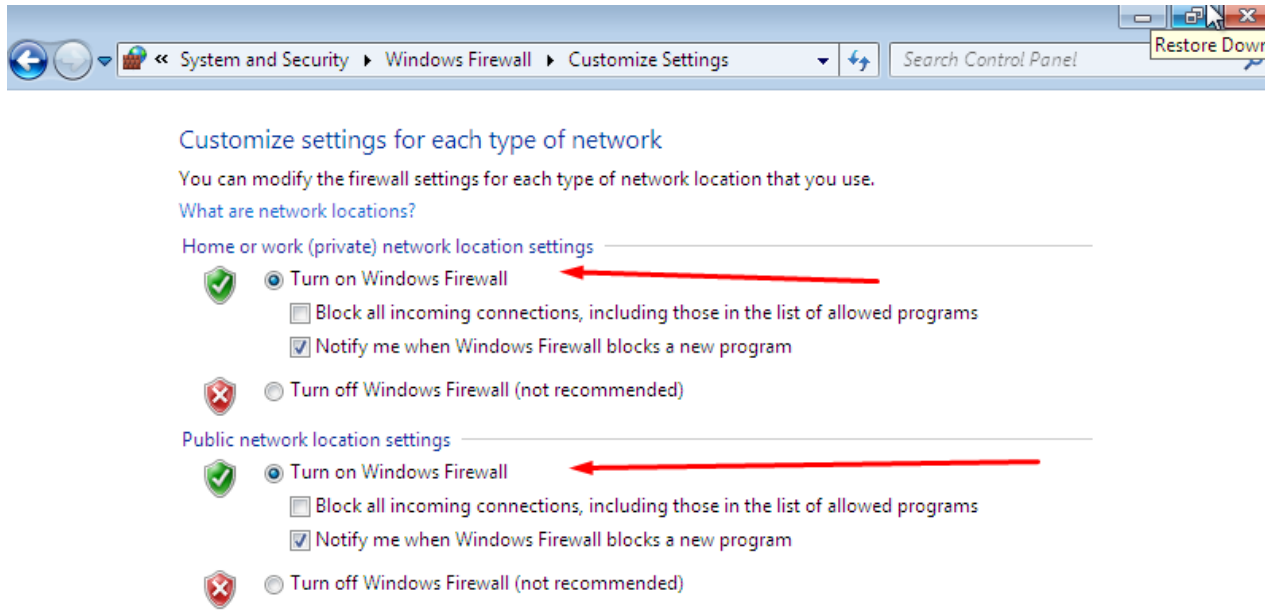


## Configurazione delle policy del Firewall e Spoofing Pacchetti con Wireshark

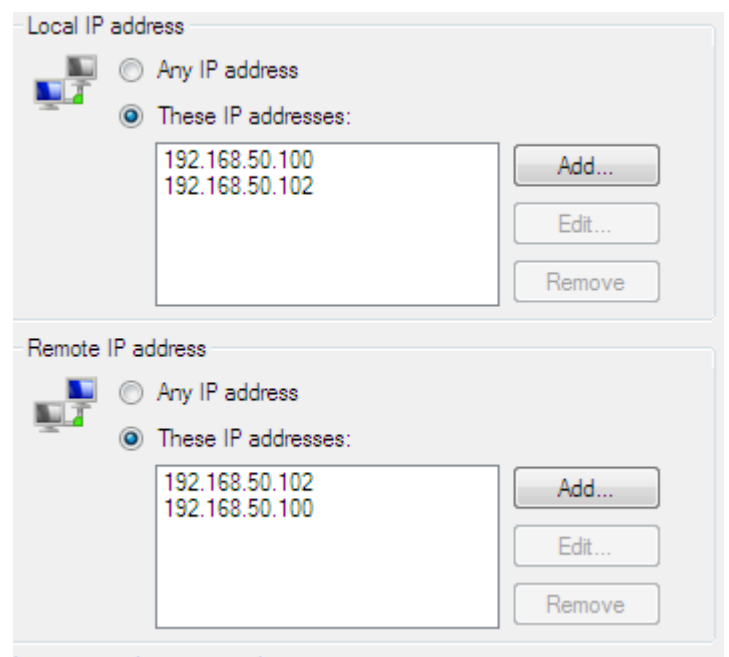
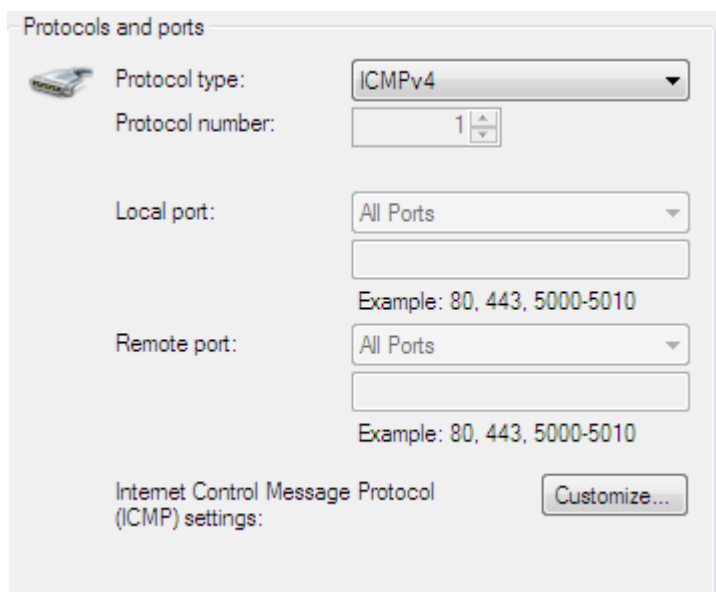
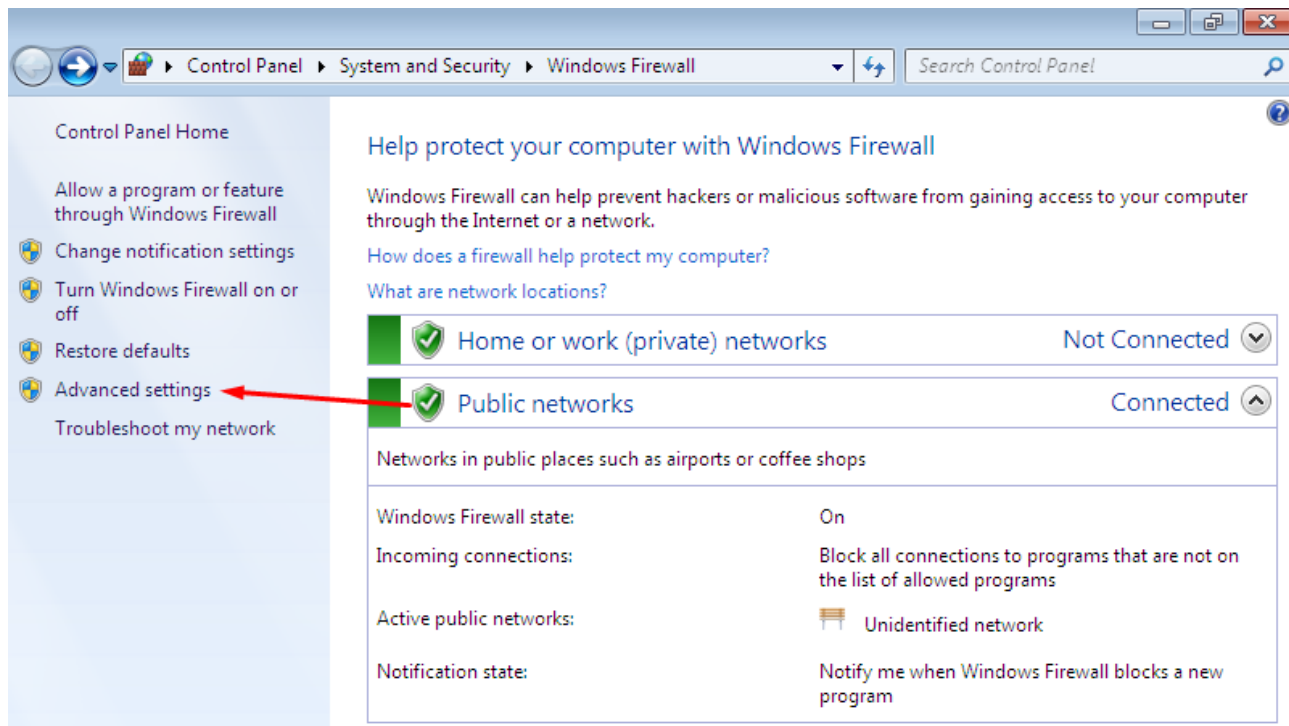
Iniziamo con l'impostare il Firewall in modalità ON:



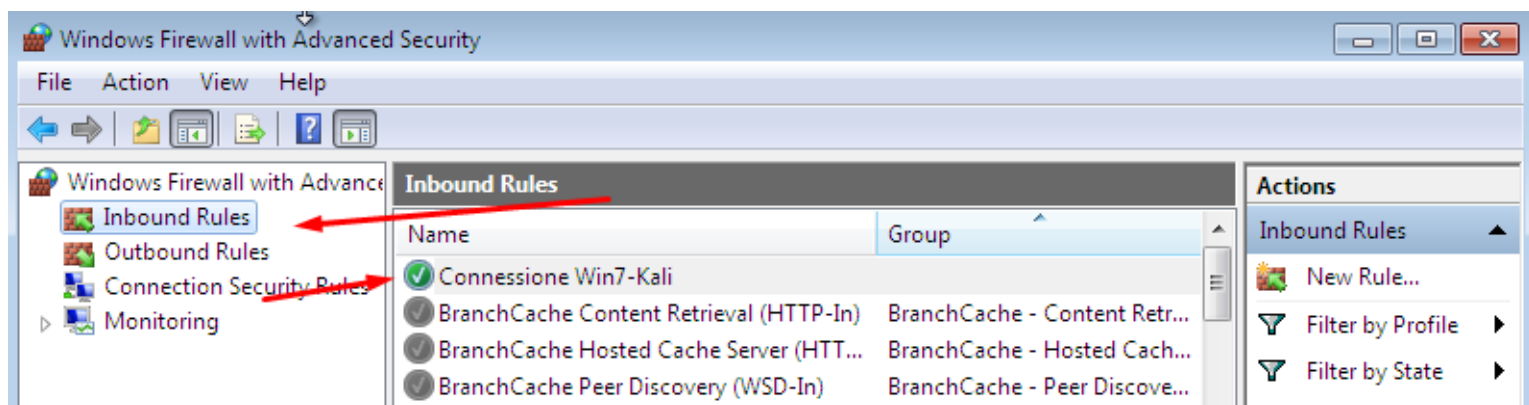
Se proviamo a pingare senza attivare queste due policy noteremo come i pacchetti non possono essere inviati:

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
[...]
```

Dopodiché si vanno ad impostare le policy:



Se si attiva la policy appena creata possiamo comunicare attraverso le due macchine.

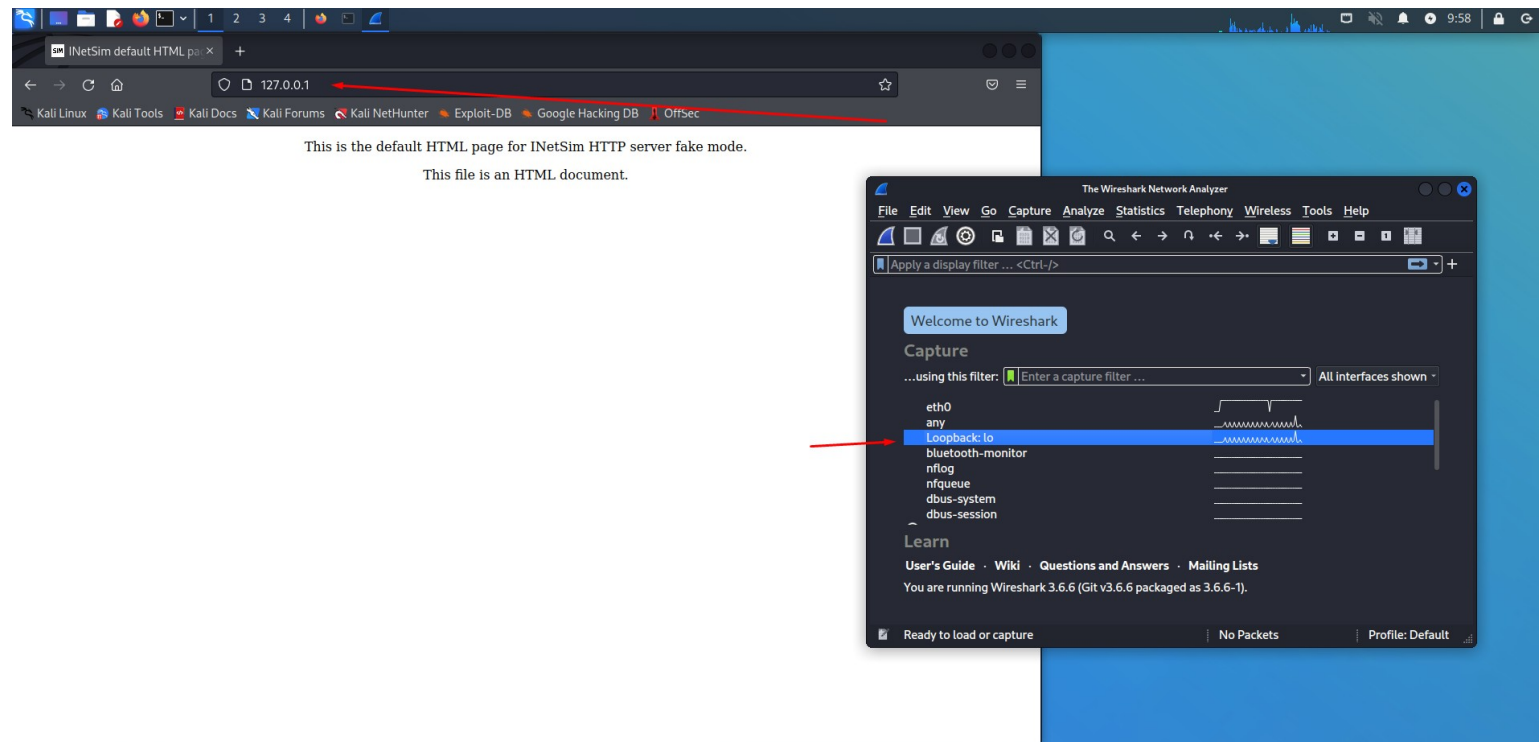


```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ping 192.168.50.102  
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.  
64 bytes from 192.168.50.102: icmp_seq=129 ttl=128 time=0.371 ms  
64 bytes from 192.168.50.102: icmp_seq=130 ttl=128 time=0.241 ms  
64 bytes from 192.168.50.102: icmp_seq=131 ttl=128 time=0.253 ms  
64 bytes from 192.168.50.102: icmp_seq=132 ttl=128 time=0.453 ms  
64 bytes from 192.168.50.102: icmp_seq=133 ttl=128 time=0.224 ms  
64 bytes from 192.168.50.102: icmp_seq=134 ttl=128 time=0.227 ms  
64 bytes from 192.168.50.102: icmp_seq=135 ttl=128 time=0.194 ms  
64 bytes from 192.168.50.102: icmp_seq=136 ttl=128 time=0.311 ms  
64 bytes from 192.168.50.102: icmp_seq=137 ttl=128 time=0.238 ms  
64 bytes from 192.168.50.102: icmp_seq=138 ttl=128 time=0.213 ms  
64 bytes from 192.168.50.102: icmp_seq=139 ttl=128 time=0.212 ms  
64 bytes from 192.168.50.102: icmp_seq=140 ttl=128 time=0.252 ms  
64 bytes from 192.168.50.102: icmp_seq=141 ttl=128 time=0.269 ms  
64 bytes from 192.168.50.102: icmp_seq=142 ttl=128 time=0.217 ms  
^Z  
zsh: suspended ping 192.168.50.102  
  
(kali@kali)-[~]  
$
```

Ora andiamo ad avviare il servizio **INETSIM** per simulare la connessione ad un server:

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo inetsim  
[sudo] password for kali:  
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg  
Using log directory: /var/log/inetsim/  
Using data directory: /var/lib/inetsim/  
Using report directory: /var/log/inetsim/report/  
Using configuration file: /etc/inetsim/inetsim.conf  
Parsing configuration file.  
Configuration file parsed successfully.  
≡ INetSim main process started (PID 8461) ≡  
Session ID: 8461  
Listening on: 127.0.0.1
```

Dopodiché avviamo Wireshark e Firefox, andando a digitare l'IP del server di INETSIM:



Infine, una volta avviato l'analisi dei pacchetti da Wireshark, possiamo notare l'invio di tutti i pacchetti della pagina.

The screenshot shows the Wireshark Network Analyzer window with the packet list pane expanded. The packet list shows 12 packets captured on the Loopback: lo interface. The packets are all from 127.0.0.1 to 127.0.0.1. The first packet is a SYN packet (Seq=0, Win=65495, Len=0). The second packet is an ACK packet (Seq=0, Ack=1, Win=65483, Len=0). The third packet is an ACK packet (Seq=1, Ack=1, Win=65536, Len=0). The fourth packet is a GET request (HTTP/1.1). The fifth packet is an ACK packet (Seq=1, Ack=441, Win=65152, Len=0). The sixth packet is a PSH, ACK packet (Seq=1, Ack=441, Win=65536, Len=150). The seventh packet is an ACK packet (Seq=441, Ack=151, Win=65408, Len=0). The eighth packet is an HTTP 200 OK response (text/html). The ninth packet is an ACK packet (Seq=441, Ack=409, Win=65152, Len=0). The tenth packet is a FIN, ACK packet (Seq=441, Ack=409, Win=65536, Len=0). The eleventh packet is a FIN, ACK packet (Seq=409, Ack=442, Win=65536, Len=0). The twelfth packet is an ACK packet (Seq=442, Ack=410, Win=65536, Len=0).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.1	TCP	74	51982 → 80 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=581821725 TSecr=0 WS...
2	0.000014757	127.0.0.1	127.0.0.1	TCP	74	80 → 51982 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=581821725...
3	0.000023982	127.0.0.1	127.0.0.1	TCP	66	51982 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=581821725 TSecr=581821725
4	0.000190515	127.0.0.1	127.0.0.1	HTTP	506	GET / HTTP/1.1
5	0.000194317	127.0.0.1	127.0.0.1	TCP	66	80 → 51982 [ACK] Seq=1 Ack=441 Win=65152 Len=0 TSval=581821725 TSecr=581821725
6	0.050960189	127.0.0.1	127.0.0.1	TCP	216	80 → 51982 [PSH, ACK] Seq=1 Ack=441 Win=65536 Len=150 TSval=581821776 TSecr=581821725 [...]
7	0.050990884	127.0.0.1	127.0.0.1	TCP	66	51982 → 80 [ACK] Seq=441 Ack=151 Win=65408 Len=0 TSval=581821776 TSecr=581821776
8	0.051001830	127.0.0.1	127.0.0.1	HTTP	324	HTTP/1.1 200 OK (text/html)
9	0.051004181	127.0.0.1	127.0.0.1	TCP	66	51982 → 80 [ACK] Seq=441 Ack=409 Win=65152 Len=0 TSval=581821776 TSecr=581821776
10	0.051167773	127.0.0.1	127.0.0.1	TCP	66	51982 → 80 [FIN, ACK] Seq=441 Ack=409 Win=65536 Len=0 TSval=581821776 TSecr=581821776
11	0.052457097	127.0.0.1	127.0.0.1	TCP	66	80 → 51982 [FIN, ACK] Seq=409 Ack=442 Win=65536 Len=0 TSval=581821777 TSecr=581821776
12	0.052473245	127.0.0.1	127.0.0.1	TCP	66	51982 → 80 [ACK] Seq=442 Ack=410 Win=65536 Len=0 TSval=581821777 TSecr=581821777