# Firewall Notes

Saturday, December 7, 2024 3:35 AM

**Machine A:**
Enable nftables and start the service

**systemctl enable nftables**
**systemctl start nftables**

make the changes in **/etc/sysconfig/nftables.conf**

```
#!/usr/sbin/nft -f

flush ruleset

#  Set your DMZ net here
define DMZ = 100.64.28.0/24

#  Machine A
table ip saclass {
  #  Incoming chain
  chain incoming {
    #  Default drop
    type filter hook input priority 0; policy drop;
    #  accept loopback
    iifname lo accept
    #  established connections
    ct state invalid drop
    ct state related,established accept
    #  saclass grader and proxy
    tcp dport {4113,4114} accept
    #  ping
    icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
    #  ssh from LAN, WAN, DMZ and VPN
    ip saddr {10.21.32.0/24,100.64.0.0/24,100.64.28.0/24,198.11.0.0/16} tcp dport 22 accept
    #  Incoming DHCP and NTP
    udp dport {67,123} accept
  }
  #  Outgoing chain
  chain outgoing {
    #  Default accept
    type filter hook output priority 0; policy accept;
    #  Block facebook
    ip daddr 157.240.28.35 drop
    ip daddr 57.144.104.1 drop
  }
  #  Forward chain
  chain forwarding {
    # Default drop
    type filter hook forward priority 0; policy drop;
    #  established connections
    ct state invalid drop
    ct state related,established accept
    #  interface based chains
    iifname "ens192" oifname "ens224" jump WAN2DMZ
    iifname "ens192" oifname "ens256" jump WAN2LAN
    iifname "ens224" oifname "ens192" jump DMZ2WAN
    iifname "ens224" oifname "ens256" jump DMZ2LAN
    iifname "ens256" oifname "ens192" jump LAN2WAN
    iifname "ens256" oifname "ens224" jump LAN2DMZ
  }
  #  WAN to DMZ chain
  chain WAN2DMZ {
    #  ping
    icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
    #  DNS
```

```
    udp dport 53 accept;
    #  ssh, html, grader
    tcp dport {22,80,4113} accept;
  }
  #  WAN to LAN chain
  chain WAN2LAN {
    # only return traffic
  }
  #  DMZ to WAN
  chain DMZ2WAN {
    #  ping
    icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
    #  DNS
    udp dport 53 accept;
    #  DNS, http, https
    tcp dport {53,80,443} accept;
  }
  #  DMZ to LAN
  chain DMZ2LAN {
    #  ping
    icmp type {echo-reply,destination-unreachable,echo-request,time-exceeded} accept
    #  ssh and NFS
    tcp dport {22,2049} accept;
  }
  #  LAN to DMZ
  chain LAN2DMZ {
    #  Allow everything
    ip saddr {10.21.32.0/24} accept;
  }
  #  LAN to WAN
  chain LAN2WAN {
    #  Block facebook
    ip daddr 157.240.28.35 drop
    ip daddr 57.144.104.1 drop
    #  Allow everything else
    ip saddr {10.21.32.0/24} accept;
  }
}
#  NAT LAN to WAN
table ip nat {
  chain POSTROUTING {
    type nat hook postrouting priority srcnat; policy accept;
    oifname "ens192" ip saddr 10.21.32.0/24 masquerade
  }
}
```

Reload the nftables service
**systemctl reload nftables**

**Machine B**

Enable and start the nftables service

**Systemctl enable nftables**
**Systemctl start nftables**

Make the rules in **/etc/sysconfig/nftables.conf**

```
[root@dns0 ~]# cat /etc/sysconfig/nftables.conf
# Uncomment the include statement here to load the default config sample
# in /etc/nftables for nftables service.

#include "/etc/nftables/main.nft"

# To customize, either edit the samples in /etc/nftables, append further
# commands to the end of this file or overwrite it after first service
# start by calling: 'nft list ruleset >/etc/sysconfig/nftables.conf'.

#!/usr/sbin/nft -f

flush ruleset

table ip dns0 {
    chain incoming {
        type filter hook input priority 0; policy drop;
        # Loopback
        iifname lo accept
        # Established connections
        ct state established,related accept
        # Ping and traceroute
        icmp type { echo-reply, destination-unreachable, echo-request, time-exceeded } accept
        # Grader port
        tcp dport 4113 accept
        # DNS and zone transfers
        udp dport 53 accept
        tcp dport 53 accept
        # Allow SSH from LAN, DMZ, WAN, and VPN subnets
        ip saddr {10.21.32.0/24, 100.64.0.0/24, 100.64.28.0/24, 198.11.0.0/16} tcp dport 22 accept
    }

    chain outgoing {
        #  Default accept
        type filter hook output priority 0; policy accept;
        #  Block facebook
        ip daddr 157.240.28.35 drop
        ip daddr 57.144.104.1 drop
   }
}
[root@dns0 ~]#
```

**Reload the nftables service**
**systemctl reload nftables**

**Machine F**

Start and enable the nftables service

**Systemctl enable nftables**
**Systemctl start nftables**

Make the rules in **/etc/nftables.conf**

```
root@dns1:~# cat /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table ip dns1 {
    chain incoming {
        type filter hook input priority 0; policy drop;
        # Loopback
        iifname lo accept
        # Established connections
        ct state established,related accept
        # Ping and traceroute
        icmp type { echo-reply, destination-unreachable, echo-request, time-exceeded } accept
        # Grader port
        tcp dport 4113 accept
        # DNS requests (UDP only, block TCP to prevent zone transfers)
        udp dport 53 accept
        # Allow SSH from LAN, WAN, DMZ, and VPN subnets
        ip saddr {10.21.32.0/24, 100.64.0.0/24, 100.64.28.0/24, 198.11.0.0/16} tcp dport 22 accept
    }
    chain outgoing {
        type filter hook output priority 0; policy accept;
         # Block Facebook
        ip daddr 157.240.229.35 drop
        ip daddr 57.144.104.1 drop

    }
}
root@dns1:~#
```

Reload the nftables service
**systemctl reload nftables**

**Machine C**
Enable and start the nftables service

**Systemctl enable nftables**
**Systemctl start nftables**

Make the rules in **/etc/nftables.conf**

```
root@web0:~# cat /etc/nftables.conf
#!/usr/sbin/nft -f
flush ruleset
table ip web0 {
    chain incoming {
        type filter hook input priority 0; policy drop;
        # Allow all traffic to and from the loopback interface
        iifname lo accept
        # Allow established and related connections
        ct state established,related accept
        # Allow SSH from LAN, WAN, DMZ, and VPN subnets
        ip saddr {10.21.32.0/24, 100.64.0.0/24, 100.64.28.0/24, 198.11.0.0/16} tcp dport 22 accept
        # Allow inbound ICMP traffic for ping and traceroute
        icmp type { echo-reply, destination-unreachable, echo-request, time-exceeded } accept
        # Allow incoming HTTP traffic
        tcp dport 80 accept
        # Allow inbound traffic for the grading script
        tcp dport 4113 accept
    }
    chain outgoing {
        type filter hook output priority 0; policy drop;
        # Allow outgoing DNS requests to Machines B and F
        ip daddr {100.64.28.2, 100.64.28.6} udp dport 53 accept
        # Allow established and related connections
        ct state established,related accept
        # Allow outgoing DHCP and NTP traffic to Machine A's DMZ
        ip daddr 100.64.28.1 udp dport {67, 123} accept
        # Allow outgoing NFS traffic to Machine E
        ip daddr 10.21.32.2 tcp dport 2049 accept
        # Allow SSH traffic only to the DMZ subnet
        ip daddr 100.64.28.0/24 tcp dport 22 accept
        # Block access to Facebook
        ip daddr 157.240.229.35 drop
        ip daddr 57.144.104.1 drop
        # Allow outgoing HTTP/HTTPS traffic for apt/dnf
        tcp dport {80, 443} accept
        # Allow ping to all except the LAN subnet
        ip saddr != 10.21.32.0/24 icmp type { echo-reply, destination-unreachable, echo-request, time-exceeded } accept
    }
}
```

Reload the nftables service
**systemctl reload nftables**

**Machine D**
Enable and start the nftables service
**Systemctl enable nftables**
**Systemctl start nftables**
Make the rules in **/etc/sysconfig/nftables.conf**

```
[root@web1 ~]# cat /etc/sysconfig/nftables.conf
# Uncomment the include statement here to load the default config sample
# in /etc/nftables for nftables service.

#include "/etc/nftables/main.nft"

# To customize, either edit the samples in /etc/nftables, append further
# commands to the end of this file or overwrite it after first service
# start by calling: 'nft list ruleset >/etc/sysconfig/nftables.conf'.

#!/usr/sbin/nft -f
flush ruleset
table ip web1 {
    chain incoming {
        type filter hook input priority 0; policy drop;
        # Allow all traffic to and from the loopback interface
        iifname lo accept
        # Allow established and related connections
        ct state established,related accept
        # Allow SSH from LAN, WAN, DMZ, and VPN subnets
        ip saddr {10.21.32.0/24, 100.64.0.0/24, 100.64.28.0/24, 198.11.0.0/16} tcp dport 22 accept
        # Allow inbound ICMP traffic for ping and traceroute
        icmp type { echo-reply, destination-unreachable, echo-request, time-exceeded } accept
        # Allow incoming HTTP traffic
        tcp dport 80 accept
        # Allow inbound traffic for the grading script
        tcp dport 4113 accept
    }
    chain outgoing {
        type filter hook output priority 0; policy drop;
        # Allow outgoing DNS requests to Machines B and F
        ip daddr {100.64.28.2, 100.64.28.6} udp dport 53 accept
        # Allow established and related connections
        ct state established,related accept
        # Allow outgoing DHCP and NTP traffic to Machine A's DMZ
        ip daddr 100.64.28.1 udp dport {67, 123} accept
        # Allow outgoing NFS traffic to Machine E
        ip daddr 10.21.32.2 tcp dport 2049 accept
        # Allow SSH traffic only to the DMZ subnet
        ip daddr 100.64.28.0/24 tcp dport 22 accept
        # Block access to Facebook
        ip daddr 157.240.229.35 drop
        ip daddr 57.144.104.1 drop
        # Allow outgoing HTTP/HTTPS traffic for apt/dnf
        tcp dport {80, 443} accept
        # Allow ping to all except the LAN subnet
        ip saddr != 10.21.32.0/24 icmp type { echo-reply, destination-unreachable, echo-request, time-exceeded } accept
    }
}
[root@web1 ~]#
```

Reload the nftables service
**systemctl reload nftables**

**Machine E**
Enable and start the nftables service
**Systemctl enable nftables**
**Systemctl start nftables**
Make the rules in **/etc/sysconfig/nftables.conf**

```
[root@nfs sysconfig]# cat nftables.conf
# Uncomment the include statement here to load the default config sample
# in /etc/nftables for nftables service.

#include "/etc/nftables/main.nft"

# To customize, either edit the samples in /etc/nftables, append further
# commands to the end of this file or overwrite it after first service
# start by calling: 'nft list ruleset >/etc/sysconfig/nftables.conf'.

#!/usr/sbin/nft -f

flush ruleset

table ip nfs {
    chain incoming {
        type filter hook input priority 0; policy drop;
        # Allow all traffic to/from the loopback interface
        iifname lo accept
        # Allow established and related connections
        ct state established,related accept
        # Allow inbound ICMP traffic for ping and traceroute
        icmp type { echo-reply, destination-unreachable, echo-request, time-exceeded } accept
        # Allow inbound traffic for the grading script
        tcp dport 4113 accept
        # Allow incoming NFS traffic from the DMZ
        ip saddr 100.64.28.0/24 tcp dport 2049 accept
        # Allow SSH from LAN, DMZ, WAN, and VPN subnets
        ip saddr {10.21.32.0/24, 100.64.0.0/24, 100.64.28.0/24, 198.11.0.0/16} tcp dport 22 accept
    }
    chain outgoing {
        type filter hook output priority 0; policy accept;
        # Block access to Facebook
        ip daddr 157.240.229.35 drop
        ip daddr 57.144.104.1 drop
    }
}
[root@nfs sysconfig]#
```

Reload the nftables service
**systemctl reload nftables**

**Machine X**
PF firewall on Machine X
Edit the file in **/etc/pf.conf**

```
root@bsd:~ # cat /etc/pf.conf
# Define network ranges
lan_net = "10.21.32.0/24"       # LAN network
vpn_net = "198.11.0.0/16"       # VPN network
wan_net = "100.64.0.0/24"       # WAN subnet
dmz_net = "100.64.28.0/24"       # DMZ network (includes this BSD machine)
facebook_ip = "57.144.104.1"    # One-time resolved IP for facebook.com

# ------------------------------
# Incoming Traffic Rules
# ------------------------------

# Allow all traffic on the loopback adapter
set skip on lo0

# Block all inbound traffic by default
block in all

# Allow specific inbound ICMP types for ping and traceroute
pass in inet proto icmp all icmp-type { echoreq, echorep, timex, unreach } keep state

# Allow inbound TCP traffic on port 4113 for grading script
pass in proto tcp from any to any port 4113 keep state

# Allow SSH access from LAN, VPN, DMZ, and WAN to this BSD machine
pass in proto tcp from { $lan_net, $vpn_net, $wan_net, $dmz_net } to port 22 keep state

# ------------------------------
# Outgoing Traffic Rules
# ------------------------------

# Block access to Facebook IP
# Allow all other outbound traffic
pass out all keep state
block drop out from any to $facebook_ip
root@bsd:~ #
```

Load the rules
**pfctl -f /etc/pf.conf**
Enable the service
**pfctl -e**

**In Machine C**
Add the following in auto.direct

```
root@web0:~# cat /etc/auto.direct
/var/www/html/dundermifflin/accounting -ro,soft,vers=4 10.21.32.2:/home/accounting/www
root@web0:~#
```

Reload the autofs

**Systemctl reload autofs**

**In Machine D**

Add the following in auto.direct

```
[root@web1 ~]# cat /etc/auto.direct
/var/www/html/dundermifflin/accounting -ro,soft,vers=4 10.21.32.2:/home/accounting/www
[root@web1 ~]#
```

Reload the autofs

**Systemctl reload autofs**

Verify whether the auto mounter is working in machine C and machine D

```
[root@web1 dundermifflin]# ls -al
total 52
drwxrwsr-x. 13       33 dundermifflin-group  4096 Nov 24 00:59 .
drwxr-xr-x.  5 root     root                   79 Sep 29 20:40 ..
-rw-rw----.  1 abernard dundermifflin-group    16 Oct  1 19:09 abernard-mirror
drwxr-xr-x.  2       33 dundermifflin-group    24 Sep  5  2022 about
drwxrws---.  2 root     accounting             39 Nov 19 08:06 accounting
```

**Verification**

Try ping Facebook.com in all the machines

**Machine A**

```
[root@router ~]# ping facebook.com
PING facebook.com (57.144.104.1) 56(84) bytes of data.
^C
--- facebook.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1007ms
```

**Machine B**

```
[root@dns0 ~]# ping facebook.com
PING facebook.com (57.144.104.1) 56(84) bytes of data.
^C
--- facebook.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

**Machine C**

```
[root@web1 dundermifflin]# ping facebook.com
PING facebook.com (57.144.104.1) 56(84) bytes of data.
^C
--- facebook.com ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5139ms

[root@web1 dundermifflin]#
```

**Machine D**

```
[root@web1 ~]# ping facebook.com
PING facebook.com (57.144.104.1) 56(84) bytes of data.
^C
--- facebook.com ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

[root@web1 ~]#
```

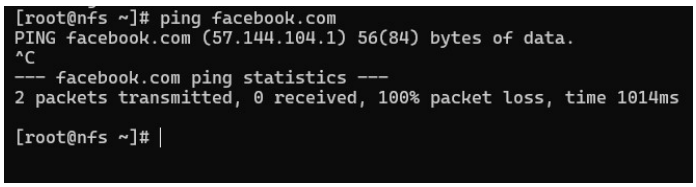
**Machine F**

```
root@dns1:~# ping facebook.com
PING facebook.com (57.144.104.1) 56(84) bytes of data.
^C
--- facebook.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1020ms
```

**Machine X**

```
root@bsd:~ # ping facebook.com
PING facebook.com (57.144.104.1): 56 data bytes
ping: sendto: Permission denied
ping: sendto: Permission denied
ping: sendto: Permission denied
^C
--- facebook.com ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
root@bsd:~ #
```

**Machine E**


[root@nfs ~]# ping facebook.com
PING facebook.com (57.144.104.1) 56(84) bytes of data.
^C
--- facebook.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1014ms
[root@nfs ~]#