

Gaurav Chaudhari

240840127033

1. Write firewall rules for the configuration described below using pfSense or any other firewall:

Allow ICMP traffic for all LAN IPs

```
[root@localhost dhpcsa]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client dns http https squid ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@localhost dhpcsa]# firewall-cmd --zone=internal --add-rich-rule='rule protocol value="icmp" accept' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --reload
success
```

```
[root@localhost dhpcsa]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client dns http https squid ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
    rule protocol value="icmp" accept
    rule family="ipv4" service name="http" accept
[root@localhost dhpcsa]#
```

Enable web browsing only from LAN IPs to WAN IPs using the NAT option

```
[root@localhost dhpcsa]# firewall-cmd --zone=internal --add-rich-rule='rule family="ipv4" masquerade' --permanent
Warning: ALREADY_ENABLED: rule family="ipv4" masquerade
success
[root@localhost dhpcsa]# firewall-cmd --zone=internal --add-rich-rule='rule family="ipv4" service name="http" accept' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --zone=internal --add-rich-rule='rule family="ipv4" service name="https" accept' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --reload
success
```

```
[root@localhost dhpcsa]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" masquerade' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="http" accept' --permanent
Warning: ALREADY_ENABLED: rule family="ipv4" service name="http" accept
success
[root@localhost dhpcsa]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" service name="https" accept' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --reload
success
[root@localhost dhpcsa]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client dns http https squid ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
    rule family="ipv4" service name="https" accept
    rule protocol value="icmp" accept
    rule family="ipv4" service name="http" accept
    rule family="ipv4" masquerade
```

Configure a dmz and forward all incoming traffic on WAN IP port on 443 to a specific local LAN IP

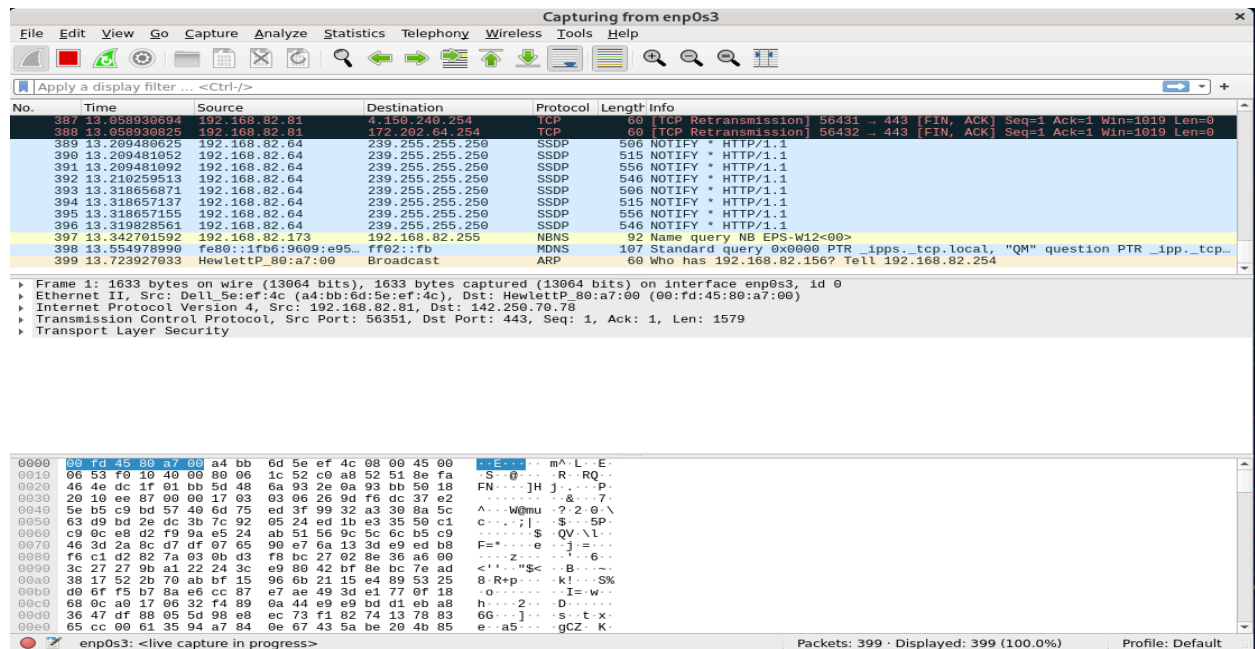
```
[root@localhost dhpcsa]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" forward-port port="443" protocol="tcp" to-addr="192.168.82.97" to-port="443"' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --zone=dmz --add-rich-rule='rule family="ipv4" service name="https" accept' --permanent
success
[root@localhost dhpcsa]# firewall-cmd --reload
success
[root@localhost dhpcsa]# firewall-cmd --list-all
public (active)
target: default
icmp-block-inversion: no
interfaces: enp0s3
sources:
services: cockpit dhcpv6-client dns http https squid ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
    rule protocol value="icmp" accept
    rule family="ipv4" service name="https" accept
    rule family="ipv4" forward-port port="443" protocol="tcp" to-port="443" to-addr="192.168.82.97"
    rule family="ipv4" service name="http" accept
    rule family="ipv4" masquerade
[root@localhost dhpcsa]#
```

All rules set successfully

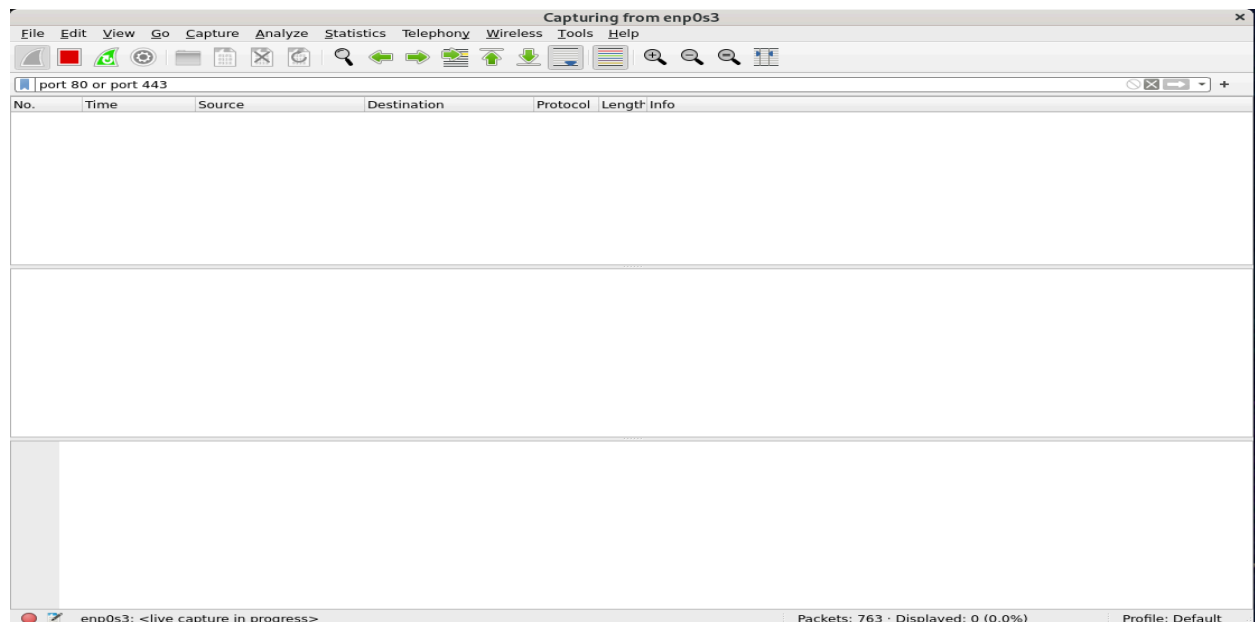
```
[root@localhost dhpcsa]# firewall-cmd --list-rich-rules
rule protocol value="icmp" accept
rule family="ipv4" service name="https" accept
rule family="ipv4" forward-port port="443" protocol="tcp" to-port="443" to-addr="192.168.82.97"
rule family="ipv4" service name="http" accept
rule family="ipv4" masquerade
[root@localhost dhpcsa]#
```

3. Configure Wireshark to capture traffic on port 80 and simulate a web browser request to capture the data of the page being browsed by the user

Install wireshark and start the wireshark using sudo or root permission



Filter port on 80 or port 443

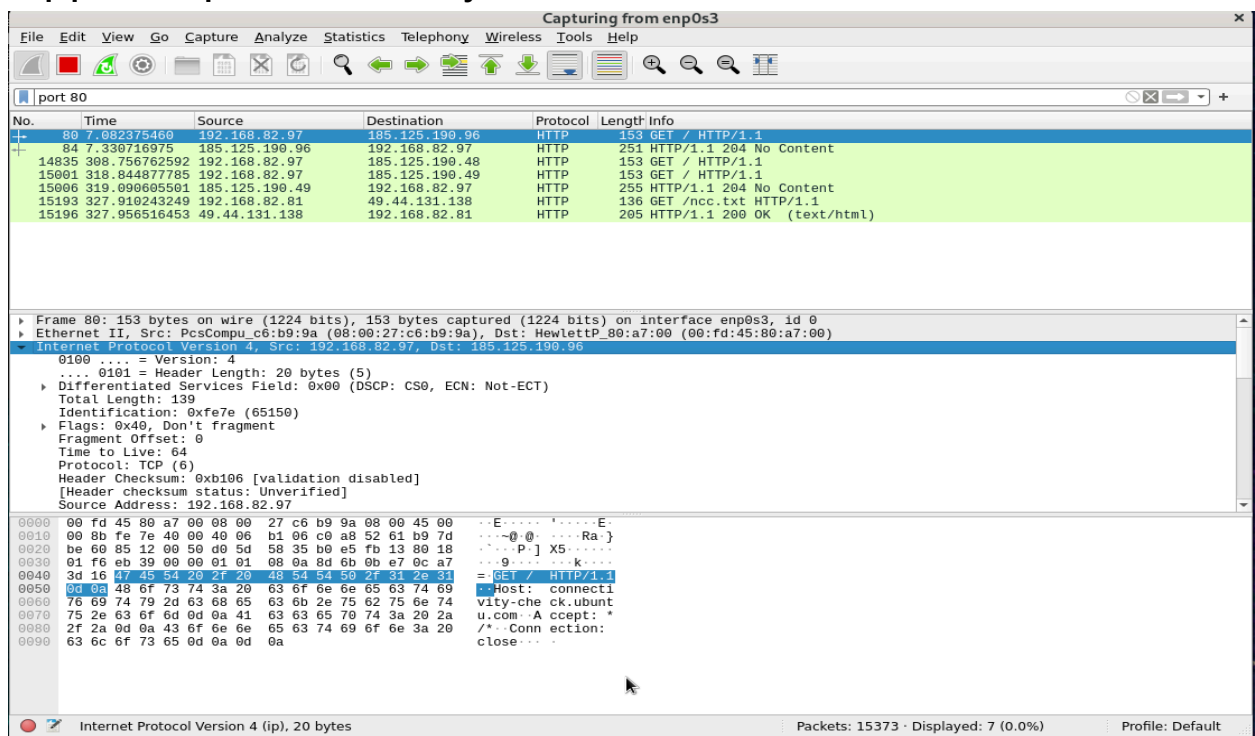


Web page hosted on server open from client machine or user machine



Hpcsa main server

Http packet captured successfully



Also using ip address and port to see the traffic on http port

Wireshark capture of HTTP traffic on interface enp0s3. The filter is `ip.addr == 192.168.82.97 && http`. The packet list shows four packets: three GET requests and one 204 No Content response. The packet details for packet 986 show the Hypertext Transfer Protocol section.

No.	Time	Source	Destination	Protocol	Length	Info
888	48.691904366	192.168.82.97	192.168.82.14	HTTP	143	GET / HTTP/1.1
890	48.70266761	192.168.82.14	192.168.82.97	HTTP	331	HTTP/1.1 200 OK (text/html)
986	57.883292555	192.168.82.97	185.125.190.98	HTTP	153	GET / HTTP/1.1
989	58.151921866	185.125.190.98	192.168.82.97	HTTP	251	HTTP/1.1 204 No Content

Frame 986: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_c6:b9:9a (08:00:27:c6:b9:9a), Dst: HewlettP_80:a7:00 (00:fd:45:80:a7:00)
Internet Protocol Version 4, Src: 192.168.82.97, Dst: 185.125.190.98
Transmission Control Protocol, Src Port: 35688, Dst Port: 80, Seq: 1, Ack: 1, Len: 87
Hypertext Transfer Protocol

0000 00 fd 45 80 a7 00 08 00 27 c6 b9 9a 08 00 45 00 ..E.....E.
0010 00 8b f4 a4 40 00 40 06 ba de c0 a8 52 61 b9 7d ...@.....Ra.
0020 be 62 8b 68 00 50 c9 3f a5 c6 7e e5 fe 7b 80 18 ...b.h.P?....
0030 01 f6 28 ff 00 00 01 01 08 9a 2b 3a 75 fa 0c ab+;u..
0040 0d 37 47 45 54 20 2f 20 48 54 50 2f 31 2e 31 ..7GET / HTTP/1.1
0050 0d 9a 48 6f 73 74 3a 20 63 6f 6e 6e 63 74 69 ..Host: connecti
0060 76 69 74 79 2d 63 68 65 63 6b 2e 75 62 75 6e 74 vity-che ck.ubunt
0070 75 2e 63 6f 6d 0d 0a 41 63 65 70 74 3a 20 2a u.com-A ccept: *
0080 2f 2a 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 /*. Conn ction:
0090 63 6c 6f 73 65 0d 0a 0d 0a close..

Hypertext Transfer Protocol: Protocol Packets: 1628 · Displayed: 4 (0.2%) Profile: Default

Wireshark capture of traffic on interface enp0s3. The filter is `ip.addr == 192.168.82.97 && port 80`. The packet list shows various traffic including DNS queries, TCP SYN/ACK, and HTTP requests. The packet details for packet 21741 show the Internet Protocol Version 4 section.

No.	Time	Source	Destination	Protocol	Length	Info
75	7.079888624	192.168.82.97	192.168.72.20	DNS	100	Standard query 0xb8ce A connectivity-check.ubuntu.com OPT
76	7.080436862	192.168.72.20	192.168.82.97	DNS	292	Standard query response 0xb8ce A connectivity-check.ubuntu.com A 185.12...
77	7.081203643	192.168.82.97	185.125.190.96	TCP	74	34066 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=23726...
78	7.081740892	185.125.190.96	192.168.82.97	TCP	74	80 → 34066 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 ...
79	7.081973209	192.168.82.97	185.125.190.96	TCP	66	34066 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2372602855 TSecr=212...
80	7.082375460	192.168.82.97	185.125.190.96	HTTP	153	GET / HTTP/1.1
81	7.082782548	185.125.190.96	192.168.82.97	TCP	66	80 → 34066 [ACK] Seq=1 Ack=88 Win=14592 Len=0 TSval=212286742 TSecr=237...
84	7.330716975	185.125.190.96	192.168.82.97	HTTP	251	HTTP/1.1 204 No Content
85	7.330717241	185.125.190.96	192.168.82.97	TCP	66	80 → 34066 [FIN, ACK] Seq=186 Ack=88 Win=14592 Len=0 TSval=212286767 TS...
86	7.331009950	192.168.82.97	185.125.190.96	TCP	66	34066 → 80 [ACK] Seq=88 Ack=186 Win=64128 Len=0 TSval=2372603104 TSecr=...
87	7.331424848	192.168.82.97	185.125.190.96	TCP	66	34066 → 80 [FIN, ACK] Seq=88 Ack=187 Win=64128 Len=0 TSval=2372603104 T...
88	7.331701975	185.125.190.96	192.168.82.97	TCP	66	80 → 34066 [ACK] Seq=187 Ack=89 Win=14592 Len=0 TSval=212286767 TSecr=2...
99	9.769610514	192.168.82.97	192.168.72.20	DNS	85	Standard query 0x1a25 A www.google.com OPT
100	9.769610788	192.168.82.97	192.168.72.20	DNS	85	Standard query 0x9255 AAAA www.google.com OPT

Frame 21741: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface enp0s3, id 0
Ethernet II, Src: Dell_5e:ef:4c (a4:bb:6d:5e:ef:4c), Dst: PcsCompu_c6:b9:9a (08:00:27:c6:b9:9a)
Internet Protocol Version 4, Src: 192.168.82.81, Dst: 192.168.82.97
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x0497 (1175)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0xd001 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.82.81

0000 08 00 27 c6 b9 9a a4 bb 6d 5e ef 4c 08 00 45 00 ...m^..L..E.
0010 00 5c 04 97 40 00 80 06 d0 01 c0 a8 52 51 c0 a8 ..\..@.....RQ..
0020 52 61 db a5 00 16 03 fc 4c a4 ff 6b 40 e3 50 18 Ra.....L..kQ P..
0030 0a 02 82 50 00 00 00 00 00 20 31 ef b9 fd 22 dd ...P.....
0040 9a ec cb 7d 46 28 d1 19 db 2d a7 13 6b a4 e5 a0 ...F.....k...
0050 5d 20 4c 19 c1 74 ef c3 7b f1 52 c8 d6 a6 3f a9 j L..t...(.R...?
0060 81 b9 e3 3d 88 97 61 60 08 12a.....

"80" was unexpected in this context. Packets: 22332 · Displayed: 1124 (5.0%) Profile: Default