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

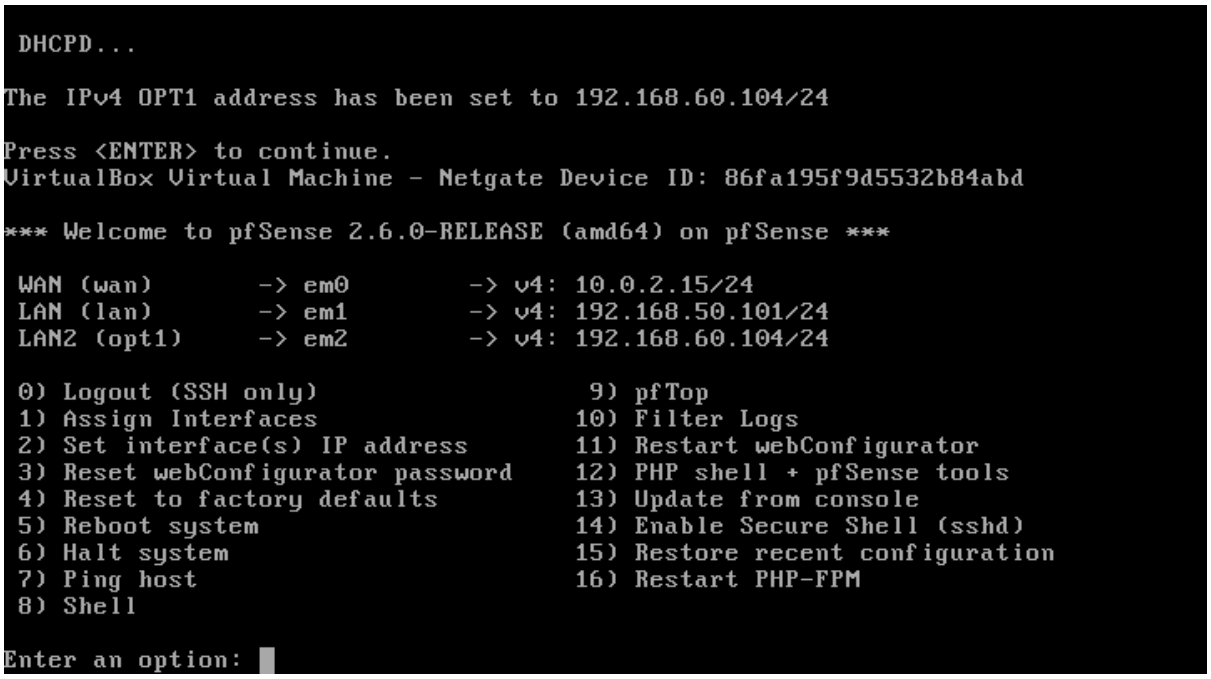


Figura 2

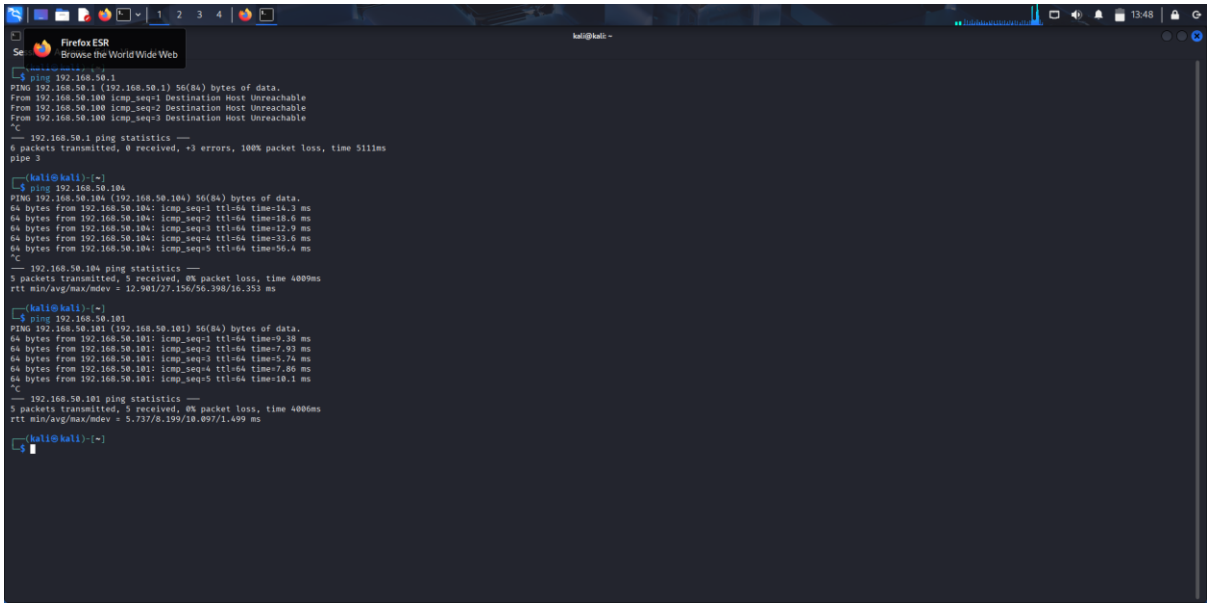
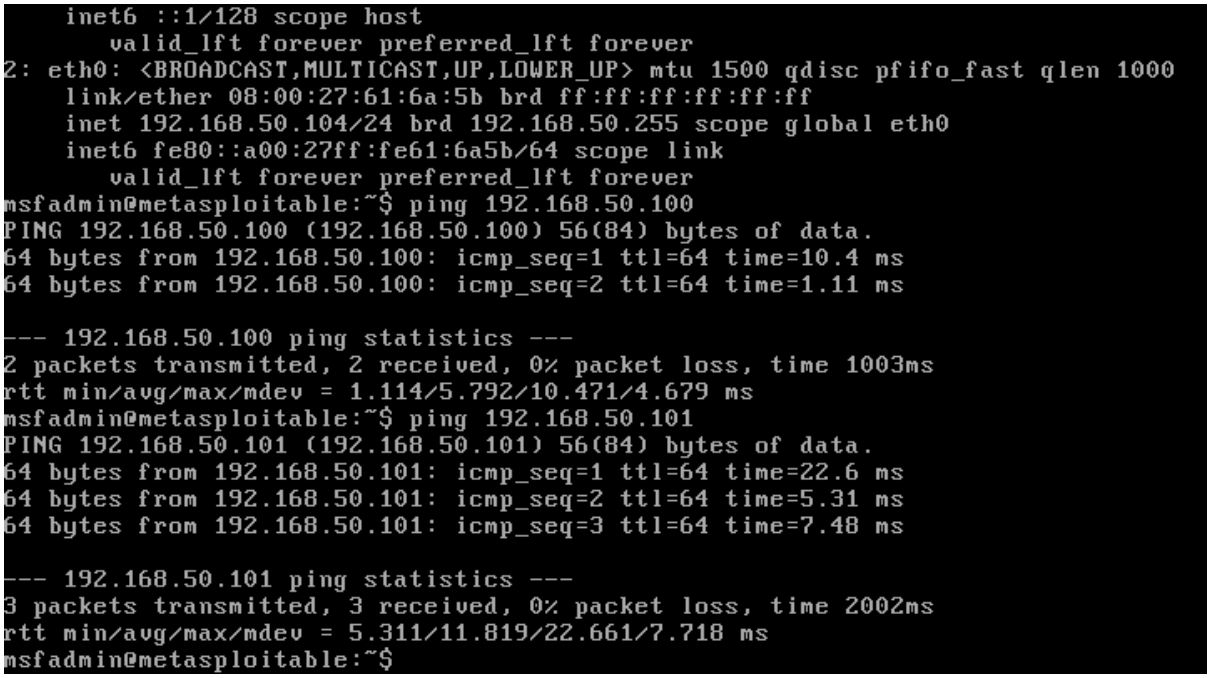
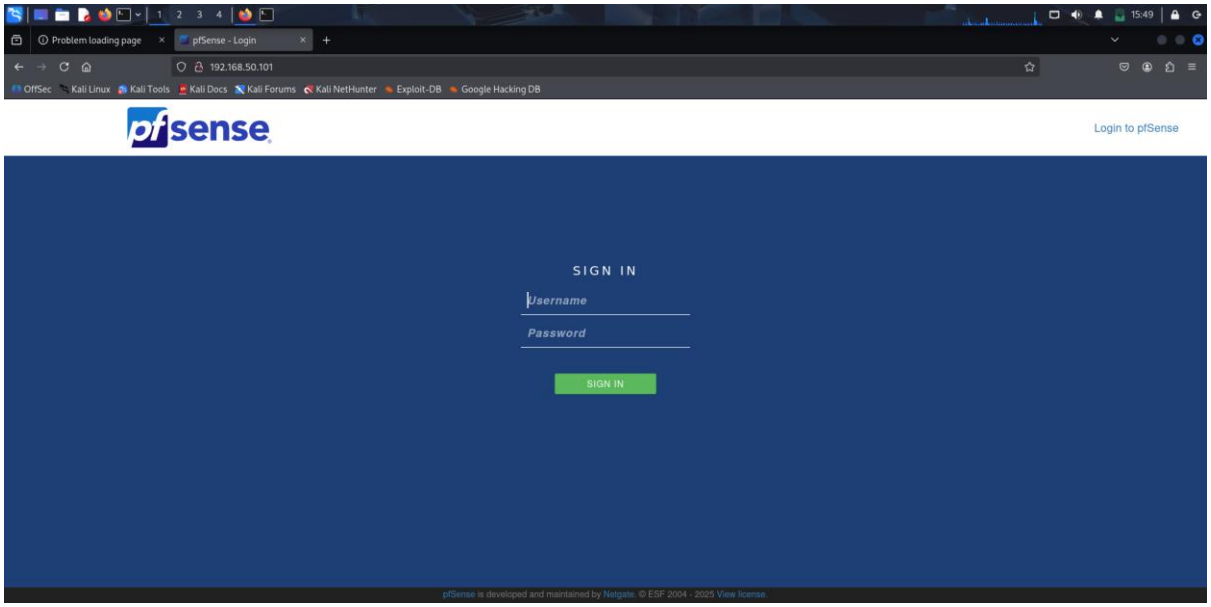
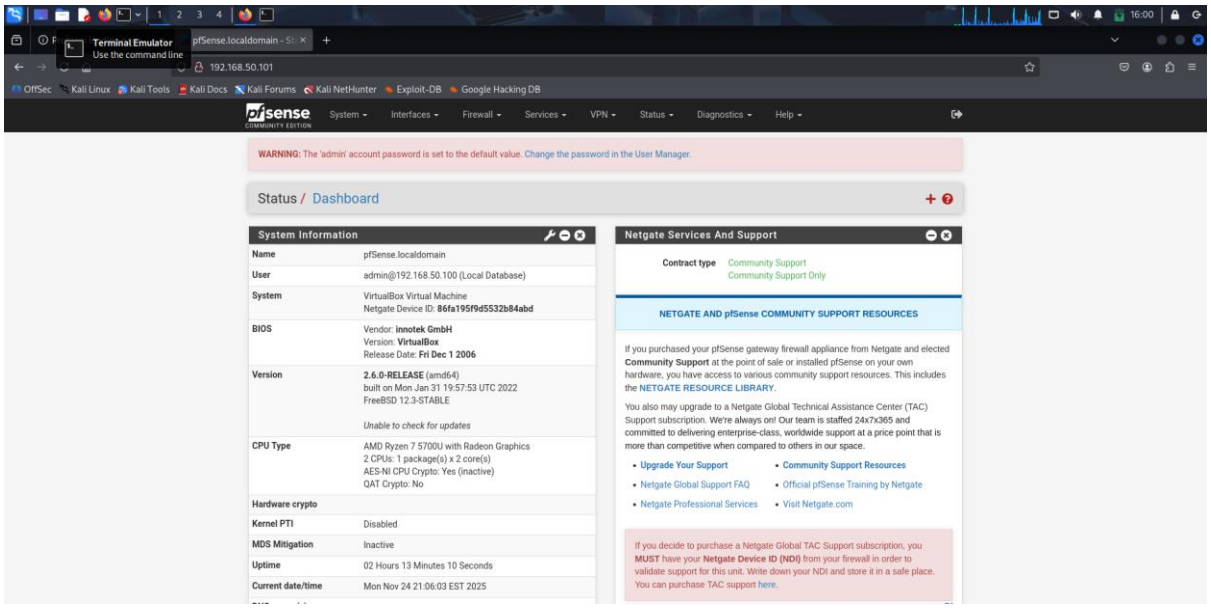


Figura 3



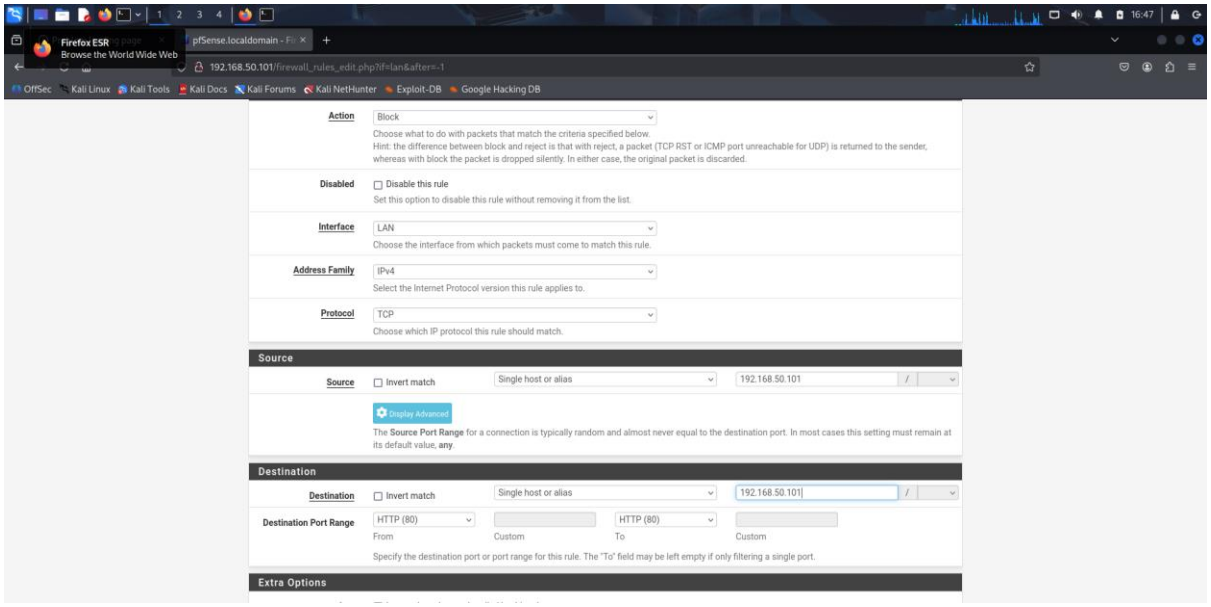
Si prosegue con la verifica su una pagina web nella quale è inserito l'ip 192.168.50.101 che rimanda alla home di Pfsense.



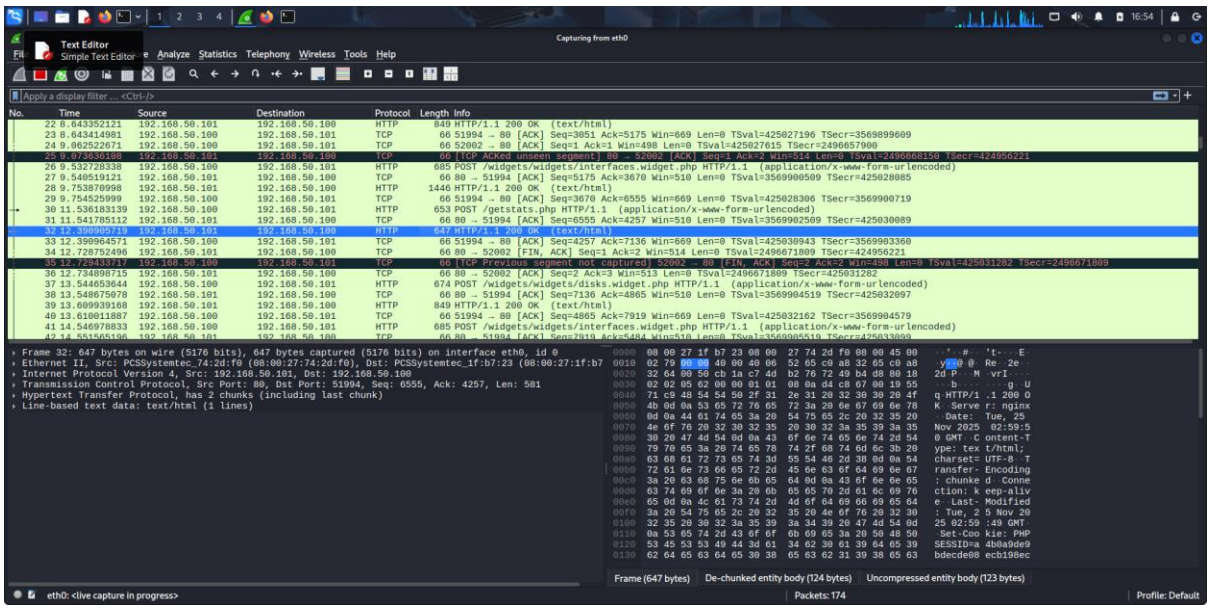


Si può creare da questo momento in avanti la regola per il firewall.

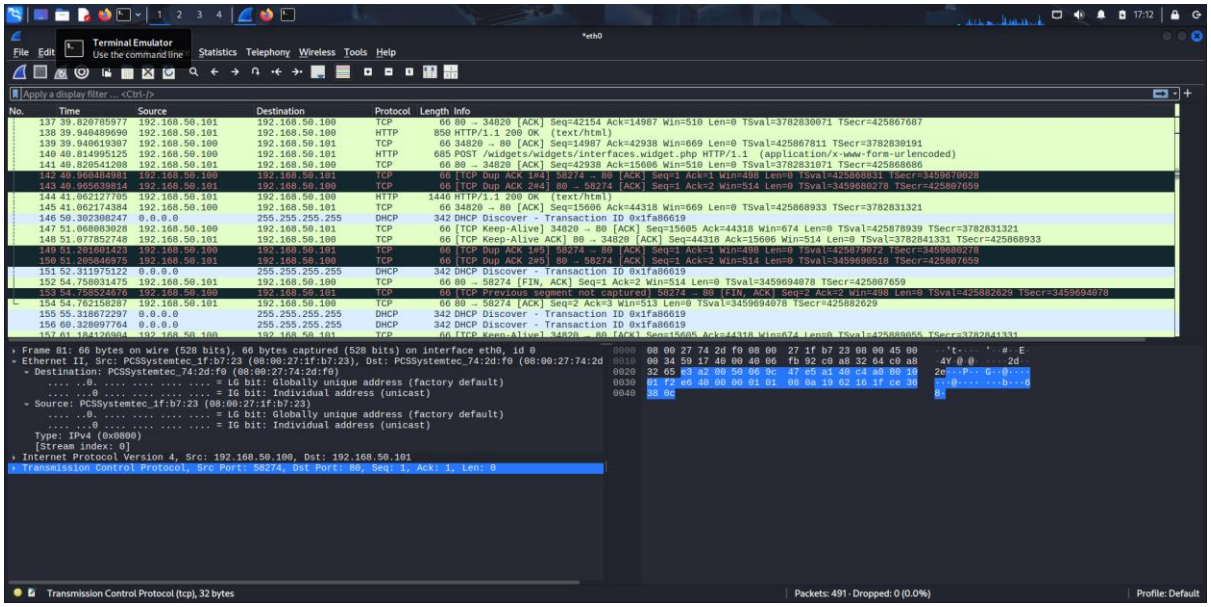
Sulla lan 2 (meta) bisogna abilitare il server dhcp e successivamente bloccare il traffico di pacchetti da kali a meta sulla porta 80. Flag sui log.



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
Use the command line
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
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 39.940489690 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 40.820541208 192.168.50.101 192.168.50.100 TCP 66 80 → 34820 [ACK] Seq=42938 Ack=15606 Win=510 Len=0 TSval=3782831071 TSecr=425868686
142 40.960484011 192.168.50.100 192.168.50.101 TCP 66 [TCP Dup ACK 1#4] 58274 → 80 [ACK] Seq=1 Ack=1 Win=498 Len=0 TSval=425868831 TSecr=3459670028
143 40.965639814 192.168.50.101 192.168.50.100 TCP 66 [TCP Dup ACK 2#4] 80 → 58274 [ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=3459680278 TSecr=425807659
144 41.062127705 192.168.50.101 192.168.50.100 HTTP 1446 HTTP/1.1 200 OK (text/html)
145 41.062174384 192.168.50.100 192.168.50.101 TCP 66 34820 → 80 [ACK] Seq=15606 Ack=44318 Win=669 Len=0 TSval=425868933 TSecr=3782831321
146 50.302308247 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x1fa86619
147 51.068083028 192.168.50.100 192.168.50.101 TCP 66 [TCP Keep-Alive] 34820 → 80 [ACK] Seq=15605 Ack=44318 Win=674 Len=0 TSval=425878939 TSecr=3782831321
148 51.077852748 192.168.50.101 192.168.50.100 TCP 66 [TCP Keep-Alive ACK] 80 → 34820 [ACK] Seq=44318 Ack=15606 Win=514 Len=0 TSval=3782841331 TSecr=425868933
149 51.201601423 192.168.50.100 192.168.50.101 TCP 66 [TCP Dup ACK 1#5] 58274 → 80 [ACK] Seq=1 Ack=1 Win=498 Len=0 TSval=425879072 TSecr=3459680278
150 51.205846975 192.168.50.101 192.168.50.100 TCP 66 [TCP Dup ACK 2#5] 80 → 58274 [ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=3459690518 TSecr=425807659
151 52.311975122 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x1fa86619
152 54.758031475 192.168.50.101 192.168.50.100 TCP 66 80 → 58274 [FIN, ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=3459694078 TSecr=425807659
153 54.758524678 192.168.50.100 192.168.50.101 TCP 66 [TCP Previous segment not captured] 58274 → 80 [FIN, ACK] Seq=2 Ack=2 Win=498 Len=0 TSval=425882629 TSecr=3459694078
154 54.762158287 192.168.50.101 192.168.50.100 TCP 66 80 → 58274 [ACK] Seq=2 Ack=3 Win=513 Len=0 TSval=3459694078 TSecr=425882629
155 55.318672297 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x1fa86619
156 60.328097764 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x1fa86619
157 61.184126904 192.168.50.100 192.168.50.101 TCP 66 [TCP Keep-Alive] 34820 → 80 [ACK] Seq=15605 Ack=44318 Win=674 Len=0 TSval=425889055 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:f0 (08:00:27:74:2d:f0)
Destination: PCSSystemtec_74:2d:f0 (08:00:27:74:2d:f0)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: PCSSystemtec_1f:b7:23 (08:00:27:1f:b7:23)
.... ..0. .... = LG 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: 58274, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 08 00 27 74 2d f0 08 00 27 1f b7 23 08 00 45 00
0010 00 34 59 17 40 00 40 06 fb 92 c0 a8 32 64 c0 a8
0020 32 65 e3 a2 00 50 00 9c 47 e5 a1 40 c4 a0 80 10
0030 01 f7 e6 40 00 00 01 01 08 0a 19 62 16 1f ce 36
0040 38 0c
Transmission Control Protocol (tcp), 32 bytes
Packets: 491 · Dropped: 0 (0.0%)
Profile: Default