10 CRON[1720]: (michael) CMD (uptime >> /tmp/system-report.txt)
```