

PF Firewall Rules - Protect a LAN network behind NAT

Here are pf.conf rules for protecting a LAN network behind a public IP with NAT. The firewall principle is default deny, allow only needed traffic:

RULES 1 Allow all traffic from LAN to Internet (connections initiated from LAN, stateful filtering)

```
# ----- pf.conf -----
ext_if="fxp0"
int_if="fxp1"
lan_hosts="{192.168.0.2 192.168.0.3}"

set block-policy drop
set optimization normal
set loginterface none

# normalize packets in and out, all interfaces
scrub in all
scrub out all

nat on $ext_if from { 192.168.0.1/16 } to any -> ($ext_if)

# by default block all
block in log all

# allow traffic initiated from Router to outside
pass out quick on $ext_if from ($ext_if) to any flags S/SA modulate state

# allow all traffic only for connections initiated from LAN to Internet
pass in quick on $int_if from $lan_hosts to any flags S/SA modulate state

# allow SSH traffic from Internet
pass in quick on $ext_if proto tcp from any to ($ext_if) port 22 flags S/SA modulate state

# allow traffic from Router to LAN hosts
pass out quick on $int_if from ($int_if) to $lan_hosts flags S/SA modulate state

antispoof for $ext_if
antispoof for $int_if
# ----- end pf.conf -----
```

RULES2 Allow only HTTP traffic from LAN to Internet

```
# ----- pf.conf -----
ext_if="fxp0"
int_if="fxp1"
lan_hosts="{192.168.0.2 192.168.0.3}"

set block-policy drop
set optimization normal
set loginterface none

# normalize packets in and out, all interfaces
scrub in all
scrub out all

nat on $ext_if from { 192.168.0.1/16 } to any -> ($ext_if)

# by default block all
block in log all

# allow traffic initiated from Router to outside
pass out quick on $ext_if from ($ext_if) to any flags S/SA modulate state
```

```
# allow all traffic only for connections initiated from LAN to Internet
pass in quick on $int_if proto tcp from $lan_hosts to any port 80 flags S/SA modulate state
```

```
# allow traffic from Router to LAN hosts
pass out quick on $int_if from ($int_if) to $lan_hosts flags S/SA modulate state
```

```
antispoof for $ext_if
```

```
antispoof for $int_if
```

```
# ----- end pf.conf -----
```