

W9D4_pfsense

Per l'utilizzo del firewall Pfsense è necessario creare una infrastruttura che permetta alle macchine virtuali Meta e Kali una comunicazione che avviene su due reti diverse. Questo perchè come si evince in *figura 1*, il firewall si 'trova' tra l'host e le reti.

è assegnato un indirizzo WAN 10.02.15/24 per consentire la comunicazione verso l'esterno e due indirizzi su rete interna : LAN 1 192.168.50.101 per la vm Kali e 192.168.60.104 per la meta.

Per verificare la comunicazione tra le macchine e la corretta configurazione delle reti è stato lanciato un ping dalle vm verso pfsense che ha dato i risultati come mostrato in figura 2 e 3 e successivamente anche da pfsense verso le machine kali e meta

-l'ip di pfsense è uguale al gateway della kali.

Figura 1

```
DHCPD...
The IPv4 OPT1 address has been set to 192.168.60.104/24
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 86fa195f9d5532b84abd

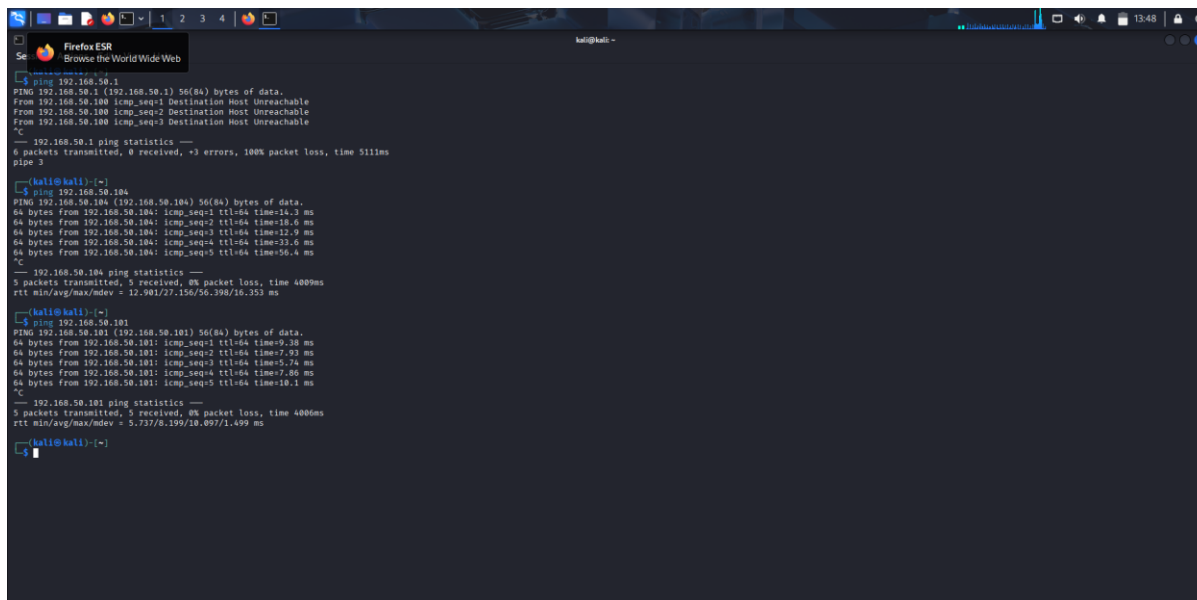
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.101/24
LAN2 (opt1)    -> em2      -> v4: 192.168.60.104/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Figura 2



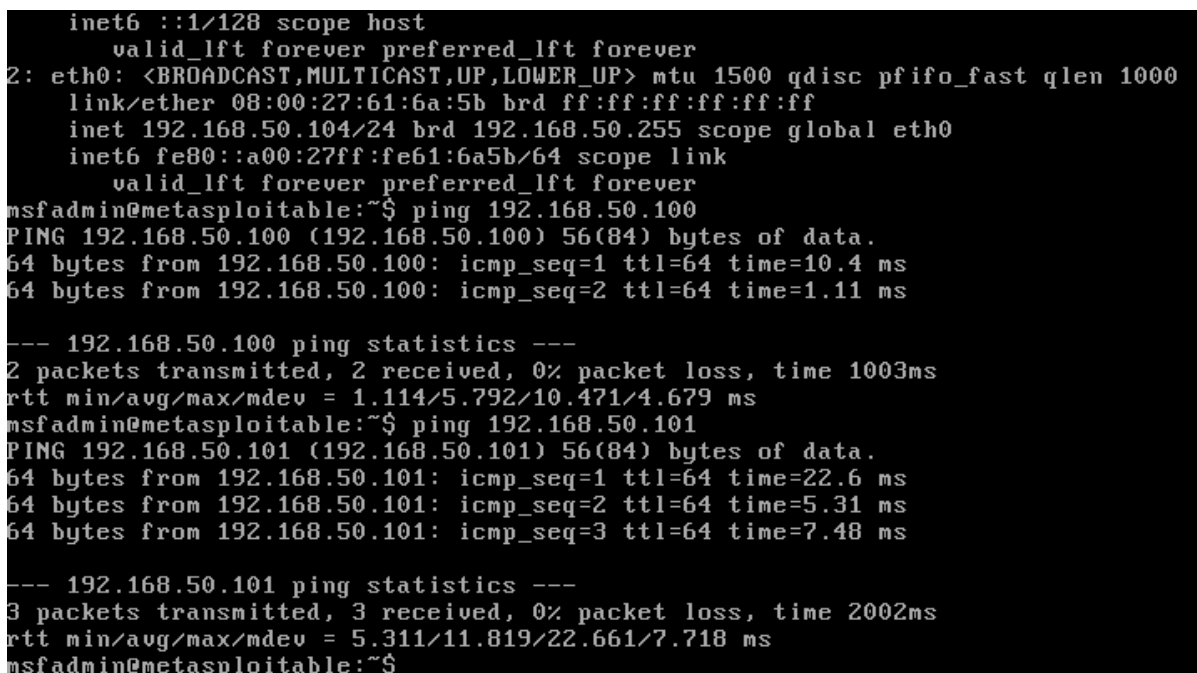
```
kali@kali:~$ ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
From 192.168.50.100: icmp_seq=1 Destination Host Unreachable
From 192.168.50.100: icmp_seq=2 Destination Host Unreachable
From 192.168.50.100: icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.50.1 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 511ms
pipe 3

kali@kali:~$ ping 192.168.50.104
PING 192.168.50.104 (192.168.50.104) 56(84) bytes of data.
64 bytes from 192.168.50.104: icmp_seq=1 ttl=64 time=16.3 ms
64 bytes from 192.168.50.104: icmp_seq=2 ttl=64 time=18.6 ms
64 bytes from 192.168.50.104: icmp_seq=3 ttl=64 time=12.9 ms
64 bytes from 192.168.50.104: icmp_seq=4 ttl=64 time=33.6 ms
64 bytes from 192.168.50.104: icmp_seq=5 ttl=64 time=56.4 ms
^C
--- 192.168.50.104 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/mdev = 12.901/27.156/56.398/16.353 ms

kali@kali:~$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=9.38 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=7.93 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=5.74 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=7.06 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=19.1 ms
^C
--- 192.168.50.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 400ms
rtt min/avg/max/mdev = 5.737/8.199/19.097/1.499 ms

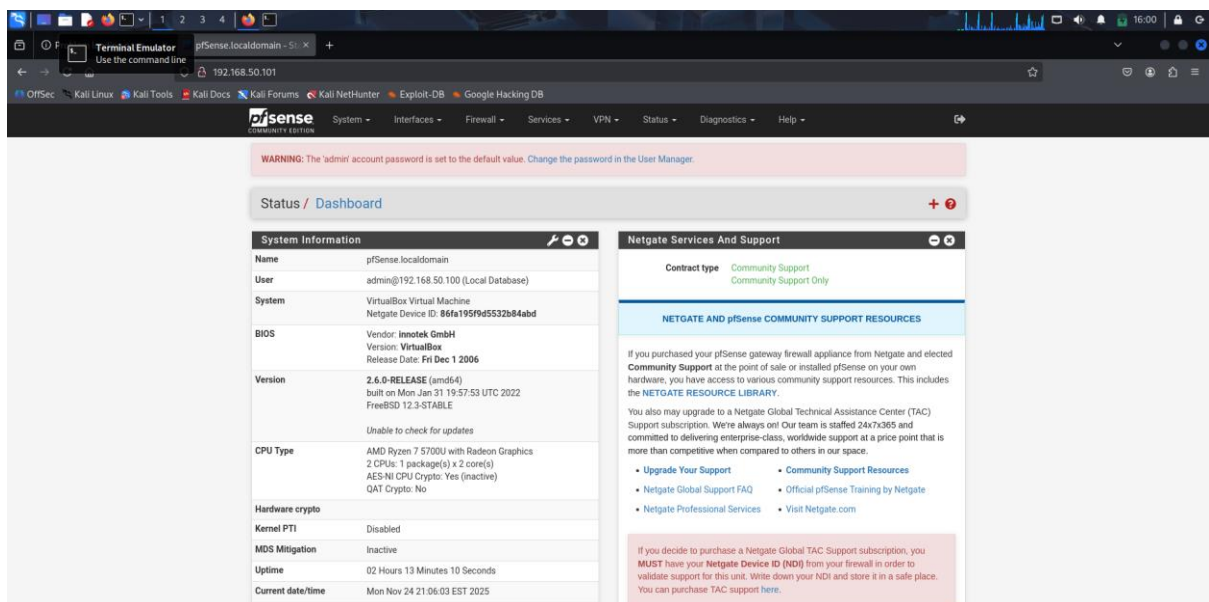
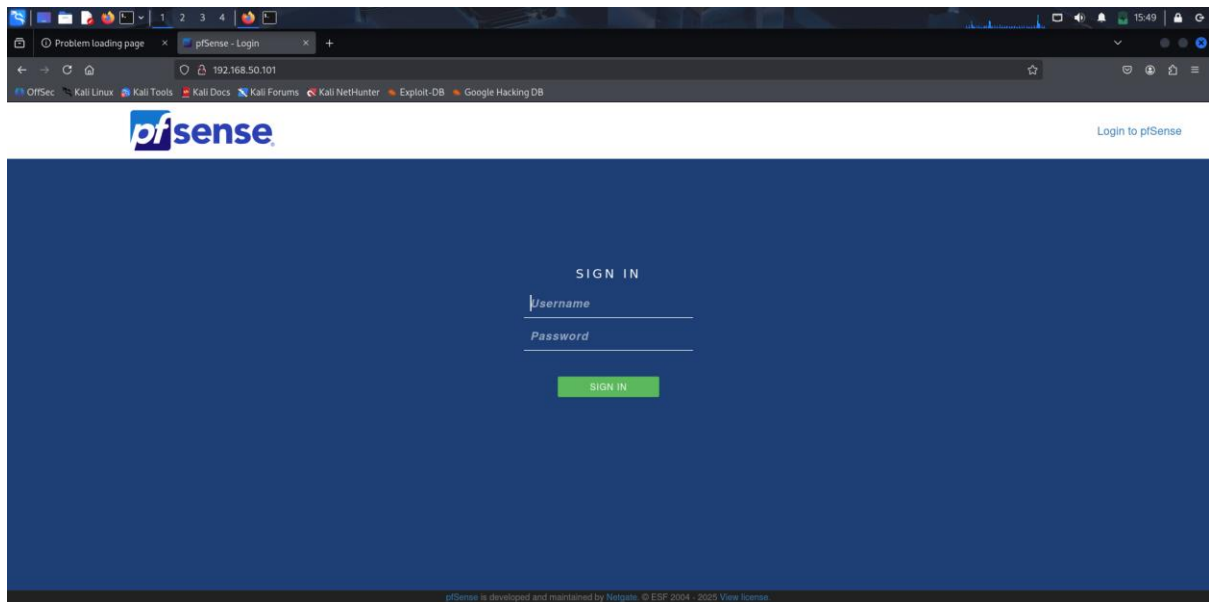
kali@kali:~$
```

Figura 3



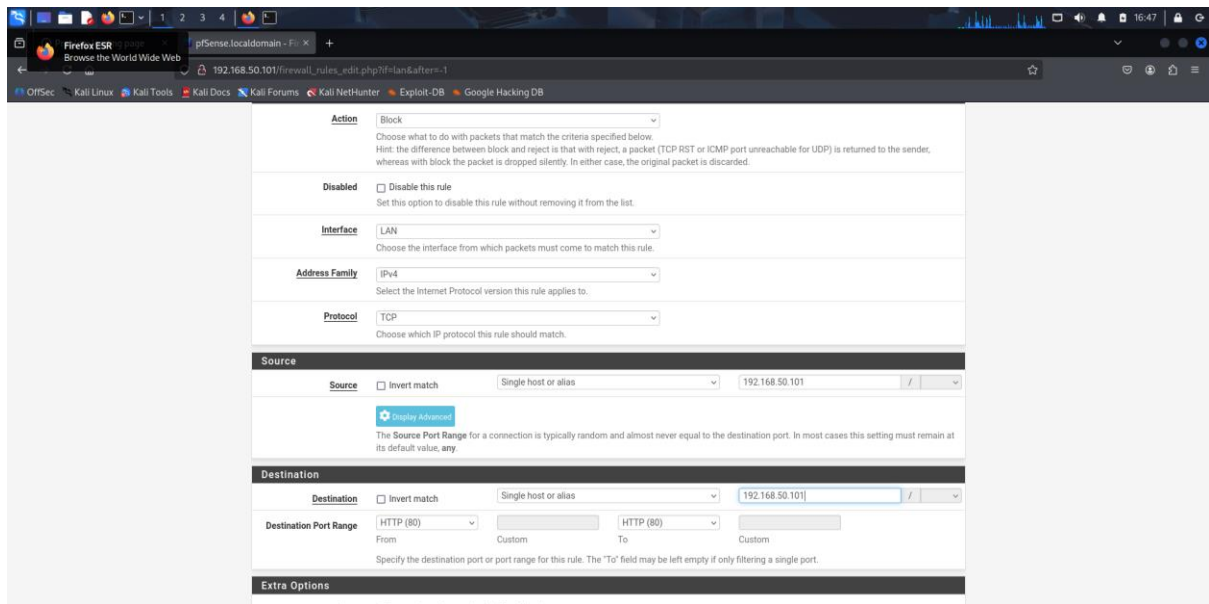
```
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:61:6a:5b brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.104/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe61:6a5b/64 scope link
    valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=10.4 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.11 ms
^C
--- 192.168.50.100 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.114/5.792/10.471/4.679 ms
msfadmin@metasploitable:~$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=22.6 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=5.31 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=7.48 ms
^C
--- 192.168.50.101 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 5.311/11.819/22.661/7.718 ms
msfadmin@metasploitable:~$
```

Si prosegue con la verifica su una pagina web nella quale è inserito l'ip 192.168.50.101 che rimanda alla home di PfSense.

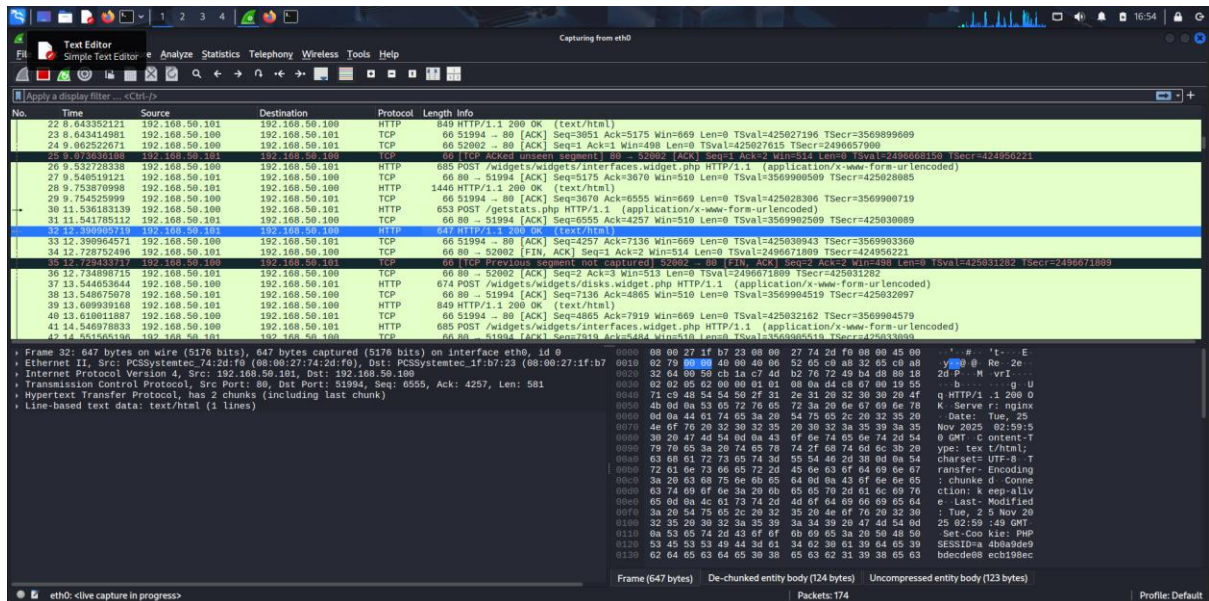


Si può creare da questo momento in avanti la regola per il firewall.

Sulla lan 2 (meta) bisogna abilitare il server dhcp e successivamente bloccare il traffico di pacchetti da kali a meta sulla porta 80. Flag sui log.



Se vi è comunicazione la cattura in wireshark mostra la connessione



Con il blocco della porta 80 per il protocollo http la cattura restituirà un risultato diverso.

Terminal Emulator

Apply a display filter: `<Ctrl>F`

No.	Time	Source	Destination	Protocol	Length	Info
137	39.820785977	192.168.50.101	192.168.50.100	TCP	66	80 → 34820 [ACK] Seq=42154 Ack=14987 Win=510 Len=0 TSval=3782830071 TSecr=425867687
138	39.848498990	192.168.50.101	192.168.50.100	HTTP	850	HTTP/1.1 200 OK (text/html)
139	39.940619307	192.168.50.100	192.168.50.101	TCP	66	34820 → 80 [ACK] Seq=14987 Ack=42938 Win=669 Len=0 TSval=425867811 TSecr=3782830191
140	40.814995125	192.168.50.100	192.168.50.101	HTTP	685	POST /widgets/widgets/interfaces.widget.php HTTP/1.1 (application/x-www-form-urlencoded)
141	40.829541380	192.168.50.101	192.168.50.100	TCP	66	80 → 34820 [ACK] Seq=42938 Ack=15006 Win=510 Len=0 TSval=3782831071 TSecr=425866866
142	40.968484381	192.168.50.100	192.168.50.101	TCP	66	[TCP Dup ACK 184] 38274 → 80 [ACK] Seq=1 Ack=1 Win=488 Len=0 TSval=425868831 TSecr=3458676028
143	40.965638814	192.168.50.101	192.168.50.100	TCP	66	[TCP Dup ACK 243] 80 → 38274 [ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=3458688278 TSecr=425867659
144	41.022277803	192.168.50.101	192.168.50.100	HTTP	1448	HTTP/1.1 200 OK (text/html)
145	41.062174384	192.168.50.100	192.168.50.101	TCP	66	34820 → 80 [ACK] Seq=15006 Ack=44318 Win=669 Len=0 TSval=425868933 TSecr=3782831321
146	50.382388247	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1fa86619
147	51.068803820	192.168.50.101	192.168.50.101	TCP	66	[TCP Keep-Alive] 34820 → 80 [ACK] Seq=15005 Ack=44318 Win=674 Len=0 TSval=425878939 TSecr=3782831321
148	51.07852748	192.168.50.101	192.168.50.100	TCP	66	[TCP Keep-Alive ACK] 80 → 34820 [ACK] Seq=44318 Ack=15006 Win=514 Len=0 TSval=3782841331 TSecr=425868933
149	51.201601423	192.168.50.100	192.168.50.101	TCP	66	[TCP Dup ACK 185] 38274 → 80 [ACK] Seq=1 Ack=1 Win=488 Len=0 TSval=425878072 TSecr=3458688278
150	51.208446975	192.168.50.101	192.168.50.100	TCP	66	[TCP Dup ACK 245] 80 → 38274 [ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=3458688219 TSecr=425867659
151	52.311975122	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1fa86619
152	54.7588931475	192.168.50.101	192.168.50.100	TCP	66	80 → 58274 [FIN, ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=3458694078 TSecr=425867659
153	54.76562490	192.168.50.100	192.168.50.101	TCP	66	[TCP Dup ACK 186] 38274 → 80 [ACK] Seq=1 Ack=1 Win=488 Len=0 TSval=425882629 TSecr=3458694078
154	54.762158287	192.168.50.101	192.168.50.100	TCP	66	80 → 58274 [ACK] Seq=2 Ack=3 Win=514 Len=0 TSval=3458694078 TSecr=425882629
155	55.318672297	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1fa86619
156	60.328897764	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1fa86619
157	61.184126084	192.168.50.100	192.168.50.101	TCP	66	[TCP Keep-Alive] 34820 → 80 [ACK] Seq=15005 Ack=44318 Win=674 Len=0 TSval=425888056 TSecr=3782841331

Frame 81: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23), Dst: PCSSystemtec_74:2d:f9 (08:00:27:74:2d:f9)

Destination: PCSSystemtec_74:2d:f9 (08:00:27:74:2d:f9)

.....0..... = IG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Source: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)

.....0..... = IG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

[Stream index: 0]

Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.50.101

Transmission Control Protocol, Src Port: 34820, Dst Port: 80, Seq: 1, Len: 0

Transmission Control Protocol (tcp), 32 bytes

Packets: 491 - Dropped: 0 (0.0%)

Profile: Default