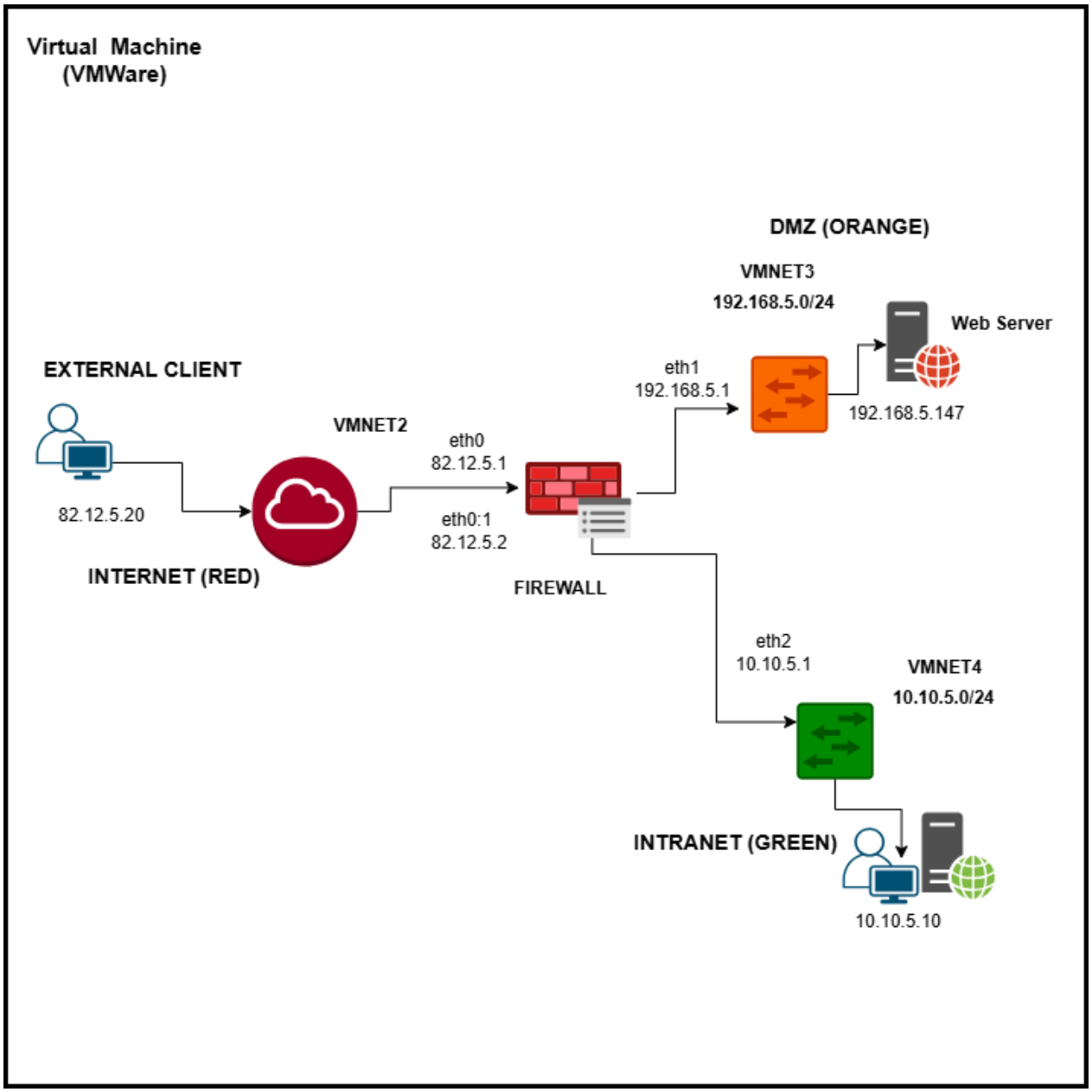
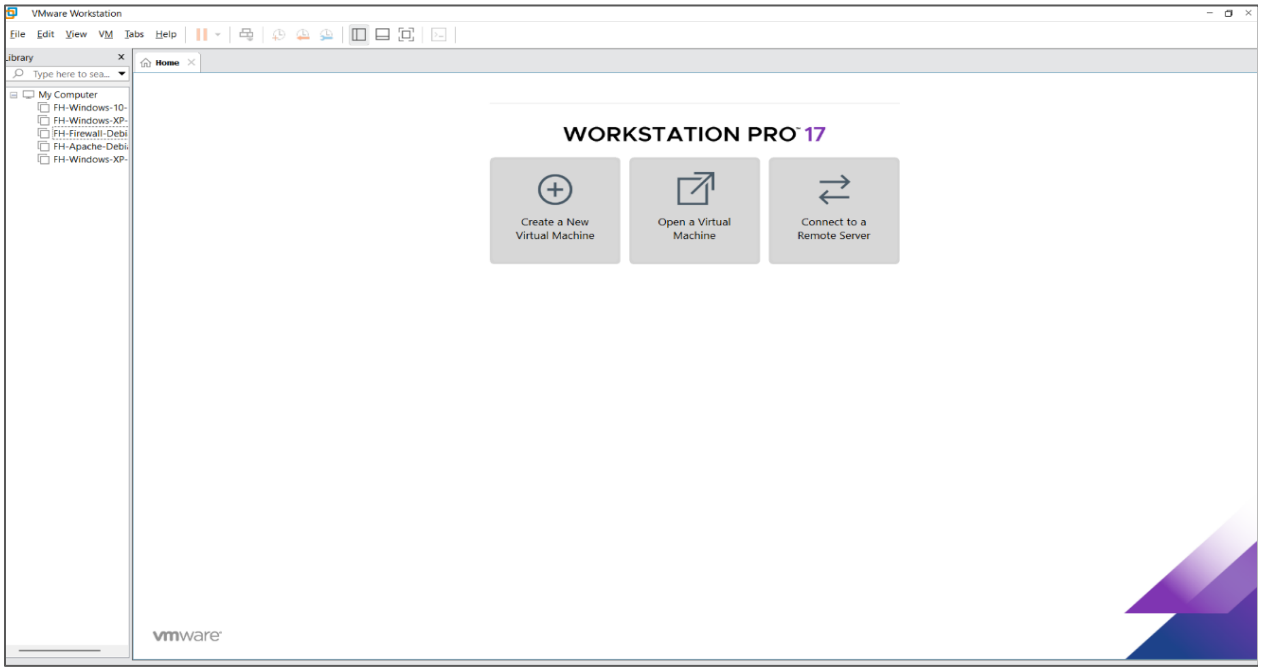
IT-Network Planning Network

Basics, Corporate Network with NAT and DMZ

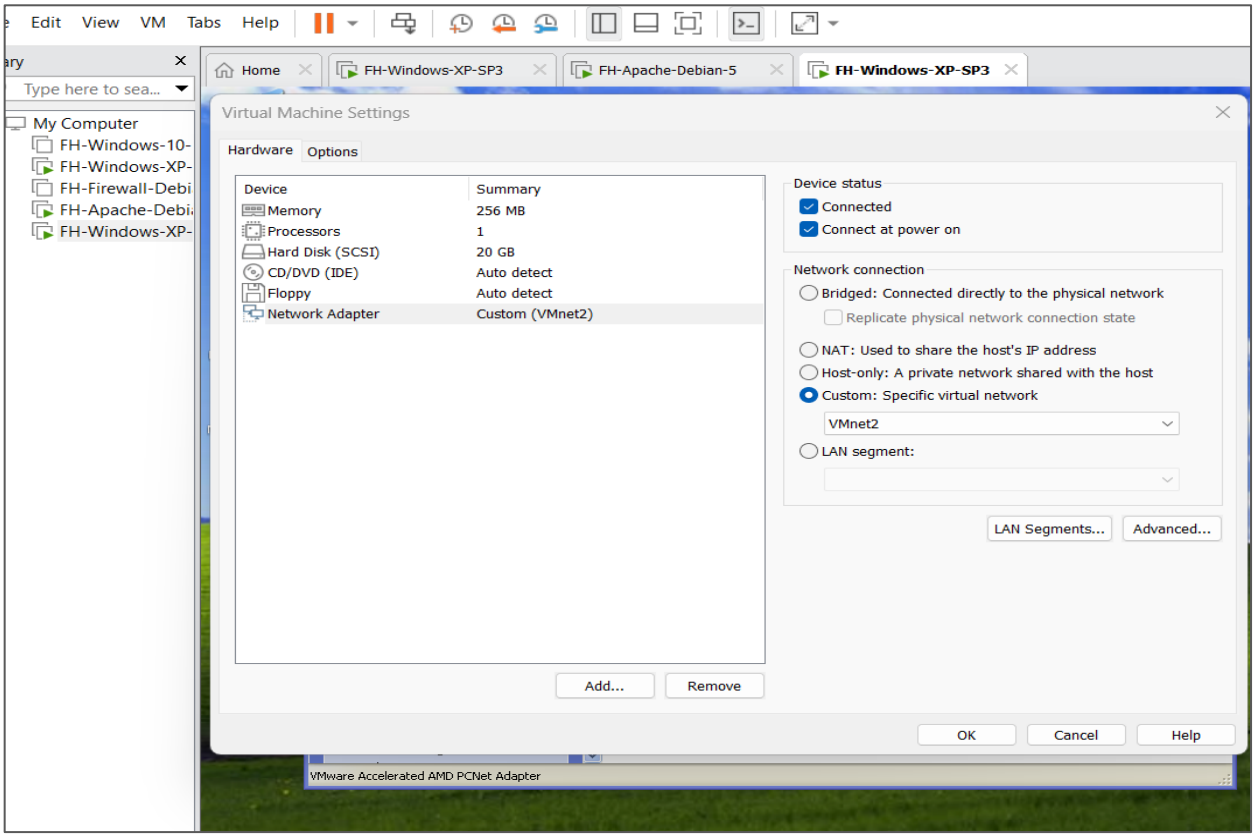


1. VMware Installation: Install VMware Workstation/Player.



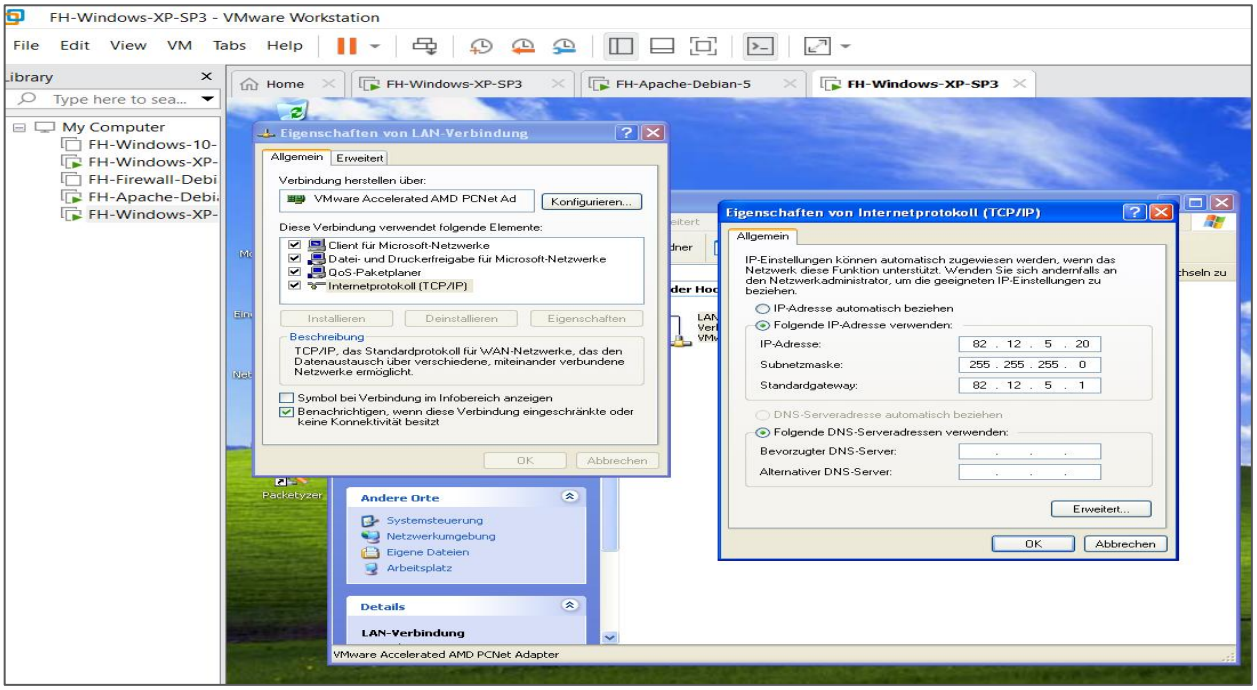
2. Network Configuration:

a) Create **VMnet2** ((External - Network/RED (FH-Windows-IT-Security Windows-XP-External: 82.12.5.20/24)

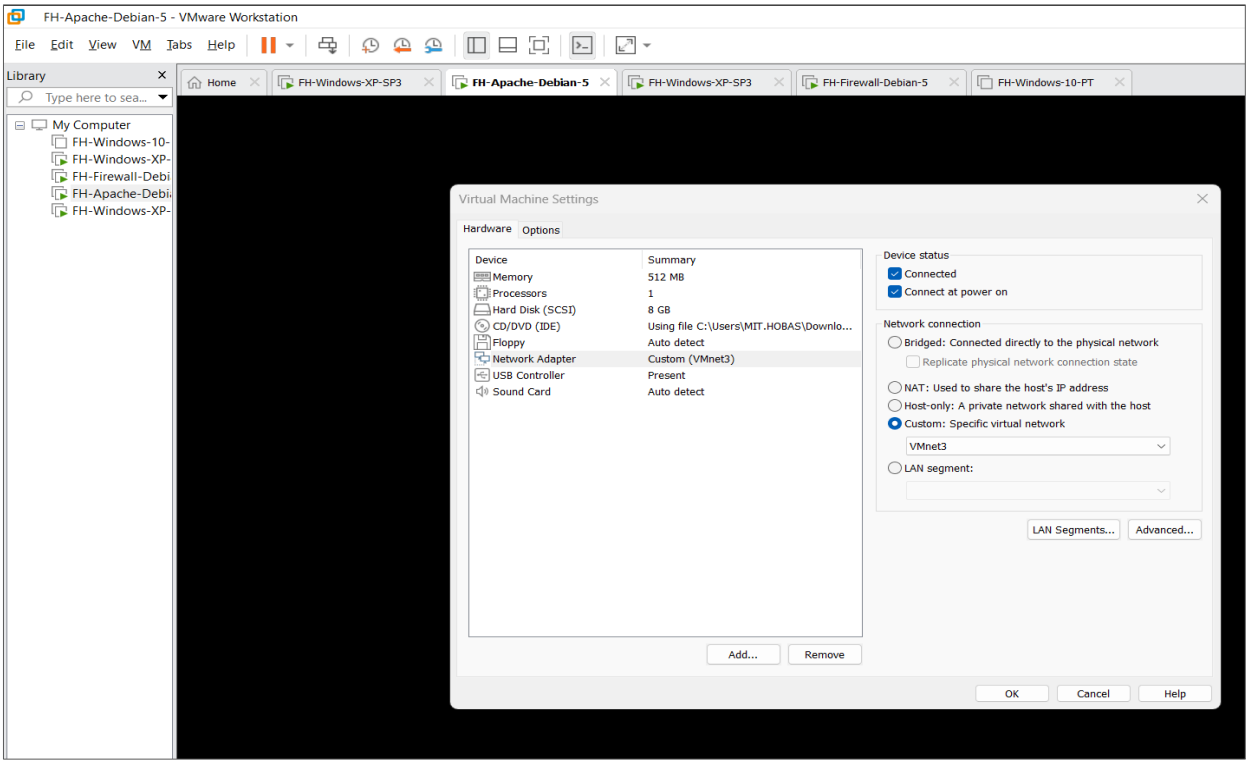


a.1) Assign:

- Static IP Address – 82.12.5.20
- Subnet Mask = 255.255.255.0
- Default Gateway – 82.12.5.1



b) Create **VMnet3** (DMZ (FH-IT-Security-Apache-Debian): 192.168.5.147/24



b.1) Assign:

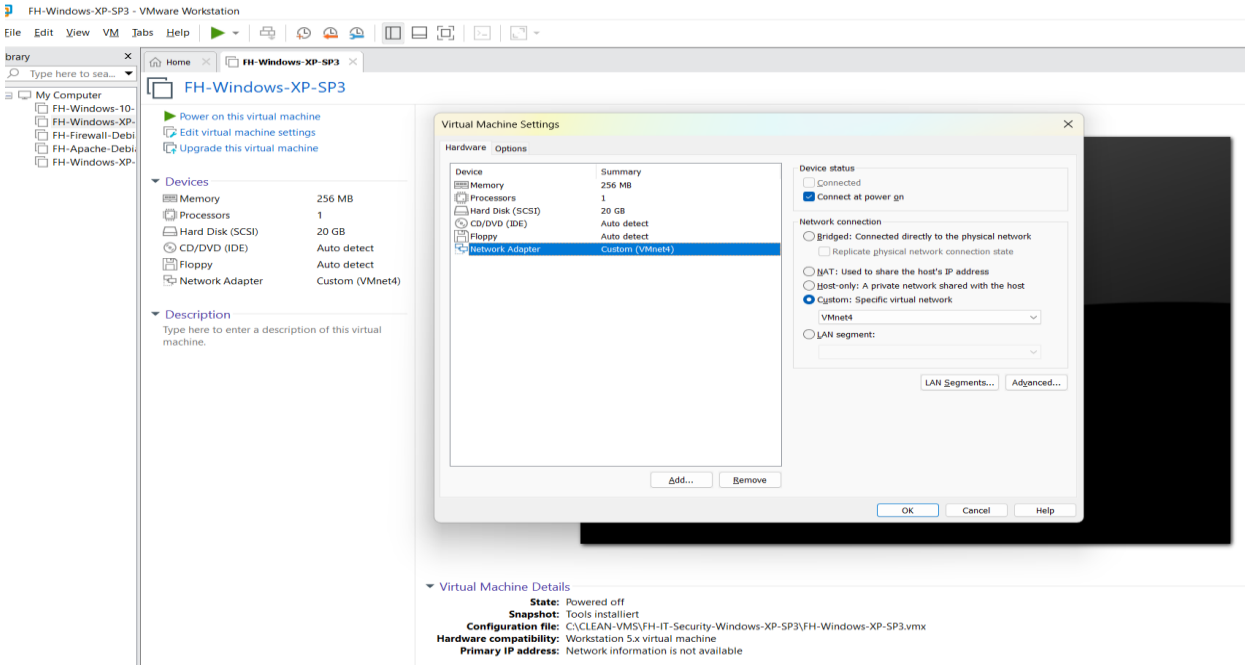
- Static IP Address – 192.168.5.147
- Subnet Mask = 255.255.255.0
- Default Gateway = 192.168.5.1

```
  GNU nano 2.0.7          File: /etc/network/interfaces


# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
# allow-hotplug eth0
auto eth0
iface eth0 inet static
        address 192.168.5.147
        netmask 255.255.255.0
        gateway 192.168.5.1




Search (to replace): _
^G Get Help     ^Y First Line   ^R No Replace   M-B Backwards   ^P PrevHstory
^C Cancel       ^V Last Line    M-C Case Sens   M-R Regexp      ^N NextHstory
```

b.2) Use the ***ifconfig*** command to confirm the IP interfaces.

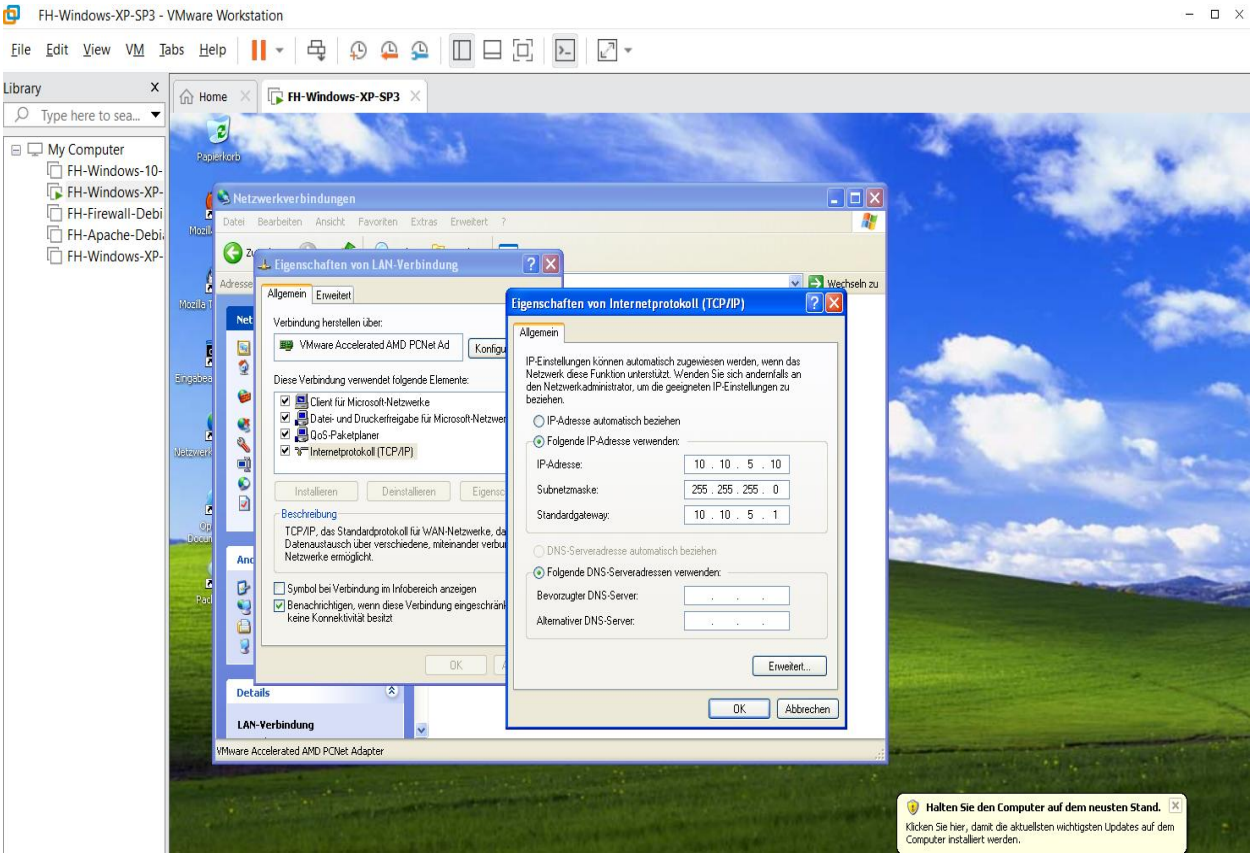
```
                                [ Cancelled ]

FH-SERVER:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:ef:eb:dd
          inet addr:192.168.5.147  Bcast:192.168.5.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feef:ebdd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:468 (468.0 B)
          Interrupt:18 Base address:0x1400

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:76 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:35329 (34.5 KiB)  TX bytes:35329 (34.5 KiB)

FH-SERVER:~#
```

c) Create **VMnet4** (Internal-Network/GREEN(FH-Windows-IT-Security-Windows-XP: 10.10.5.10/24)



c.1) Assign:

- Static IP Address – 10.10.5.10
- Subnet Mask = 255.255.255.0
- Default Gateway – 10.10.5.1



3. **Attach Interfaces to Linux Firewall**

-Use command ***nano /etc/network/interfaces*** to add interfaces

a) **eth0 (External): 82.12.5.1/24**

```
  GNU nano 2.0.7          File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0

auto eth0
iface eth0 inet static
        address 82.12.5.1
        netmask 255.255.255.0
        network 82.12.5.0
        # broadcast 82.12.12.0
        # gateway 192.168.237.0
        # dns-* options are implemented by the resolvconf package, if installed
        dns-nameservers 192.168.237.1
        dns-search FH
                                [ Read 41 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

b) **Eth01 (External): 82.12.5.2 /24**

```
  GNU nano 2.0.7          File: /etc/network/interfaces                Modified


auto eth0:1
iface eth0:1 inet static
        address 82.12.5.2
        netmask 255.255.255.0
```

c) **eth1 (DMZ): 192.168.5.1/24**

```
auto eth1
iface eth1 inet static
        address 192.168.5.1
        netmask 255.255.255.0
        network 192.168.5.0
```

d) **eth2 (Internal): 10.10.5.1/24**

```
auto eth2
iface eth2 inet static
        address 10.10.5.1
        netmask 255.255.255.0
```

4. **Verify the attached Interfaces assignments using:** ***ifconfig|more***

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:72:82:ce
          inet addr:82.12.5.1  Bcast:82.12.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2319 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2153 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:239882 (234.2 KiB)  TX bytes:217978 (212.8 KiB)
          Interrupt:18 Base address:0x1400

eth0:1    Link encap:Ethernet  HWaddr 00:0c:29:72:82:ce
          inet addr:82.12.5.2  Bcast:82.12.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          Interrupt:18 Base address:0x1400

eth1      Link encap:Ethernet  HWaddr 00:0c:29:72:82:d8
          inet addr:192.168.5.1  Bcast:192.168.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:364 errors:0 dropped:0 overruns:0 frame:0
          TX packets:287 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:58471 (57.1 KiB)  TX bytes:32823 (32.0 KiB)
          Interrupt:19 Base address:0x1480

eth2      Link encap:Ethernet  HWaddr 00:0c:29:72:82:e2
--More--
eth2      Link encap:Ethernet  HWaddr 00:0c:29:72:82:e2
          inet addr:10.10.5.1  Bcast:10.10.5.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:479 errors:0 dropped:0 overruns:0 frame:0
          TX packets:323 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:61307 (59.8 KiB)  TX bytes:41745 (40.7 KiB)
          Interrupt:16 Base address:0x1800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:13 errors:0 dropped:0 overruns:0 frame:0
          TX packets:13 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1092 (1.0 KiB)  TX bytes:1092 (1.0 KiB)

FH-FIREWALL:~#
```

5. **Enable IP Forwarding and Multicast Routing**
   - echo 1 > /proc/sys/net/ipv4/ip_forward
   - Change the value from 0 (False) to 1 (True) to enable IP forwarding

```
  GNU nano 2.0.7        File: /proc/sys/net/ipv4/ip_forward

  1

                                [ Read 1 line ]
  ^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
  ^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

6. Test Connectivity Using Ping (ICMP)

a) From the Firewall to the Web Server (**DMZ**)

```
FH-FIREWALL:~# ping 192.168.5.147
PING 192.168.5.147 (192.168.5.147) 56(84) bytes of data.
64 bytes from 192.168.5.147: icmp_seq=1 ttl=64 time=4.66 ms
64 bytes from 192.168.5.147: icmp_seq=2 ttl=64 time=0.661 ms
64 bytes from 192.168.5.147: icmp_seq=3 ttl=64 time=0.692 ms
64 bytes from 192.168.5.147: icmp_seq=4 ttl=64 time=1.61 ms
64 bytes from 192.168.5.147: icmp_seq=5 ttl=64 time=2.91 ms
64 bytes from 192.168.5.147: icmp_seq=6 ttl=64 time=2.14 ms
64 bytes from 192.168.5.147: icmp_seq=7 ttl=64 time=1.25 ms
64 bytes from 192.168.5.147: icmp_seq=8 ttl=64 time=1.39 ms
64 bytes from 192.168.5.147: icmp_seq=9 ttl=64 time=0.961 ms
```

b) From the Firewall to an Internal Client (**GREEN**)

```
FH-FIREWALL:~# ping 10.10.5.10
PING 10.10.5.10 (10.10.5.10) 56(84) bytes of data.
64 bytes from 10.10.5.10: icmp_seq=1 ttl=128 time=0.730 ms
64 bytes from 10.10.5.10: icmp_seq=2 ttl=128 time=1.13 ms
64 bytes from 10.10.5.10: icmp_seq=3 ttl=128 time=0.699 ms
64 bytes from 10.10.5.10: icmp_seq=4 ttl=128 time=0.626 ms
64 bytes from 10.10.5.10: icmp_seq=5 ttl=128 time=0.594 ms
64 bytes from 10.10.5.10: icmp_seq=6 ttl=128 time=0.508 ms
64 bytes from 10.10.5.10: icmp_seq=7 ttl=128 time=0.570 ms
64 bytes from 10.10.5.10: icmp_seq=8 ttl=128 time=0.752 ms
64 bytes from 10.10.5.10: icmp_seq=9 ttl=128 time=0.578 ms
```

c) From the Firewall to an External Client **(RED)**

```
FH-FIREWALL:~# ping 82.12.5.20
PING 82.12.5.20 (82.12.5.20) 56(84) bytes of data.
64 bytes from 82.12.5.20: icmp_seq=1 ttl=128 time=1.36 ms
64 bytes from 82.12.5.20: icmp_seq=2 ttl=128 time=0.968 ms
64 bytes from 82.12.5.20: icmp_seq=3 ttl=128 time=0.897 ms
64 bytes from 82.12.5.20: icmp_seq=4 ttl=128 time=1.16 ms
64 bytes from 82.12.5.20: icmp_seq=5 ttl=128 time=0.926 ms
64 bytes from 82.12.5.20: icmp_seq=6 ttl=128 time=0.554 ms
64 bytes from 82.12.5.20: icmp_seq=7 ttl=128 time=0.734 ms
64 bytes from 82.12.5.20: icmp_seq=8 ttl=128 time=0.543 ms
```

d) From an Internal Client to the Web Server **(DMZ)**

```
Eingabeaufforderung
Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 10.10.5.10
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 10.10.5.1

C:\Dokumente und Einstellungen\Administrator>ping 192.168.5.147

Ping wird ausgeführt für 192.168.5.147 mit 32 Bytes Daten:

Antwort von 192.168.5.147: Bytes=32 Zeit=3ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=4ms TTL=63

Ping-Statistik für 192.168.5.147:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 4ms, Mittelwert = 2ms
```

e) From an Internal Client to the External Client **(RED)**

```
Eingabeaufforderung
Antwort von 192.168.5.147: Bytes=32 Zeit=3ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=2ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=4ms TTL=63

Ping-Statistik für 192.168.5.147:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 4ms, Mittelwert = 2ms

C:\Dokumente und Einstellungen\Administrator>ping 82.12.5.20

Ping wird ausgeführt für 82.12.5.20 mit 32 Bytes Daten:

Antwort von 82.12.5.20: Bytes=32 Zeit=2ms TTL=127
Antwort von 82.12.5.20: Bytes=32 Zeit=4ms TTL=127
Antwort von 82.12.5.20: Bytes=32 Zeit=3ms TTL=127
Antwort von 82.12.5.20: Bytes=32 Zeit=7ms TTL=127

Ping-Statistik für 82.12.5.20:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 2ms, Maximum = 7ms, Mittelwert = 4ms
```

f) From an External Client to the Web Server (**DMZ**)

```
Eingabeaufforderung
Windows-IP-Konfiguration

Ethernetadapter LAN-Verbindung:

        Verbindungsspezifisches DNS-Suffix:
        IP-Adresse. . . . . . . . . . . . : 82.12.5.20
        Subnetzmaske. . . . . . . . . . . : 255.255.255.0
        Standardgateway . . . . . . . . . : 82.12.5.1

C:\Dokumente und Einstellungen\Administrator>ping 192.168.5.147

Ping wird ausgeführt für 192.168.5.147 mit 32 Bytes Daten:

Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63

Ping-Statistik für 192.168.5.147:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms

C:\Dokumente und Einstellungen\Administrator>
```

e) From an External Client to the Internal Client **(GREEN)**

```
Eingabeaufforderung
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63
Antwort von 192.168.5.147: Bytes=32 Zeit=1ms TTL=63

Ping-Statistik für 192.168.5.147:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms

C:\Dokumente und Einstellungen\Administrator>ping 10.10.5.10

Ping wird ausgeführt für 10.10.5.10 mit 32 Bytes Daten:

Antwort von 10.10.5.10: Bytes=32 Zeit=4ms TTL=127
Antwort von 10.10.5.10: Bytes=32 Zeit=1ms TTL=127
Antwort von 10.10.5.10: Bytes=32 Zeit<1ms TTL=127
Antwort von 10.10.5.10: Bytes=32 Zeit<1ms TTL=127

Ping-Statistik für 10.10.5.10:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 4ms, Mittelwert = 1ms

C:\Dokumente und Einstellungen\Administrator>_
```

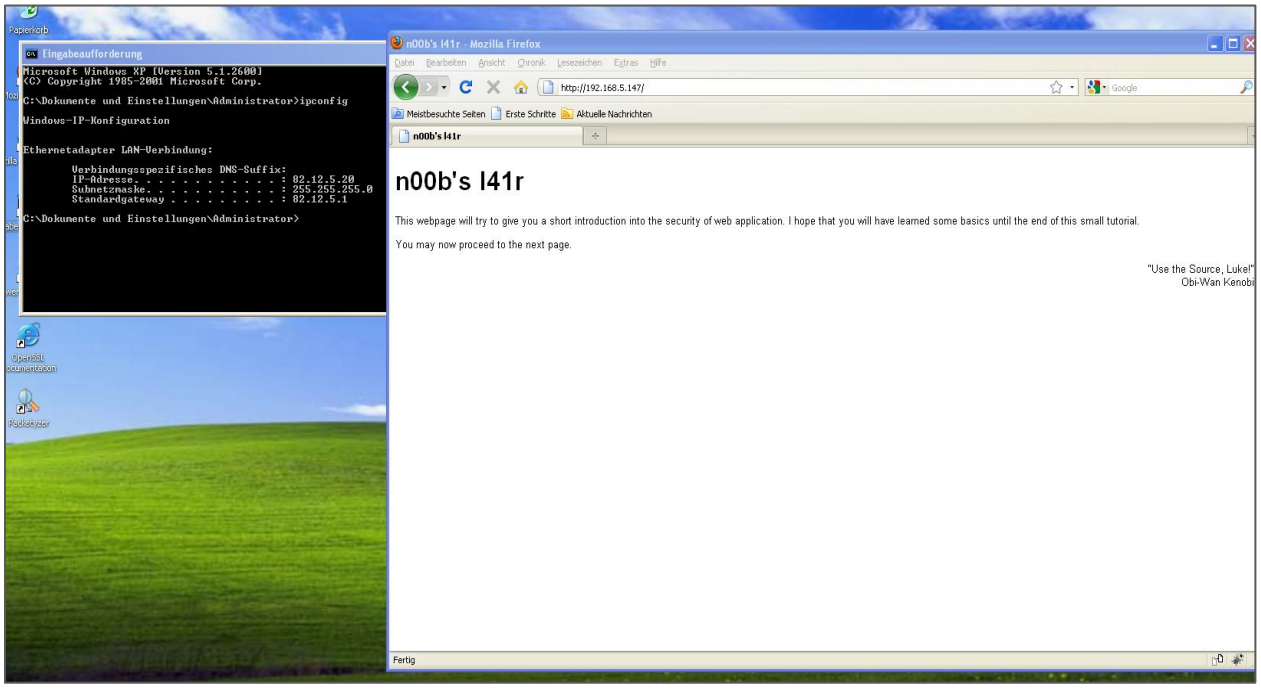
f) From Web Server to External Client **(RED)**

```
FH-SERVER:~# ping 82.12.5.20
PING 82.12.5.20 (82.12.5.20) 56(84) bytes of data.
64 bytes from 82.12.5.20: icmp_seq=1 ttl=127 time=12.1 ms
64 bytes from 82.12.5.20: icmp_seq=2 ttl=127 time=2.09 ms
64 bytes from 82.12.5.20: icmp_seq=3 ttl=127 time=2.84 ms
64 bytes from 82.12.5.20: icmp_seq=4 ttl=127 time=1.82 ms
64 bytes from 82.12.5.20: icmp_seq=5 ttl=127 time=4.68 ms
64 bytes from 82.12.5.20: icmp_seq=6 ttl=127 time=1.46 ms
64 bytes from 82.12.5.20: icmp_seq=7 ttl=127 time=1.59 ms
64 bytes from 82.12.5.20: icmp_seq=8 ttl=127 time=0.942 ms
```

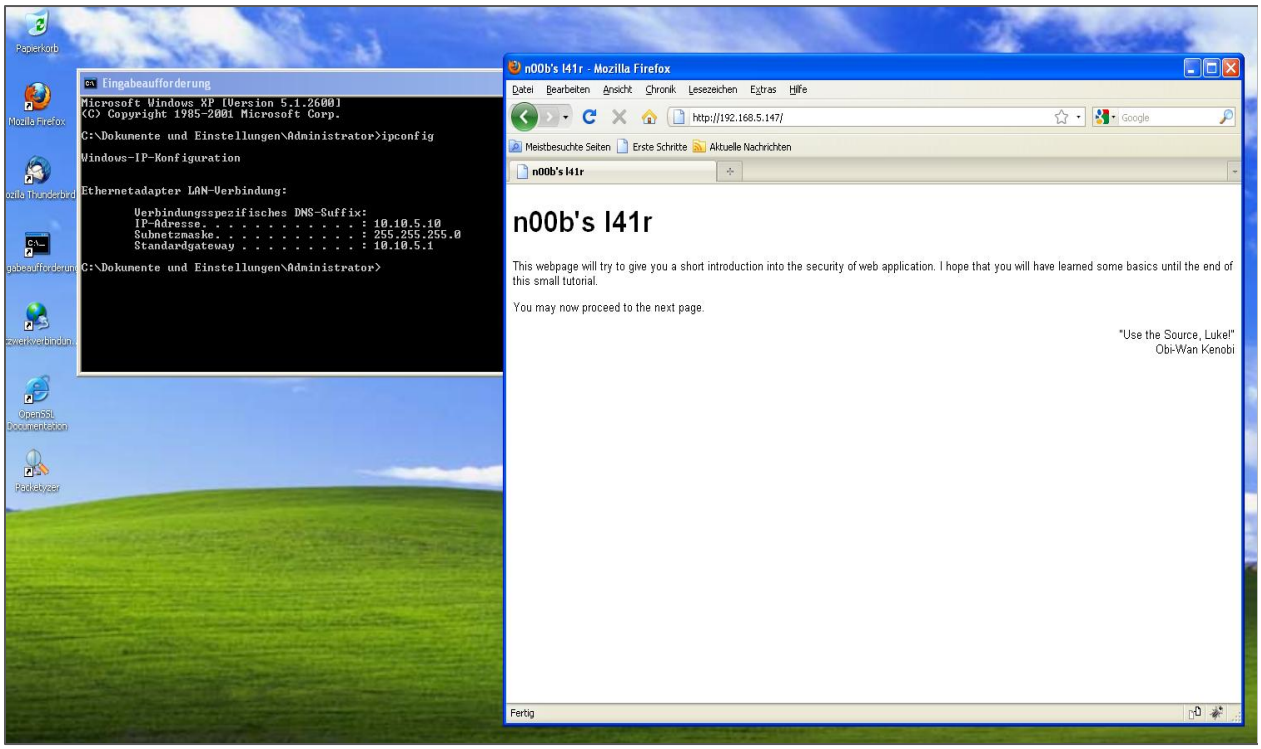
g) From Web Server to Internal Client **(GREEN)**

```
FH-SERVER:~# ping 10.10.5.10
PING 10.10.5.10 (10.10.5.10) 56(84) bytes of data.
64 bytes from 10.10.5.10: icmp_seq=1 ttl=127 time=5.50 ms
64 bytes from 10.10.5.10: icmp_seq=2 ttl=127 time=3.36 ms
64 bytes from 10.10.5.10: icmp_seq=3 ttl=127 time=2.38 ms
64 bytes from 10.10.5.10: icmp_seq=4 ttl=127 time=1.67 ms
64 bytes from 10.10.5.10: icmp_seq=5 ttl=127 time=2.27 ms
64 bytes from 10.10.5.10: icmp_seq=6 ttl=127 time=2.84 ms
64 bytes from 10.10.5.10: icmp_seq=7 ttl=127 time=2.35 ms
64 bytes from 10.10.5.10: icmp_seq=8 ttl=127 time=3.22 ms
64 bytes from 10.10.5.10: icmp_seq=9 ttl=127 time=2.80 ms
64 bytes from 10.10.5.10: icmp_seq=10 ttl=127 time=1.57 ms
```

7. **Check the external web server access using the web browser**



8. **Check the internal web server access using the web browser**



9. Difference Between Routing and Port Forwarding (DNAT)

a) Routing

- directing data packets between different networks based on their destination IP addresses. It determines the best path for data to travel from the source to the destination.
- The firewall routes traffic between:
  - RED (External): 82.12.5.0/24
  - ORANGE (DMZ): 192.168.5.0/24
  - GREEN (Internal): 10.10.5.0/24
- if a packet from the GREEN network (10.10.5.10) is destined for the ORANGE network (192.168.5.147), the firewall routes it based on its routing table.

b) Port Forwarding (DNAT)

- A packet arrives at the firewall with a destination IP address and port.
- The firewall modifies the destination IP address and/or port to forward the packet to an internal server.
- The internal server processes the request and sends the response back through the firewall, which translates the source address back to the original.

- **External Access to Web Server:**
  - An external user (RED network) tries to access the web server at http://82.12.5.2:80
  - The firewall uses DNAT to forward this traffic to the web server in the ORANGE (DMZ) network at 192.168.5.147:80
  - The web server responds, and the firewall translates the source address back to 82.12.5.2 before sending the response to the external user.

10. Firewall Configuration

a) Set the Default Rule

- This ensures that all traffic not explicitly allowed is dropped.

- ***iptables -P INPUT DROP***
- ***iptables -P FORWARD DROP***
- ***iptables -P OUTPUT DROP***

```
FH-FIREWALL:~# iptables -P INPUT DROP
FH-FIREWALL:~# iptables -P OUTPUT DROP
FH-FIREWALL:~# iptables -P FORWARD DROP
FH-FIREWALL:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
FH-FIREWALL:~# _
```

b) Firewall Rules for ICMP (from All Networks)

- ***iptables -A INPUT -j ACCEPT*** - allows the firewall itself to respond to ICMP requests
- ***iptables -A FORWARD -j ACCEPT***- allows ICMP traffic to pass through the firewall between networks - from GREEN to ORANGE or RED.
- ***iptables -A OUTPUT -j ACCEPT*** - allows the firewall to send ICMP requests to other devices

```
FH-FIREWALL:~# iptables -A INPUT -j ACCEPT
FH-FIREWALL:~# iptables -A OUTPUT -j ACCEPT
FH-FIREWALL:~# iptables -A FORWARD -j ACCEPT
FH-FIREWALL:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
FH-FIREWALL:~# _
```

c) Stateless Firewall Rules

- Both rules allow traffic from two specific subnets (192.168.5.0/24 and 10.10.5.0/24) to be forwarded through the firewall.
- Any traffic from these source IP ranges will be permitted to pass through the firewall to any destination.
  - ***iptables -A FORWARD* -s 192.168.5.0/24 -j ACCEPT**
  - ***iptables -A FORWARD* -s 10.10.5.0/24 -j ACCEPT**

```
FH-FIREWALL:~# iptables -A FORWARD -s 192.168.5.0/24 -j ACCEPT
FH-FIREWALL:~# iptables -A FORWARD -s 10.10.5.0/24 -j ACCEPT
FH-FIREWALL:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  192.168.5.0/24       anywhere
ACCEPT     all  --  10.10.5.0/24         anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
FH-FIREWALL:~#
```

d) Enable Destination Network Address Translation (DNAT)

d.1) Configure NAT for HTTP (Port 80)

- Forwards incoming TCP traffic on port 80 destined for 82.12.5.1 to the Web Server 192.168.5.147 on port 80.
  - ***iptables -t nat -A PREROUTING -p tcp -d 82.12.5.1 --dport 80 -j DNAT --to-destination 192.168.5.147:80***

d.2) Configure NAT for SSH (Port 22)

- Forwards incoming TCP traffic on port 22 destined for 82.12.5.2 to the Web Server 192.168.5.147 on port 22.
  - ***iptables -t nat -A PREROUTING -p tcp -d 82.12.5.2 --dport 22 -j DNAT --to-destination 192.168.5.147:22***

```
FH-FIREWALL:~# iptables -t nat -A PREROUTING -p tcp -d 82.12.5.1 --dport 80 -j D
NAT --to-destination 192.168.5.147:80
FH-FIREWALL:~# iptables -t nat -A PREROUTING -p tcp -d 82.12.5.2 --dport 22 -j D
NAT --to-destination 192.168.5.147:22
FH-FIREWALL:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.5.147       tcp dpt:ssh
ACCEPT     tcp  --  anywhere             192.168.5.147       tcp dpt:www
ACCEPT     all  --  192.168.5.0/24       anywhere
ACCEPT     all  --  10.10.5.0/24         anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
FH-FIREWALL:~#
```

e) Configure Masquerading as part of NAT settings

e.1) Masquerade outgoing traffic from the web server to the external network.

- *iptables -t nat -A POSTROUTING -p tcp -s 192.168.5.147 -j SNAT --to-source 80.12.5.1*
- *iptables -t nat -A POSTROUTING -p tcp -j MASQUERADE*

```
FH-FIREWALL:~# iptables -t nat -A POSTROUTING -p tcp -s 192.168.5.147 -j SNAT --
to-source 80.12.5.1
FH-FIREWALL:~# iptables -t nat -A POSTROUTING -p tcp -j MASQUERADE
FH-FIREWALL:~# iptables-save > /root/firewall.rules
FH-FIREWALL:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.5.147       tcp dpt:ssh
ACCEPT     tcp  --  anywhere             192.168.5.147       tcp dpt:www
ACCEPT     all  --  192.168.5.0/24       anywhere
ACCEPT     all  --  10.10.5.0/24         anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
FH-FIREWALL:~#
```

f) Stateful Filtering

1. Allow Loopback and Established Traffic

- *iptables -A INPUT -i lo -j ACCEPT*
- *iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT*

2. Allow External Traffic to DMZ Web Server

➢ **HTTP/HTTPS to DMZ Web Server (192.168.5.147)**

- *iptables -A FORWARD -i eth0 -o eth1 -d 192.168.5.147 -p tcp --dport 80 -j ACCEPT*
- *iptables -A FORWARD -i eth0 -o eth1 -d 192.168.5.147 -p tcp --dport 443 -j ACCEPT*

➢ **Allow return traffic from DMZ to External**

- *iptables -A FORWARD -i eth1 -o eth0 -s 192.168.5.147 -j ACCEPT*

3. Block External Traffic to Internal Network

- *iptables -A FORWARD -i eth0 -o eth2 -j DROP*

4. Allow Internal (GREEN) to Access Internet and DMZ

➢ **GREEN → Internet (via NAT)**

- *iptables -t nat -A POSTROUTING -o eth0 -s 10.10.5.0/24 -j SNAT --to-source 82.12.5.2*

- **GREEN → DMZ Web Server**

  - *iptables -A FORWARD -i eth2 -o eth1 -s 10.10.10.0/24 -d 192.168.5.147 -p tcp --dport 80 -j ACCEPT*
  - *iptables -A FORWARD -i eth2 -o eth1 -s 10.10.10.0/24 -d 192.168.5.147 -p tcp --dport 443 -j ACCEPT*

4. Allow SSH from GREEN to Firewall

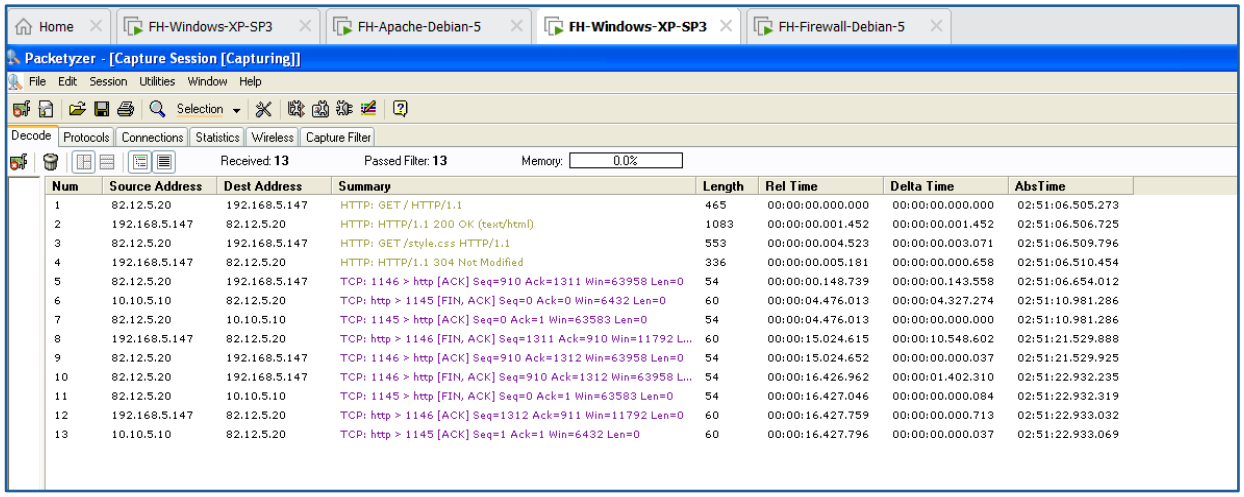
- *iptables -A INPUT -i eth2 -s 10.10.5.0/24 -p tcp --dport 22 -j ACCEPT*

g) Save Current iptables Rules

```
FH-FIREWALL:~# iptables-save > /root/firewall.rules
FH-FIREWALL:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  192.168.5.0/24       anywhere
ACCEPT     all  --  10.10.5.0/24         anywhere
ACCEPT     tcp  --  anywhere             192.168.5.147       tcp dpt:www
ACCEPT     tcp  --  anywhere             192.168.5.147       tcp dpt:ssh
ACCEPT     tcp  --  82.12.5.1            10.10.5.10          tcp dpt:http-alt st
ate NEW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh state N
EW,ESTABLISHED
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:www state N
EW,ESTABLISHED
ACCEPT     all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
FH-FIREWALL:~#
```

1. **External (RED) to DMZ (ORANGE)**:
   - Allows HTTP/HTTPS to the DMZ web server (192.168.5.147).
   - Blocks all other traffic from RED to GREEN.
2. **Internal (GREEN) to DMZ/Internet**:
   - GREEN clients can access the DMZ web server and the internet via NAT.
   - NAT rule (SNAT) masks internal IPs with the firewall's external IP (82.12.5.2).
3. **SSH** :
   - Only GREEN clients (10.10.5.0/24) can SSH into the firewall.
4. **Stateful Filtering**:
   - ESTABLISHED,RELATED rules allow return traffic for existing connections.

Anaylze Network Traffic
(Packetyzer)



Num	Source Address	Dest Address	Summary	Length	Rel Time	Delta Time	AbsTime
1	82.12.5.20	192.168.5.147	HTTP: GET / HTTP/1.1	465	00:00:00.000.000	00:00:00.000.000	02:51:06.505.273
2	192.168.5.147	82.12.5.20	HTTP: HTTP/1.1 200 OK (text/html)	1083	00:00:00.001.452	00:00:00.001.452	02:51:06.506.725
3	82.12.5.20	192.168.5.147	HTTP: GET /style.css HTTP/1.1	553	00:00:00.004.523	00:00:00.003.071	02:51:06.509.796
4	192.168.5.147	82.12.5.20	HTTP: HTTP/1.1 304 Not Modified	336	00:00:00.005.181	00:00:00.000.658	02:51:06.510.454
5	82.12.5.20	192.168.5.147	TCP: 1146 > http [ACK] Seq=910 Ack=1311 Win=63958 Len=0	54	00:00:00.148.739	00:00:00.143.558	02:51:06.654.012
6	10.10.5.10	82.12.5.20	TCP: http > 1145 [FIN, ACK] Seq=0 Ack=0 Win=6432 Len=0	60	00:00:04.476.013	00:00:04.327.274	02:51:10.981.286
7	82.12.5.20	10.10.5.10	TCP: 1145 > http [ACK] Seq=0 Ack=1 Win=63583 Len=0	54	00:00:04.476.013	00:00:00.000.000	02:51:10.981.286
8	192.168.5.147	82.12.5.20	TCP: http > 1146 [FIN, ACK] Seq=1311 Ack=910 Win=11792 L...	60	00:00:15.024.615	00:00:10.548.602	02:51:21.529.888
9	82.12.5.20	192.168.5.147	TCP: 1146 > http [ACK] Seq=910 Ack=1312 Win=63958 Len=0	54	00:00:15.024.652	00:00:00.000.037	02:51:21.529.925
10	82.12.5.20	192.168.5.147	TCP: 1146 > http [FIN, ACK] Seq=910 Ack=1312 Win=63958 L...	54	00:00:16.426.962	00:00:01.402.310	02:51:22.932.235
11	82.12.5.20	10.10.5.10	TCP: 1145 > http [FIN, ACK] Seq=0 Ack=1 Win=63583 Len=0	54	00:00:16.427.046	00:00:00.000.084	02:51:22.932.319
12	192.168.5.147	82.12.5.20	TCP: http > 1146 [ACK] Seq=1312 Ack=911 Win=11792 Len=0	60	00:00:16.427.759	00:00:00.000.713	02:51:22.933.032
13	10.10.5.10	82.12.5.20	TCP: http > 1145 [ACK] Seq=1 Ack=1 Win=6432 Len=0	60	00:00:16.427.796	00:00:00.000.037	02:51:22.933.069

1. Frame 1

1.1. Ethernet Layer (Layer 2 - Data Link)

- Source MAC: 00:0c:29:ac:12:c4
- Destination MAC: 00:0c:29:72:82:ce
- Type: IPv4 (0x0800)

  This shows that the packet is traveling within a local network segment between two MAC addresses.

1.2 Internet Layer (Layer 3 - IP)

- Source IP: 82.12.5.20
- Destination IP: 192.168.5.147
- Protocol: TCP (0x06)
- Total Length: 451 bytes
- Flags: 0x04 (Don't Fragment)

  This means:
- The client with IP 82.12.5.20 is sending a request to the web server at 192.168.5.147.
- The packet is part of an HTTP request (Layer 7 application traffic).
- No fragmentation is allowed, meaning the entire packet must be delivered in one piece.

1.3Transport Layer (Layer 4 - TCP)

- Source Port: 1146 (random client port)
- Destination Port: 80 (HTTP)
- Sequence Number: 0 (First packet of the TCP stream)
- Acknowledgment Number: 0 (No prior data acknowledged)
- Flags: PSH, ACK (0x0018)
- Window Size: 62929

  Key points:
- The PSH (Push) flag means the packet should be delivered immediately.
- The ACK (Acknowledgment) flag indicates an ongoing TCP connection.
- This is part of an established connection where the client is sending a request to an HTTP server.

Packetyzer - [Capture Session [Capturing]]

File Edit Session Utilities Window Help

Selection

Decode | Protocols | Connections | Statistics | Wireless | Capture Filter

Received: 15 Passed Filter: 15 Memory: 0.0%

- Frame 1 (465 bytes on wire, 465 bytes captured)
- Ethernet II, Src: 00:0c:29:ac:12:c4 (00:0c:29:ac:12:c4), Dst: 00:0c:29:72:82:ce (00:0c:29:72:82:ce)
  - Destination: 00:0c:29:72:82:ce (00:0c:29:72:82:ce)
  - Source: 00:0c:29:ac:12:c4 (00:0c:29:ac:12:c4)
  - Type: IP (0x0800)
- Internet Protocol, Src: 82.12.5.20 (82.12.5.20), Dst: 192.168.5.147 (192.168.5.147)
  - Version: 4
  - Header length: 20 bytes
  - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  - Total Length: 451
  - Identification: 0x16ab (5803)
  - Flags: 0x04 (Don't Fragment)
  - Fragment offset: 0
  - Time to live: 128
  - Protocol: TCP (0x06)
  - Header checksum: 0xc52e [correct]
  - Source: 82.12.5.20 (82.12.5.20)
  - Destination: 192.168.5.147 (192.168.5.147)
- Transmission Control Protocol, Src Port: 1146 (1146), Dst Port: http (80), Seq: 0, Ack: 0, Len: 411
  - Source port: 1146 (1146)
  - Destination port: http (80)
  - Sequence number: 0 (relative sequence number)
  - Next sequence number: 411 (relative sequence number)
  - Acknowledgement number: 0 (relative ack number)
  - Header length: 20 bytes
  - Flags: 0x0018 (PSH, ACK)
  - Window size: 62929
  - Checksum: 0x9a8c [correct]
- Hypertext Transfer Protocol
  - GET / HTTP/1.1\r\n
  - Host: 192.168.5.147\r\n
  - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.1.7) Gecko/20091221 Firefox/3.5.7\r\n
  - Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  - Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3\r\n
  - Accept-Encoding: gzip,deflate\r\n
  - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
  - Keep-Alive: 300\r\n
  - Connection: keep-alive\r\n
  - Cache-Control: max-age=0\r\n
  - \r\n

2. Frame 2 (1083 bytes on wire, 1083 bytes captured)

2.1 Ethernet II Layer

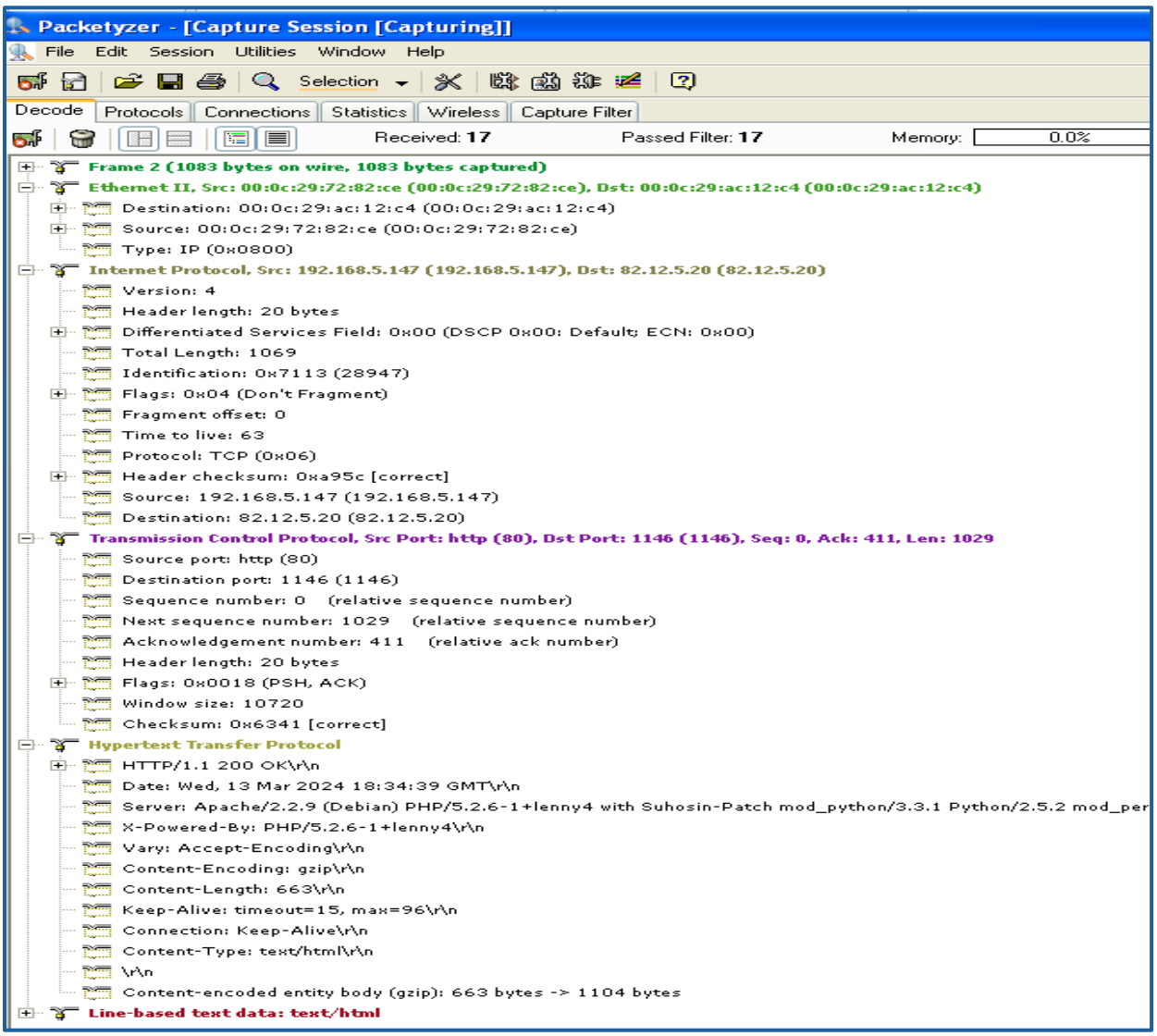
- Source MAC Address: 00:0c:29:72:82:ce
- Destination MAC Address**:** 00:0c:29:ac:12:c4
- **Type:** IPv4 (0x0800)

2.2 Internet Protocol (IP) Layer

- Source IP: 192.168.5.147 (Web SERVER)
- Destination IP: 82.12.5.20 (Public IP, external server)
- Protocol: TCP (0x06)

2.3 Transmission Control Protocol (TCP) Layer

- Source Port: 80 (HTTP server)
- Destination Port: 1146 (Client-side port)
- Sequence Number: 0 (Relative)
- Acknowledgment Number: 411
- Flags: PSH, ACK
- Window Size: 10720
- Checksum: Correct



3. Frame 6 Frame 6 (60 bytes on wire, 60 bytes captured)

3.1 **Ethernet II Layer**

- Source MAC: 00:0c:29:72:82:ce
- Destination MAC: 00:0c:29:ac:12:c4
- Type: IPv4 (0x0800)

3.2 Internet Protocol (IP) Layer

- Source IP: 10.10.5.10 (internal network)
- Destination IP: 82.12.5.20 (Public server)
- Protocol: TCP (0x06)
- Total Length: 40 bytes (suggesting no additional payload)

3.3 **Transmission Control Protocol (TCP) Layer**

- Source Port: 80 (Web Server)
- Destination Port: 1145 (Client-side port)
- Sequence Number: 0
- Acknowledgment Number: 0
- Flags: FIN, ACK (0x0011)
- Window Size: 6432
- Checksum: Correct