Scenario 2

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.1

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:56 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 22:56
Scanning 172.16.20.1 [4 ports]
Completed Ping Scan at 22:56, 2.01s elapsed (1 total hosts)
Nmap scan report for 172.16.20.1 [host down]
NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.48 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.5

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:56 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 22:56
Scanning 172.16.20.5 [4 ports]
Completed Ping Scan at 22:56, 2.01s elapsed (1 total hosts)
Nmap scan report for 172.16.20.5 [host down]
NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.47 seconds
           Raw packets sent: 8 (304B) | Rcvd: 2 (152B)
```

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.126

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:56 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 22:56
Scanning 172.16.20.126 [1 port]
Completed ARP Ping Scan at 22:56, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:56
Completed Parallel DNS resolution of 1 host. at 22:56, 0.00s elapsed
Initiating SYN Stealth Scan at 22:56
Scanning 172.16.20.126 [1000 ports]
Completed SYN Stealth Scan at 22:56, 21.27s elapsed (1000 total ports)
Initiating Service scan at 22:56
Initiating OS detection (try #1) against 172.16.20.126
Retrying OS detection (try #2) against 172.16.20.126
NSE: Script scanning 172.16.20.126.
Initiating NSE at 22:56
Completed NSE at 22:56, 0.00s elapsed
Nmap scan report for 172.16.20.126
Host is up (0.00027s latency).
All 1000 scanned ports on 172.16.20.126 are filtered
MAC Address: 00:0C:29:97:0E:99 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.27 ms 172.16.20.126

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.37 seconds
           Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)
```

#!/bin/bash

#Flush tables and set policies to drop

```
iptables -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

#Create Logging Chain for accepted packets on INPUT CHAIN
iptables -N accept-input

#Rules for accept-input Chain
iptables -A accept-input -j LOG --log-prefix "INPUT-ACCEPTED"
iptables -A accept-input -j ACCEPT

#Create Logging Chain for dropped packets on INPUT CHAIN
iptables -N drop-input

#Rules for drop-input chain
iptables -A drop-input -j LOG --log-prefix "INPUT-DROPPED"
iptables -A drop-input -j DROP

#Create Logging Chain for accepted packets on OUTPUT CHAIN
iptables -N accept-output

#Rules for accept-output Chain
```

```
iptables -A accept-output -j LOG --log-prefix "OUTPUT-ACCEPTED"
iptables -A accept-output -j ACCEPT

#Create Logging Chain for dropped packets on OUTPUT CHAIN
iptables -N drop-output

#Rules for drop-output Chain
iptables -A drop-output -j LOG --log-prefix "OUTPUT-DROPPED"
iptables -A drop-output -j DROP

#Create Logging Chain for accepted packets on FORWARD CHAIN
iptables -N accept-forward

#Rules for accept-forward Chain
iptables -A accept-forward -j LOG --log-prefix "FORWARD-ACCEPTED"
iptables -A accept-forward -j ACCEPT

#Create Logging Chain for dropped packets on FORWARD CHAIN
iptables -N drop-forward

#Rules for drop-forward Chain
iptables -A drop-forward -j LOG --log-prefix "FORWARD-DROPPED"
iptables -A drop-forward -j DROP
```

#Create logging Chain for dropped inbound packets on DROP-INBOUND CHAIN

iptables -N drop-inbound

#Rules for drop-inbound chain

iptables -A drop-inbound -j LOG --log-prefix "DROPPED-INBOUND"

iptables -A drop-inbound -j DROP

#SSH/SCP to Router

iptables -A INPUT -p tcp -s 172.16.20.64/26 --dport 3535 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p tcp -d 172.16.20.64/26 --sport 3535 -m state --state ESTABLISHED,RELATED -j accept-output

#SSH/SCP to Server

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5353 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5353 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL IMAP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 143 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 143 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL SMTP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 25 -m state --state ESTABLISHED,RELATED -j accept-forward

#FTP UNENCRYPTED

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 21 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 20 -m state --state ESTABLISHED,RELATED -j accept-forward

#MySQL

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 3306 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 3306 -m state --state ESTABLISHED,RELATED -j accept-forward

#DNS

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -s 172.16.20.64/26 --dport 53 -m state --state

NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

#DHCP

iptables -A INPUT -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p udp --sport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-output

iptables -A FORWARD -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp --sport 67:68 -m state --state ESTABLISHED,RELATED -j accept-forward

#Allow Apache

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5151 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5151 -m state --state ESTABLISHED,RELATED -j accept-forward

#Allow IIS

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 1515 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 1515 -m state --state ESTABLISHED,RELATED -j accept-forward

```
#Allow Traceroute
#iptables -A INPUT -p icmp -j accept-input
#iptables -A INPUT -p udp --dport 33434:33474 -j accept-input
iptables -A FORWARD -p icmp   -j drop-inbound
iptables -A FORWARD -p udp --dport 33343:33474 -j drop-inbound
#iptables -A OUTPUT -p icmp -j accept-output
#iptables -A OUTPUT -p udp --dport 33434:33474 -j accept-output

#INPUT CHAIN RULES
iptables -A INPUT -j drop-input

#OUTPUT CHAIN RULES
iptables -A OUTPUT -j drop-output

#FORWARD CHAIN RULES
iptables -A FORWARD -j drop-forward

iptables -L -n
```

Scenario 3

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.1

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:58 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 22:58
Scanning 172.16.20.1 [4 ports]
Completed Ping Scan at 22:58, 2.01s elapsed (1 total hosts)
Nmap scan report for 172.16.20.1 [host down]
NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.47 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.5

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:58 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 22:58
Scanning 172.16.20.5 [4 ports]
Completed Ping Scan at 22:58, 2.01s elapsed (1 total hosts)
Nmap scan report for 172.16.20.5 [host down]
NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.47 seconds
           Raw packets sent: 8 (304B) | Rcvd: 2 (150B)
```

,

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.126

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:58 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 22:58
Scanning 172.16.20.126 [1 port]
Completed ARP Ping Scan at 22:58, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:58
Completed Parallel DNS resolution of 1 host. at 22:58, 0.00s elapsed
Initiating SYN Stealth Scan at 22:58
Scanning 172.16.20.126 [1000 ports]
Completed SYN Stealth Scan at 22:58, 21.27s elapsed (1000 total ports)
Initiating Service scan at 22:58
Initiating OS detection (try #1) against 172.16.20.126
Retrying OS detection (try #2) against 172.16.20.126
NSE: Script scanning 172.16.20.126.
Initiating NSE at 22:58
Completed NSE at 22:58, 0.00s elapsed
Nmap scan report for 172.16.20.126
Host is up (0.00033s latency).
All 1000 scanned ports on 172.16.20.126 are filtered
MAC Address: 00:0C:29:97:0E:99 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.33 ms 172.16.20.126

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.36 seconds
           Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)
```

!/bin/bash

```
#Flush tables and set policies to drop
iptables -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

#Create Logging Chain for accepted packets on INPUT CHAIN
iptables -N accept-input

#Rules for accept-input Chain
iptables -A accept-input -j LOG --log-prefix "INPUT-ACCEPTED"
iptables -A accept-input -j ACCEPT

#Create Logging Chain for dropped packets on INPUT CHAIN
iptables -N drop-input

#Rules for drop-input chain
iptables -A drop-input -j LOG --log-prefix "INPUT-DROPPED"
iptables -A drop-input -j DROP

#Create Logging Chain for accepted packets on OUTPUT CHAIN
iptables -N accept-output
```

```
#Rules for accept-output Chain
iptables -A accept-output -j LOG --log-prefix "OUTPUT-ACCEPTED"
iptables -A accept-output -j ACCEPT

#Create Logging Chain for dropped packets on OUTPUT CHAIN
iptables -N drop-output

#Rules for drop-output Chain
iptables -A drop-output -j LOG --log-prefix "OUTPUT-DROPPED"
iptables -A drop-output -j DROP

#Create Logging Chain for accepted packets on FORWARD CHAIN
iptables -N accept-forward

#Rules for accept-forward Chain
iptables -A accept-forward -j LOG --log-prefix "FORWARD-ACCEPTED"
iptables -A accept-forward -j ACCEPT

#Create Logging Chain for dropped packets on FORWARD CHAIN
iptables -N drop-forward

#Rules for drop-forward Chain
iptables -A drop-forward -j LOG --log-prefix "FORWARD-DROPPED"
iptables -A drop-forward -j DROP
```

#Create logging Chain for dropped inbound packets on DROP-INBOUND CHAIN

iptables -N drop-inbound

#Rules for drop-inbound chain

iptables -A drop-inbound -j LOG --log-prefix "DROPPED-INBOUND"

iptables -A drop-inbound -j DROP

#SSH/SCP to Router

iptables -A INPUT -p tcp -s 172.16.20.64/26 --dport 3535 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p tcp -d 172.16.20.64/26 --sport 3535 -m state --state ESTABLISHED,RELATED -j accept-output

#SSH/SCP to Server

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5353 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5353 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL IMAP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 143 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 143 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL SMTP

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 25 -m state --state ESTABLISHED,RELATED -j accept-forward

#FTP UNENCRYPTED

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 21 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 20 -m state --state ESTABLISHED,RELATED -j accept-forward

#MySQL

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 3306 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 3306 -m state --state ESTABLISHED,RELATED -j accept-forward

#DNS

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -s 172.16.20.64/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

#DHCP

iptables -A INPUT -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p udp --sport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-output

iptables -A FORWARD -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp --sport 67:68 -m state --state ESTABLISHED,RELATED -j accept-forward

#Allow Apache

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5151 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5151 -m state --state ESTABLISHED,RELATED -j accept-forward

#Allow IIS

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 1515 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

#iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 1515 -m state --state ESTABLISHED,RELATED -j accept-forward

```
#Allow Traceroute
#iptables -A INPUT -p icmp -j accept-input
#iptables -A INPUT -p udp --dport 33434:33474 -j accept-input
iptables -A FORWARD -p icmp   -j drop-inbound
iptables -A FORWARD -p udp --dport 33343:33474 -j drop-inbound
#iptables -A OUTPUT -p icmp -j accept-output
#iptables -A OUTPUT -p udp --dport 33434:33474 -j accept-output

#INPUT CHAIN RULES
iptables -A INPUT -j drop-input

#OUTPUT CHAIN RULES
iptables -A OUTPUT -j drop-output

#FORWARD CHAIN RULES
iptables -A FORWARD -j drop-forward

iptables -L -n
```

Scenario 4

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.1

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:59 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 22:59
Scanning 172.16.20.1 [4 ports]
Completed Ping Scan at 22:59, 2.01s elapsed (1 total hosts)
Nmap scan report for 172.16.20.1 [host down]
NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.48 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.5

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 22:59 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 22:59
Scanning 172.16.20.5 [4 ports]
Completed Ping Scan at 22:59, 2.01s elapsed (1 total hosts)
Nmap scan report for 172.16.20.5 [host down]
NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.49 seconds
           Raw packets sent: 8 (304B) | Rcvd: 0 (0B)
```

```
[root@localhost ~]# nmap -T4 -A -v 172.16.20.126

Starting Nmap 6.40 ( http://nmap.org ) at 2020-03-15 23:00 EDT
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 23:00
Scanning 172.16.20.126 [1 port]
Completed ARP Ping Scan at 23:00, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:00
Completed Parallel DNS resolution of 1 host. at 23:00, 0.00s elapsed
Initiating SYN Stealth Scan at 23:00
Scanning 172.16.20.126 [1000 ports]
Completed SYN Stealth Scan at 23:00, 21.27s elapsed (1000 total ports)
Initiating Service scan at 23:00
Initiating OS detection (try #1) against 172.16.20.126
Retrying OS detection (try #2) against 172.16.20.126
NSE: Script scanning 172.16.20.126.
Initiating NSE at 23:00
Completed NSE at 23:00, 0.00s elapsed
Nmap scan report for 172.16.20.126
Host is up (0.00031s latency).
All 1000 scanned ports on 172.16.20.126 are filtered
MAC Address: 00:0C:29:97:0E:99 (VMware)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.31 ms 172.16.20.126

NSE: Script Post-scanning.
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.44 seconds
           Raw packets sent: 2049 (94.700KB) | Rcvd: 1 (28B)
```

#!/bin/bash

#Flush tables and set policies to drop

```
iptables -F
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
iptables -t nat -A POSTROUTING -o ens33 -j MASQUERADE

#Create Logging Chain for accepted packets on INPUT CHAIN
iptables -N accept-input

#Rules for accept-input Chain
iptables -A accept-input -j LOG --log-prefix "INPUT-ACCEPTED"
iptables -A accept-input -j ACCEPT

#Create Logging Chain for dropped packets on INPUT CHAIN
iptables -N drop-input

#Rules for drop-input chain
iptables -A drop-input -j LOG --log-prefix "INPUT-DROPPED"
iptables -A drop-input -j DROP

#Create Logging Chain for accepted packets on OUTPUT CHAIN
iptables -N accept-output

#Rules for accept-output Chain
```

```
iptables -A accept-output -j LOG --log-prefix "OUTPUT-ACCEPTED"
iptables -A accept-output -j ACCEPT

#Create Logging Chain for dropped packets on OUTPUT CHAIN
iptables -N drop-output

#Rules for drop-output Chain
iptables -A drop-output -j LOG --log-prefix "OUTPUT-DROPPED"
iptables -A drop-output -j DROP

#Create Logging Chain for accepted packets on FORWARD CHAIN
iptables -N accept-forward

#Rules for accept-forward Chain
iptables -A accept-forward -j LOG --log-prefix "FORWARD-ACCEPTED"
iptables -A accept-forward -j ACCEPT

#Create Logging Chain for dropped packets on FORWARD CHAIN
iptables -N drop-forward

#Rules for drop-forward Chain
iptables -A drop-forward -j LOG --log-prefix "FORWARD-DROPPED"
iptables -A drop-forward -j DROP
```

#Create Logging Chain for dropped inbound packets on DROP-OUTBOUND CHAIN

iptables -N drop-outbound

#Rules for drop-outbound chain

iptables -A drop-outbound -j LOG --log-prefix "DROPPED-OUTBOUND"

iptables -A drop-outbound -j DROP

#SSH/SCP to Router

iptables -A INPUT -p tcp -s 172.16.20.64/26 --dport 3535 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p tcp -d 172.16.20.64/26 --sport 3535 -m state --state ESTABLISHED,RELATED -j accept-output

#SSH/SCP to Server

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5353 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5353 -m state --state ESTABLISHED,RELATED -j accept-forward

#HMAIL IMAP

#iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 143 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 143 -m state --state ESTABLISHED,RELATED -j drop-outbound

#HMAIL SMTP

#iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 25 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 25 -m state --state ESTABLISHED,RELATED -j drop-outbound

#FTP UNENCRYPTED

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 21 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 21 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 20 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 20 -m state --state ESTABLISHED,RELATED -j accept-forward

#MySQL

#iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 3306 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 3306 -m state --state ESTABLISHED,RELATED -j drop-outbound

#DNS

iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 53 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -s 172.16.20.64/26 --dport 53 -m state --state

NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp -d 172.16.20.64/26 --sport 53 -m state --state ESTABLISHED,RELATED -j accept-forward

#DHCP

iptables -A INPUT -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-input

iptables -A OUTPUT -p udp --sport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-output

iptables -A FORWARD -p udp --dport 67:68 -m state --state NEW,ESTABLISHED,RELATED -j accept-forward

iptables -A FORWARD -p udp --sport 67:68 -m state --state ESTABLISHED,RELATED -j accept-forward

#Allow Apache

#iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 5151 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 5151 -m state --state ESTABLISHED,RELATED -j drop-outbound

#Allow IIS

#iptables -A FORWARD -p tcp -s 172.16.20.64/26 --dport 1515 -m state --state NEW,ESTABLISHED,RELATED -j drop-inbound

iptables -A FORWARD -p tcp -d 172.16.20.64/26 --sport 1515 -m state --state ESTABLISHED,RELATED -j drop-outbound

#Allow Traceroute

#iptables -A INPUT -p icmp -j accept-input

#iptables -A INPUT -p udp --dport 33434:33474 -j accept-input

iptables -A FORWARD -p icmp -j drop-outbound

iptables -A FORWARD -p udp --dport 33343:33474 -j drop-outbound

#iptables -A OUTPUT -p icmp -j accept-output

#iptables -A OUTPUT -p udp --dport 33434:33474 -j accept-output

#INPUT CHAIN RULES

iptables -A INPUT -j drop-input

#OUTPUT CHAIN RULES

iptables -A OUTPUT -j drop-output

#FORWARD CHAIN RULES

iptables -A FORWARD -j drop-forward

iptables -L -n

Logging

Cat /var/log/messages

A DROPPED APACHE request from you Client

```
[root@router ipch4]# cat /var/log/messages | grep "DROPPED" | grep "SRC=172.16.20.70" | grep "DPT=5151"
Mar 15 21:51:40 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=30677 DF PROTO=TCP SPT=53498
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:40 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=12819 DF PROTO=TCP SPT=53500
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:41 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=30678 DF PROTO=TCP SPT=53498
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:41 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=12820 DF PROTO=TCP SPT=53500
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:43 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=30679 DF PROTO=TCP SPT=53498
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:43 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=12821 DF PROTO=TCP SPT=53500
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:47 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=30680 DF PROTO=TCP SPT=53498
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:47 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=12822 DF PROTO=TCP SPT=53500
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:55 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=30681 DF PROTO=TCP SPT=53498
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:55 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=12823 DF PROTO=TCP SPT=53500
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:52:11 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=30682 DF PROTO=TCP SPT=53498
 DPT=5151 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:52:11 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=12824 DF PROTO=TCP SPT=53500
```

A DROPPED APACHE response from your Linux Server

A DROPPED SSH request to your LINUX Server

```
[root@router ipch4]# cat /var/log/messages | grep "DROPPED" | grep "SRC=172.16.20.70" | grep "DPT=5353"
Mar 15 21:51:47 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=101 TOS=0x00 PREC=0xC0 TTL=63 ID=18821 PROTO=ICMP TYPE=3 COD
E=3 [SRC=172.16.20.5 DST=172.16.20.70 LEN=73 TOS=0x00 PREC=0x00 TTL=127 ID=29054 DF PROTO=UDP SPT=53 DPT
=53536 LEN=53 ]
Mar 15 21:51:47 router kernel: DROPPED-INBOUNDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=101 TOS=0x00 PREC=0xC0 TTL=63 ID=18822 PROTO=ICMP TYPE=3 COD
E=3 [SRC=172.16.20.5 DST=172.16.20.70 LEN=73 TOS=0x00 PREC=0x00 TTL=127 ID=29056 DF PROTO=UDP SPT=53 DPT
=53536 LEN=53 ]
Mar 15 22:16:17 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48200 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:17 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48201 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:17 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48202 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:17 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48203 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:18 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48204 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:20 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48205 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:23 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48206 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:30 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48207 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:16:44 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=96 TOS=0x10 PREC=0x00 TTL=63 ID=48208 DF PROTO=TCP SPT=34788
 DPT=5353 WINDOW=291 RES=0x00 ACK PSH URGP=0
Mar 15 22:17:08 router kernel: FORWARD-DROPPEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17
:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=18618 DF PROTO=TCP SPT=34790
```

-

A DROPPED IMAP response from your Windows Server

AN ACCEPTED MYSQL request from your Client

```
[root@router ipch4]# cat /var/log/messages | grep "ACCEPTED" | grep "DPT=3306"
Mar 15 21:51:52 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=9339 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 21:51:52 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=9340 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=229 RES=0x00 ACK URGP=0
Mar 15 21:52:02 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=9341 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=229 RES=0x00 ACK URGP=0
Mar 15 21:52:02 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=119 TOS=0x00 PREC=0x00 TTL=63 ID=9342 DF PROTO=TCP SPT=5812
2 DPT=3306 WINDOW=229 RES=0x00 ACK PSH URGP=0
Mar 15 21:52:02 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=76 TOS=0x00 PREC=0x00 TTL=63 ID=9343 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=229 RES=0x00 ACK PSH URGP=0
Mar 15 21:52:02 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=89 TOS=0x00 PREC=0x00 TTL=63 ID=9344 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=229 RES=0x00 ACK PSH URGP=0
Mar 15 21:52:02 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=9345 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=229 RES=0x00 ACK URGP=0
Mar 15 21:52:21 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=57 TOS=0x00 PREC=0x00 TTL=63 ID=9346 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=229 RES=0x00 ACK PSH URGP=0
Mar 15 21:52:21 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=9347 DF PROTO=TCP SPT=58122
 DPT=3306 WINDOW=229 RES=0x00 ACK FIN URGP=0
Mar 15 21:52:21 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens36 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.1 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=9348 DF PROTO=TCP SPT=58122
```

AN ACCEPTED SSH request to your router

```
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=88 TOS=0x10 PREC=0x00 TTL=64 ID=34418 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3601 RES=0x00 ACK PSH URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34419 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3480 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34420 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3571 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34421 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3480 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34422 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3366 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34423 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3253 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34424 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3018 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34425 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=3102 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34426 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=2988 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34427 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=2996 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34428 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=2829 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34429 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=4124 RES=0x00 ACK URGP=0
Mar 15 22:30:04 router kernel: INPUT-ACCEPTEDIN=ens37 OUT= MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:17:08:00
 SRC=172.16.20.70 DST=172.16.20.126 LEN=52 TOS=0x10 PREC=0x00 TTL=64 ID=34430 DF PROTO=TCP SPT=50764 DPT
=3535 WINDOW=4381 RES=0x00 ACK URGP=0
[root@router ipch4]# cat /var/log/messages | grep "ACCEPTED" | grep "DPT=3535" | grep "SRC=172.16.20.70"
```

AN ACCEPTED FTP response from your Windows Server (Port 20)

```
[root@router ipch4]# cat /var/log/messages | grep "ACCEPTED" | grep "DPT=21" | grep "SRC=172.16.20.70"
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=61659 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=29200 RES=0x00 SYN URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=61660 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=229 RES=0x00 ACK URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=61661 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=64 TOS=0x00 PREC=0x00 TTL=63 ID=61662 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=61663 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=68 TOS=0x00 PREC=0x00 TTL=63 ID=61664 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=58 TOS=0x00 PREC=0x00 TTL=63 ID=61665 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=58 TOS=0x00 PREC=0x00 TTL=63 ID=61666 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=57 TOS=0x00 PREC=0x00 TTL=63 ID=61667 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=61668 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=58 TOS=0x00 PREC=0x00 TTL=63 ID=61669 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=58 TOS=0x00 PREC=0x00 TTL=63 ID=61670 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK PSH URGP=0
Mar 15 22:39:27 router kernel: FORWARD-ACCEPTEDIN=ens37 OUT=ens38 MAC=00:0c:29:97:0e:99:00:0c:29:cd:9b:1
7:08:00 SRC=172.16.20.70 DST=172.16.20.5 LEN=52 TOS=0x00 PREC=0x00 TTL=63 ID=61671 DF PROTO=TCP SPT=3704
0 DPT=21 WINDOW=237 RES=0x00 ACK URGP=0
```