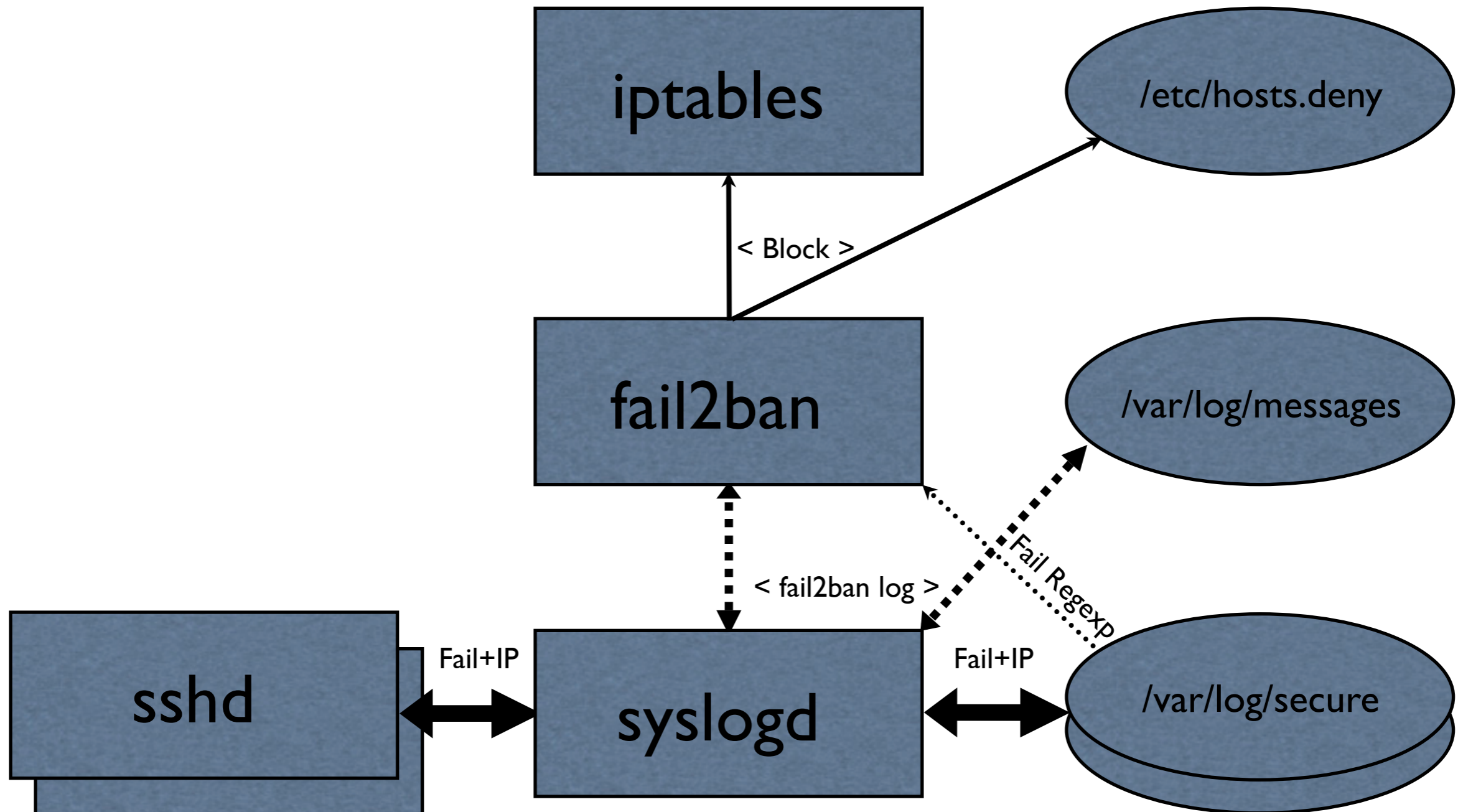


Fail2Ban Cluster Config

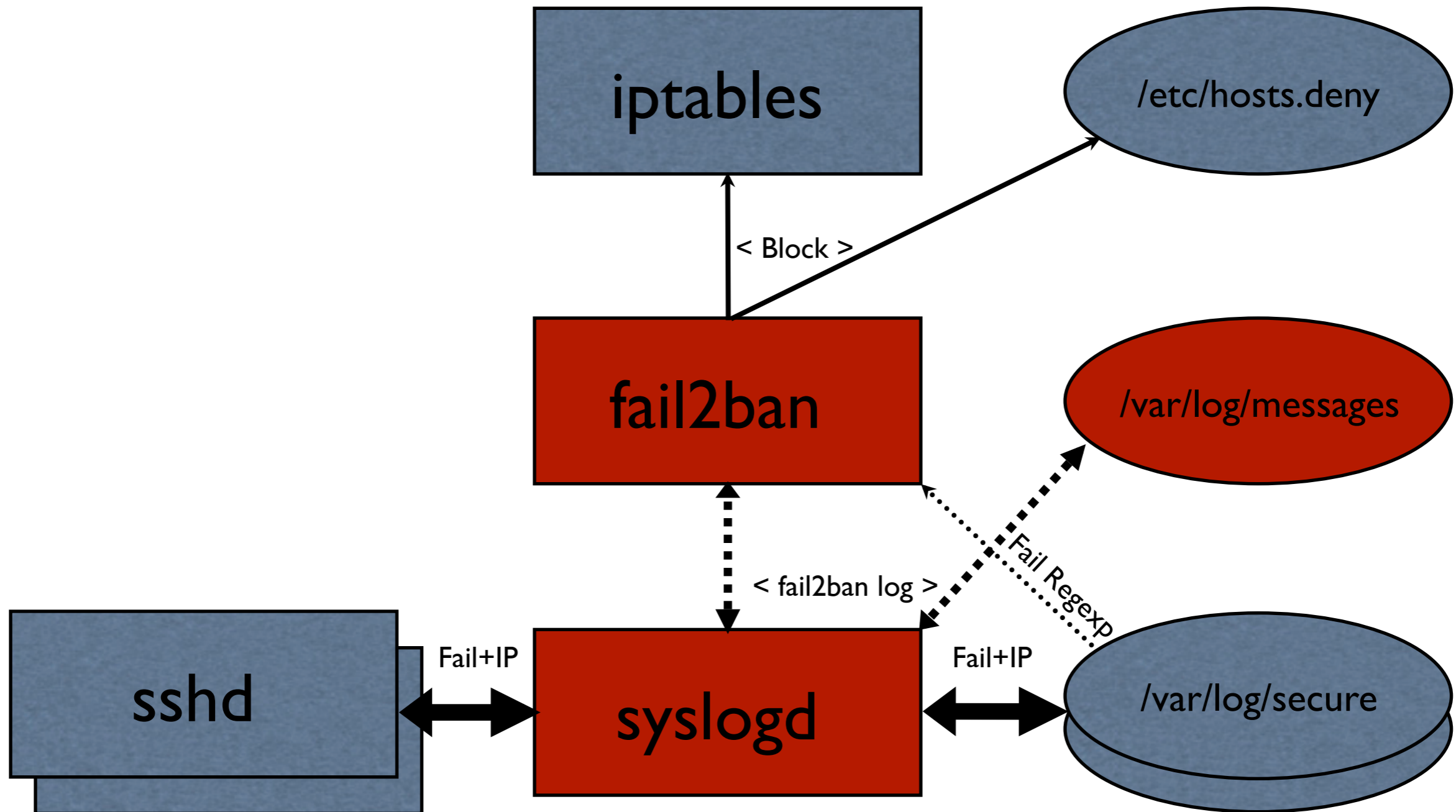
Alex Owen
&
Cozmin Timis

Particle Physics Research Centre
Queen Mary University of London

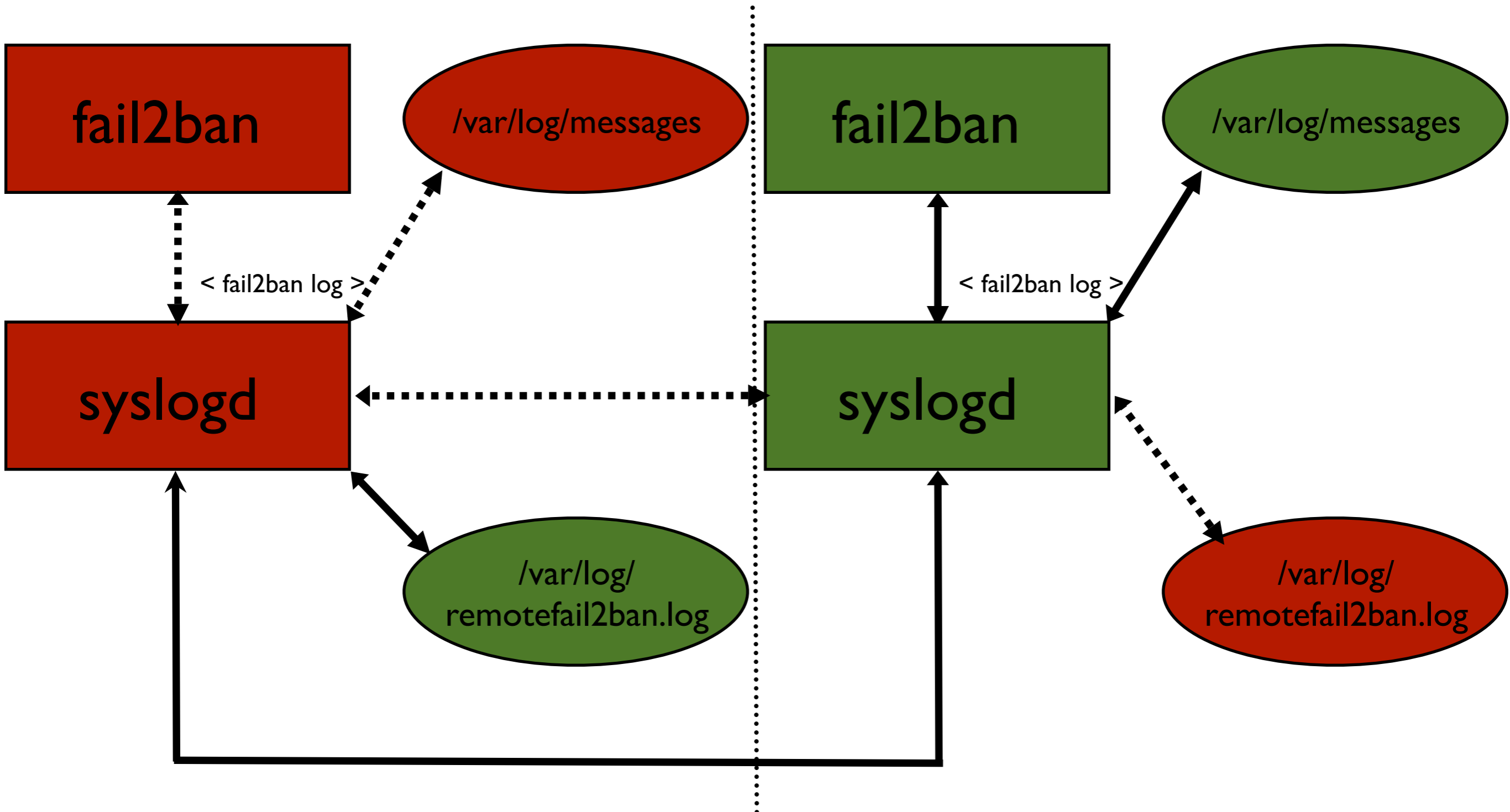
Fail2Ban Standard



Fail2Ban Action Logs



Remote Syslog Actions

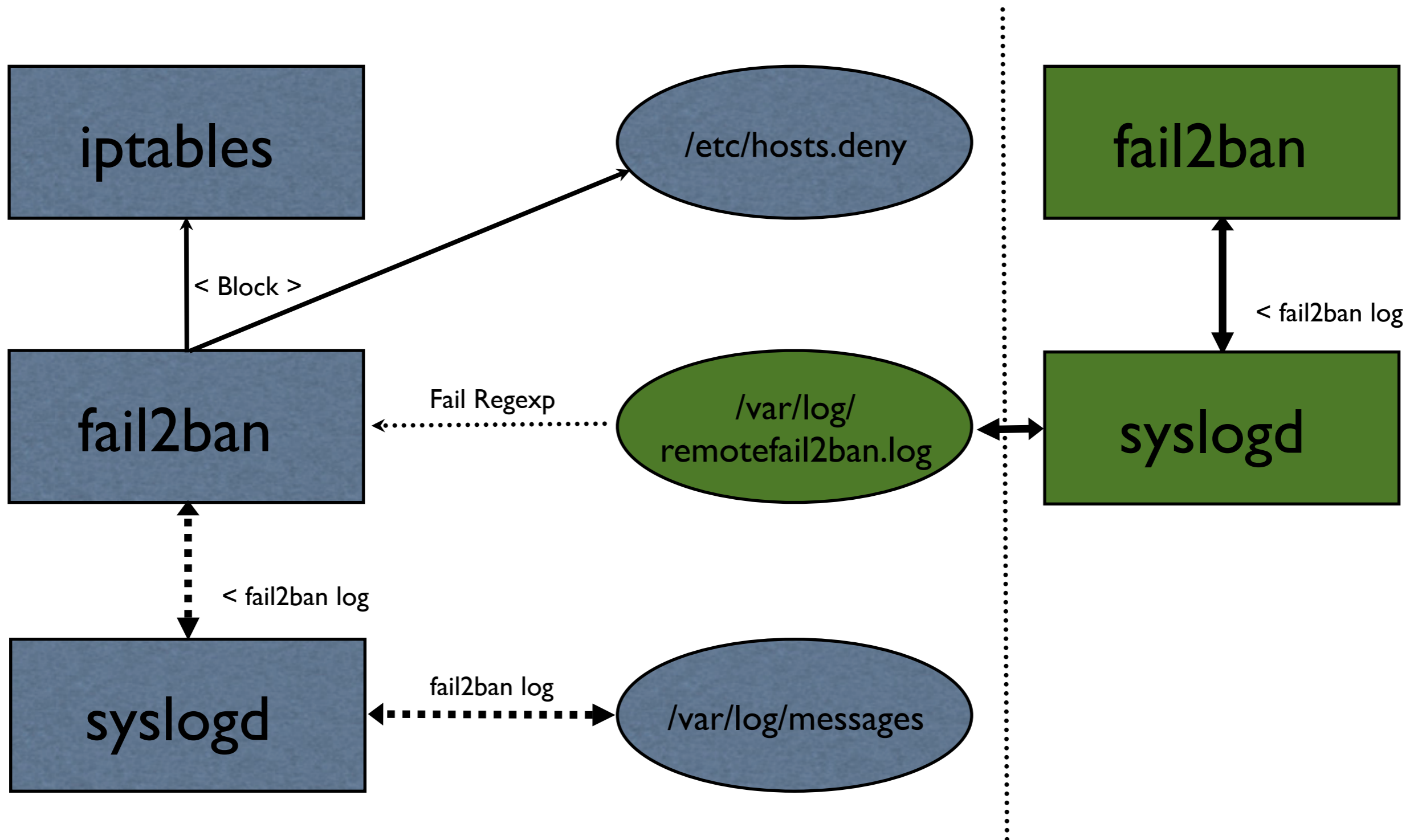


/etc/rsyslog.d/ fail2ban.conf

```
$ModLoad imudp
$UDPServerRun 514
if not( $fromhost-ip startswith '127.0.0.1' ) then /var/log/remotefail2ban.log
& ~
if $syslogfacility-text startswith 'daemon' and $syslogtag contains 'fail2ban.actions' then @remotemachine1.example.com
if $syslogfacility-text startswith 'daemon' and $syslogtag contains 'fail2ban.actions' then @remotemachine2.example.com
```

The first 2 lines enable UDP syslog reception. Adjusting your firewall to allow this for a limited case is an exercise for the reader! The next 2 lines log remote syslogs messages to a separate file and stop processing them further (to avoid infinite loops). The last 2 lines send the local Ban messages (and a few others) to the example remote hosts.

Cluster Fail2Ban



/etc/fail2ban/jail.local

```
[f2bcluster]
enabled      = true
filter       = f2bcluster
action = hostsdeny[file=/etc/hosts.deny]
           sendmail-whois[name=F2BCLUSTER, dest=root, sender=root@example.com]
logpath      = /var/log/remotefail2ban.log
maxretry     = 1
```

The stanza [f2bcluster] is the jail that monitors the remotefail2ban.log and if there is a single remote ban then triggers a local ban according to local policy. The local machine is responsible for unbanning also.

This jail uses hostsdeny you may prefer iptables

/etc/fail2ban/filter.d/ f2bcluster.local

```
[Definition]
failregex = fail2ban.actions:\ WARNING.*\ Ban\ <HOST>$
ignoreregex = f2bcluster
```

This filter is used by the f2bcluster jail to extract remote Ban messages. The ignoreregex line is important to ignore remote Ban messages due to the remote f2bcluster jail... again avoiding infinite loops!

Summary

/etc/rsyslog.d/fail2ban.conf

```
$ModLoad imudp
$UDPServerRun 514
if not( $fromhost-ip startswith '127.0.0.1' ) then /var/log/remotefail2ban.log
& ~
if $syslogfacility-text startswith 'daemon' and $syslogtag contains 'fail2ban.actions' then @remotemachine1.example.com
if $syslogfacility-text startswith 'daemon' and $syslogtag contains 'fail2ban.actions' then @remotemachine2.example.com
```

/etc/fail2ban/jail.local

```
[ssh-iptables]
enabled = false
[ssh-tcpwrapper]
enabled = true
action = hostsdeny[file=/etc/hosts.deny]
        sendmail-whois[name=SSH, dest=root, sender=root@example.com]
logpath = /var/log/secure
[f2bcluster]
enabled = true
filter = f2bcluster
action = hostsdeny[file=/etc/hosts.deny]
        sendmail-whois[name=F2BCLUSTER, dest=root, sender=root@example.com]
logpath = /var/log/remotefail2ban.log
maxretry = 1
```

/etc/fail2ban/filter.d/f2bcluster.local

```
[Definition]
failregex = fail2ban.actions:\ WARNING.*\ Ban\ <HOST>$
ignoreregex = f2bcluster
```

Imperfect

- This is a potential denial of service so think firewall
- fail2ban could be patched to “sign” with a shared secret and “check signatures” to avoid this
- This is a many to many mapping so will not scale well but is OK for small clusters eg 3

The End