

```
# NLUG Presentation - IPTables Basics
# DNI Firewalls running RedHat 8.0
#
# 2003/12/10
#
# Summary of Firewall Ruleset Contents:
# /etc/sysconfig/iptables
#

##### BEGIN FILTER TABLES #####

*filter

##### DEFINE FILTER CHAINS #####

:INPUT DROP [0:0]
:OUTPUT ACCEPT [0:0]
:FORWARD DROP [0:0]

:LOG_DROP - [0:0]
:LOG_ONLY - [0:0]

:X-State-INPUT - [0:0]
:X-Accept-INPUT - [0:0]

:X-State-OUTPUT - [0:0]
:X-Accept-OUTPUT - [0:0]

:X-Drop-FORWARD - [0:0]
:X-State-FORWARD - [0:0]
:X-Accept-FORWARD - [0:0]

:X-Accept-FORWARD-121 - [0:0]
:X-Accept-FORWARD-124 - [0:0]

##### INPUT RULESETS #####

# Call X-State-INPUT chain
-A INPUT -j X-State-INPUT
# Call X-Accept-INPUT chain
-A INPUT -j X-Accept-INPUT
# Call LOG_ONLY chain
-A INPUT -j LOG_ONLY

# Allow Incoming Packets - Established and Related Traffic
-A X-State-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Accept all traffic to local loopback interface
```

```
-A X-Accept-INPUT -i lo -j ACCEPT

# Rulesets allowing our core OSPF traffic
-A X-Accept-INPUT -p ospf -s 10.0.1.0/24 -d 224.0.0.5 -i eth1 -j ACCEPT
-A X-Accept-INPUT -p ospf -s 10.0.1.0/24 -d 224.0.0.6 -i eth1 -j ACCEPT
-A X-Accept-INPUT -p ospf -s 10.0.1.0/24 -d 10.0.1.4 -i eth1 -j ACCEPT
-A X-Accept-INPUT -p igmp -s 10.0.1.0/24 -d 224.0.0.5 -i eth1 -j ACCEPT
-A X-Accept-INPUT -p igmp -s 10.0.1.0/24 -d 224.0.0.6 -i eth1 -j ACCEPT

# Allow our NMS box access to administrative services on this firewall
# (example shows fake IP address, fake ports)
-A X-Accept-INPUT -p tcp -m tcp -m state -s 10.0.123.123 -i eth1 --dport 1234 --state NEW -j ACCEPT
-A X-Accept-INPUT -p tcp -m tcp -m state -s 10.0.123.123 -i eth1 --dport 1235 --state NEW -j ACCEPT
-A X-Accept-INPUT -p tcp -m tcp -m state -s 10.0.123.123 -i eth1 --dport 1236 --state NEW -j ACCEPT

# Allow Incoming ICMP PING request from outside to this firewall
-A X-Accept-INPUT -p icmp -m icmp -m limit -m state --icmp-type echo-request --limit 10/second --state NEW -j ACCEPT

##### OUTPUT RULESETS #####
#
# NOTE: These rulesets are irrelevant because the default
#       policy for the OUTPUT chain is ACCEPT (see above).
#
-A OUTPUT -j X-State-OUTPUT
-A OUTPUT -j X-Accept-OUTPUT

# Allow Outgoing Packets - Established and Related Traffic
-A X-State-OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Rulesets allowing our core OSPF traffic
-A X-Accept-OUTPUT -p igmp -d 224.0.0.5 -o eth1 -j ACCEPT

# Allow DNS queries from this firewall to our DNS servers
-A X-Accept-OUTPUT -p tcp -m tcp -m state -d 12.149.183.0/27 --dport 53 --state NEW -j ACCEPT

# Allow NTP queries from this firewall to our NTP servers
-A X-Accept-OUTPUT -p tcp -m tcp -m state -d 12.149.183.224/27 --dport 123 --state NEW -j ACCEPT

##### FORWARD RULESETS #####

# Call X-Drop-FORWARD
-A FORWARD -j X-Drop-FORWARD
# Call X-State-FORWARD
-A FORWARD -j X-State-FORWARD
# Call X-Accept-FORWARD
-A FORWARD -j X-Accept-FORWARD
```

```

# Call X-Accept-FORWARD-121
-A FORWARD -j X-Accept-FORWARD-121
# Call X-Accept-FORWARD-124
-A FORWARD -j X-Accept-FORWARD-124

# Log everything else
-A FORWARD -j LOG_ONLY

# Log/Drop all packets sent to our core network
# No one should need to access ANYTHING on our core network
-A X-Drop-FORWARD -m state -d 10.0.0.0/8 -i eth0 -o eth1 --state NEW -j LOG_DROP

# Allow Forwarding Packets - Established and Related Traffic
-A X-State-FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Forwarding Rulesets that apply to all hosts on this subnet
-A X-Accept-FORWARD -p udp -m udp -m state -s 12.149.183.96/27 -d 12.149.183.0/27 -i eth0 -o eth1 --dport 53 --state NEW -j ACCEPT
-A X-Accept-FORWARD -p udp -m udp -m state -s 12.149.183.96/27 -d 12.149.183.224/27 -i eth0 -o eth1 --dport 123 --state NEW -j ACCEPT
-A X-Accept-FORWARD -p udp -m udp -m state -d 12.149.183.96/27 -i eth1 -o eth0 --dport 33434:33523 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD -p icmp -m icmp -m limit -m state -d 12.149.183.96/27 -i eth1 -o eth0 --icmp-type echo-request --limit 100/second --state NEW -j
ACCEPT

# Forwarding Rulesets that apply to host 121 on this subnet
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 80 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 443 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 3864 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 25 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 110 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 21 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 3389 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 5800:5809 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -d 12.149.183.121 -i eth1 -o eth0 --dport 5900:5909 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -s 12.149.183.121 -i eth0 -o eth1 --dport 80 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -s 12.149.183.121 -i eth0 -o eth1 --dport 443 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -s 12.149.183.121 -i eth0 -o eth1 --dport 21 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-121 -p tcp -m tcp -m state -s 12.149.183.121 -i eth0 -o eth1 --dport 25 --sport 1024:65535 --state NEW -j ACCEPT

# Forwarding Rulesets that apply to host 124 on this subnet
-A X-Accept-FORWARD-124 -p tcp -m tcp -m state -d 12.149.183.123 -i eth1 -o eth0 --dport 80 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-124 -p tcp -m tcp -m state -d 12.149.183.123 -i eth1 -o eth0 --dport 21 --sport 1024:65535 --state NEW -j ACCEPT
-A X-Accept-FORWARD-124 -p tcp -m tcp -m state -s 12.149.183.0/24 -d 12.149.183.124 -i eth1 -o eth0 --dport 3389 --sport 1024:65535 --state NEW -j
ACCEPT
-A X-Accept-FORWARD-124 -p tcp -m tcp -m state -s 12.149.183.124 -d 12.149.183.0/24 -i eth0 -o eth1 --dport 8080 --sport 1024:65535 --state NEW -j
ACCEPT
-A X-Accept-FORWARD-124 -p tcp -m tcp -m state -s 12.149.183.124 -d 12.149.183.0/24 -i eth0 -o eth1 --dport 22 --sport 1024:65535 --state NEW -j
ACCEPT
-A X-Accept-FORWARD-124 -p tcp -m tcp -m state -s 12.149.183.124 -d 12.149.183.0/27 -i eth0 -o eth1 --dport 25 --sport 1024:65535 --state NEW -j
ACCEPT

```

```

# Log packet then pass packet
-A LOG_ONLY -j LOG --log-tcp-options --log-ip-options --log-prefix "[IPTABLES DROP] : "

# Log packet then drop packet
-A LOG_DROP -j LOG --log-tcp-options --log-ip-options --log-prefix "[IPTABLES DROP] : "
-A LOG_DROP -j DROP

COMMIT

##### BEGIN MANGLE TABLES #####

*mangle

##### DEFINE MANGLE CHAINS #####

:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT

##### BEGIN NAT TABLES #####

*nat

##### DEFINE NAT CHAINS #####

:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT

#####

```