

PF

pf.conf

```
#####
#####
# GLOBAL
#####
#####
block in quick on ISP proto tcp to port {9200,8080} label
"Block Spammer on port $dstport"
#####
#####
# QUEUE
#####
#####
queue rootq on em0 bandwidth 1G #, max 250M qlimit 300
    queue ssh        parent rootq bandwidth 900M #900K, min 50K burst 1M
for 200ms qlimit 50
    queue vpn        parent rootq bandwidth 900M # qlimit 100
    queue admin      parent rootq bandwidth 900M # qlimit 100
    queue main parent rootq bandwidth 200M min 10M max 200M
        queue def        parent main bandwidth 150M default
        queue rtp        parent main bandwidth 350K, min 350K burst 700K
for 200ms qlimit 50
        queue nzb        parent main bandwidth 200M qlimit 50
        queue pri        parent main bandwidth 900K, min 50K burst 1M
for 200ms qlimit 50
        queue dns        parent main bandwidth 100K, min 10K burst 200K
for 1000ms qlimit 50
        queue guests     parent main bandwidth 100M
        queue ack        parent main bandwidth 2M
        queue bulk       parent main bandwidth 160M default
#####
#####
match      proto {ospf}                                set
queue rtp          set prio 6        label "Set proto $proto to prio 6"
match      proto {tcp}                to port {bgp}                set
queue rtp          set prio 6        label "Set port $dstport to prio 6"
match      proto {esp}                                set
queue rtp          set prio 6        label "Set proto $proto to prio 6"
match      proto {udp}                to port {isakmp,ipsec-nat-t} set
queue vpn          set prio 6        label "Set port $dstport to prio 6"
match      proto {tcp}                to port {http,https}          set
queue (bulk,ack)   set prio (3, 6) label "Set port $dstport to prio
3,6"
match      proto {tcp}                to port {ssh}                set
queue ssh set tos lowdelay set prio 6        label "Set port $dstport to
prio 6"
match      proto {udp}                to port {domain}              set
```

```

queue dns                set prio 6          label "Set port $dstport to prio 6"
match    proto {tcp}      to port {563}      set
queue nzb                set prio 4          label "Set port $dstport to prio 4"
#match    proto {tcp,udp,igmp} from <guests>    set
queue guests            set prio 2          label "Set $srcaddr to $dstaddr to
prio 2"
match                                from <admin>        set
queue admin            set prio 6          label "Set $srcaddr to $dstaddr to
prio 6"
#####
#####
# GLOBAL OPTIONS
#####
#####
#set debug info
set skip on lo
set loginterface egress
set skip on lo0
set skip on enc0
#set optimization conservative
#set ruleset-optimization basic
#####
#####
# TABLES
#####
#####
table <attacker>        persist
table <tor>             persist file "/etc/pf_tables/pf.tor"
table <ransom>          persist file "/etc/pf_tables/pf.ransom"
table <malware>         persist file "/etc/pf_tables/pf.malware"
table <adhosts>         persist file "/etc/pf_tables/pf.adhosts"
table <country>         persist file "/etc/pf_tables/pf.country"
#####
#####
table <firewall>        const { self }
table <GC-MV>           persist file "/etc/pf_tables/pf.GC-MV"
table <GC-TG>           persist file "/etc/pf_tables/pf.GC-TG"
table <GC-SB>           persist file "/etc/pf_tables/pf.GC-SB"
table <HP>              persist file "/etc/pf_tables/pf.HP"
table <GC>              persist file "/etc/pf_tables/pf.GC"
table <RZ-FW>           persist file "/etc/pf_tables/pf.RZ-FW"
table <RZ-CORE>         persist file "/etc/pf_tables/pf.CORE"
table <openvpn>         persist file "/etc/pf_tables/pf.openvpn"
table <RZ>              persist file "/etc/pf_tables/pf.RZ"
table <NSAS>            persist file "/etc/pf_tables/pf.nsas"
table <NSAS-INT>        persist file "/etc/pf_tables/pf.nsas-int"
table <NSAS-VM>         { 10.192.1.0/24 }
table <ADMIN>           persist file "/etc/pf_tables/pf.admin"
table <VPN>             persist file "/etc/pf_tables/pf.vpn"
table <NET>             persist file "/etc/pf_tables/pf.net"
table <SWISSBIT>        persist file "/etc/pf_tables/pf.swissbit"

```

```

table <COMPROMISED>      persist file "/etc/pf_tables/pf.compromised"
table <FIREHOL>          persist file "/etc/pf_tables/pf.firehol"
table <shadon>           persist file "/etc/pf_tables/pf.shadon"
#####
#####
# BLOCK
#####
#####
block drop in quick log from <tor>                                label
"Block TOR"
block drop in quick log on ISP from <shadon>
label "Block SHADON"
block drop quick log from <ransom>                                label
"Block RANSOM"
block drop quick log to <ransom>                                label
"Block RANSOM"
block drop quick log to <adhosts>                                label
"Block ADWARE"
block drop in quick log on ISP from <COMPROMISED>              label
"Block COMPROMISED"
block drop in quick log on ISP from <FIREHOL>
label "Block FIREHOL"
block drop in quick log from <country>                            label
"Block COUNTRY's"
block drop in quick log from <attacker>
label "Block ATTACKER's"
block drop in log                                                label "Block
UNDEFINED"
#####
#####
match out scrub (no-df random-id reassemble tcp)
label "Normalize Traffic"
#match out all scrub (no-df random-id tcp max-mss 1500 )
label "scrub all"
#####
#####
# PASS quick
#####
#####
include "/etc/pf.conf.local"
#####
#####
# INCLUDE
#####
#####
include "/etc/pf/icmp.conf"
include "/etc/pf/ssh.conf"
include "/etc/pf/relay.conf"
include "/etc/pf/routing.conf"
#####
#####

```

```
# PASS
#####
#####
pass from { <NSAS-INT> <ADMIN> } keep state set prio (2, 5)
label "Pass from $srcaddr"
pass on CORE
label "Pass on $if"
pass on LAN
label "Pass on $if"
pass on VPN
label "Pass on $if"
#####
#####
# FIREWALL SELF
#####
#####
pass out all
label "Pass out"
#####
#####
# NAT
#####
#####
match out on ISP inet nat-to (ISP:0) label "NAT"
from $srcaddr to $dstaddr"
#####
#####
```

Test befor starting rules

```
pfctl -n -f /etc/pf.conf && pfctl -f /etc/pf.conf
```

Kill a session

```
pfctl -k ${IP}
```

Add a host to a table

```
pfctl -t TABLENAME -T add ${IP}
```

pftop

Filter examples

```
pftop -f 'host 10.192.40.4'
```

```
pftop -b -f 'proto ospf'
```

```
pftop -b -f 'host 10.192.40.4 and port 514'
```

pfsync

FW-A

[/etc/hostname.pfsync0](#)

```
up syncdev "HAINTERFACE" syncpeer "IP OF BACKUPFW" defer
```

FW-B

[/etc/hostname.pfsync0](#)

```
up syncdev "HAINTERFACE" syncpeer "IP OF PRIMARYFW" defer
```

Verify that the sync works, the count should be even on both firewalls

```
pfctl -s state | wc -l
```

Hardening

Block ransomware

[block_ransom.sh](#)

```
#!/bin/sh
curl -s
https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt
>/tmp/ransom
curl -s https://feodotracker.abuse.ch/downloads/ipblocklist.txt
>>/tmp/ransom
grep -v \# /tmp/ransom | uniq > /etc/pf_tables/pf.ransom
rm /tmp/ransom
```

[crontab](#)

```
~ * * * * /bin/sh /root/bin/block_ransom.sh ; /sbin/pfctl -t ransom -T
```

```
replace -f /etc/pf_tables/pf.ransom >/dev/null 2>&1
```

Block country

[block_country.sh](#)

```
#!/bin/sh
for c in cn il ua ru ro hk by vn il mu
do
    curl -s http://www.ipdeny.com/ipblocks/data/aggregated/${c}-
aggregated.zone
done | egrep '([[:digit:]]{1,3}\.){3}[[:digit:]]{1,3}' | uniq | sort -n
> /etc/pf_tables/pf.country
```

[crontab](#)

```
~ * * * * /bin/sh /root/bin/block_country.sh ; /sbin/pfctl -t country
-T replace -f /etc/pf_tables/pf.country >/dev/null 2>&1
```

Block TOR

[block_tor.sh](#)

```
#!/bin/sh
PATH=/root/bin:/root/scripts:/sbin:/usr/sbin:/bin:/usr/bin:/usr/X11R6/b
in:/usr/local/sbin:/usr/local/bin
curl -s https://raw.githubusercontent.com/SecOps-Institute/Tor-IP-
Addresses/master/tor-exit-nodes.lst | uniq > /etc/pf_tables/pf.tor
```

[crontab](#)

```
~ * * * * /bin/sh /root/bin/block_tor.sh ; /sbin/pfctl -t tor -T
replace -f /etc/pf_tables/pf.tor >/dev/null 2>&1
```

From:

<https://nsas.de/> - [intranet.nsas.de](https://nsas.de/)

Permanent link:

<https://nsas.de/doku.php?id=wiki:openbsd:pf&rev=1683534806>

Last update: **2023/05/08 08:33**



