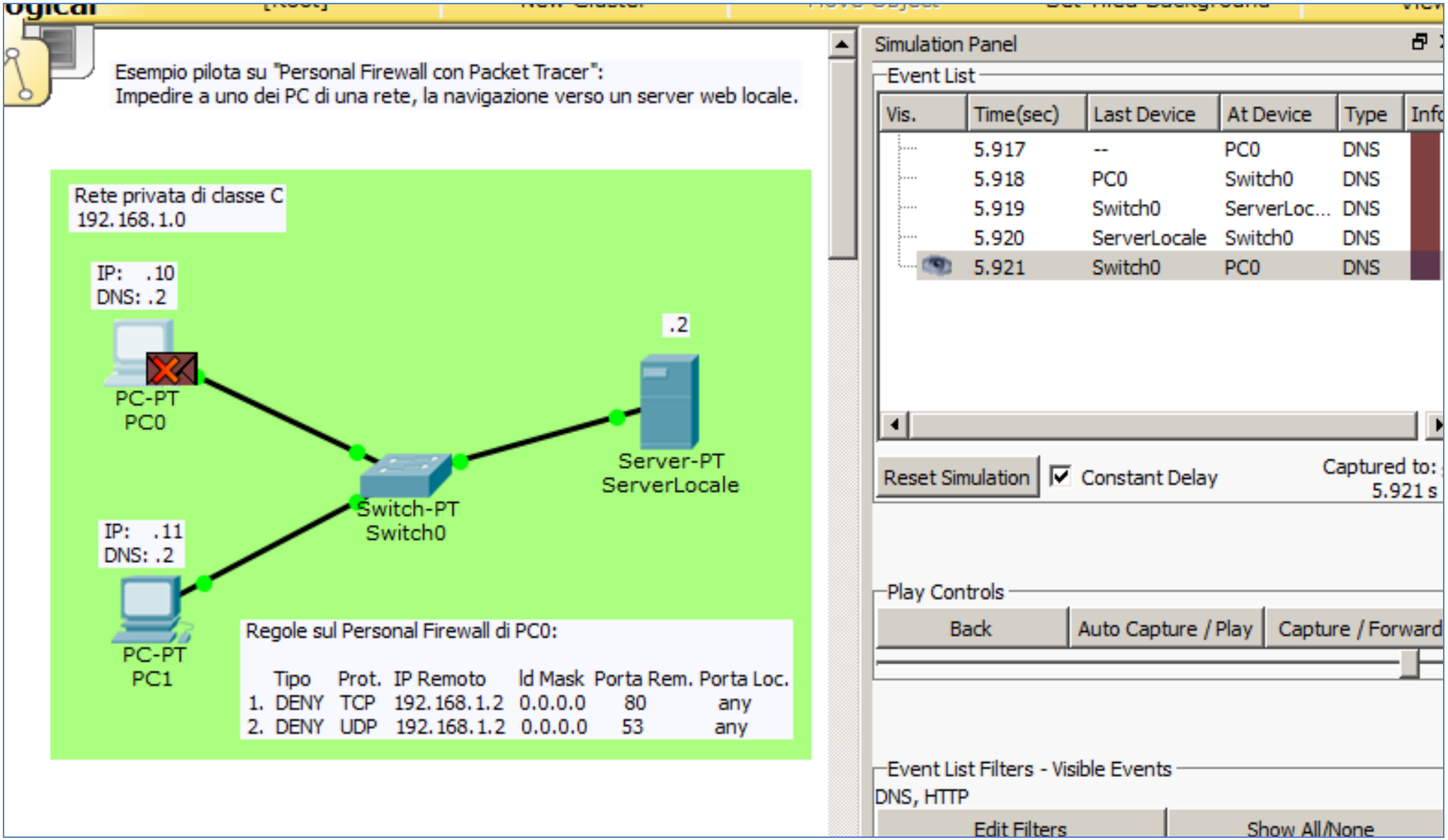
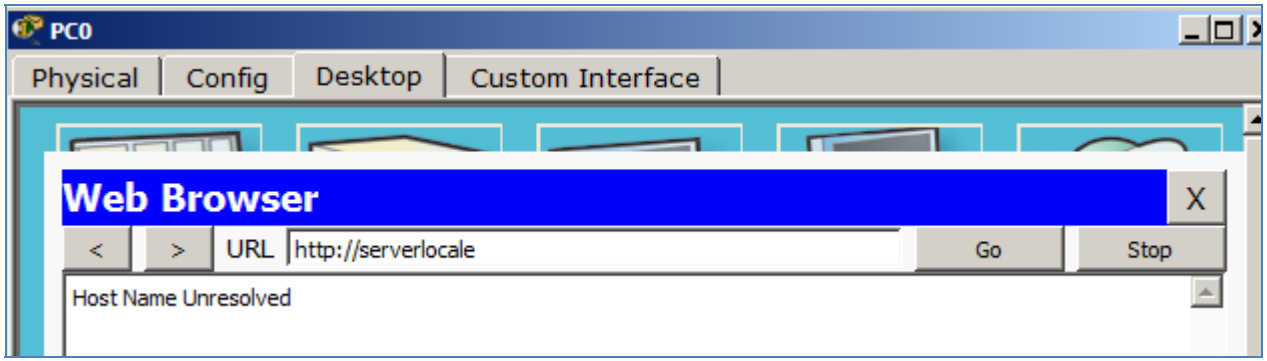
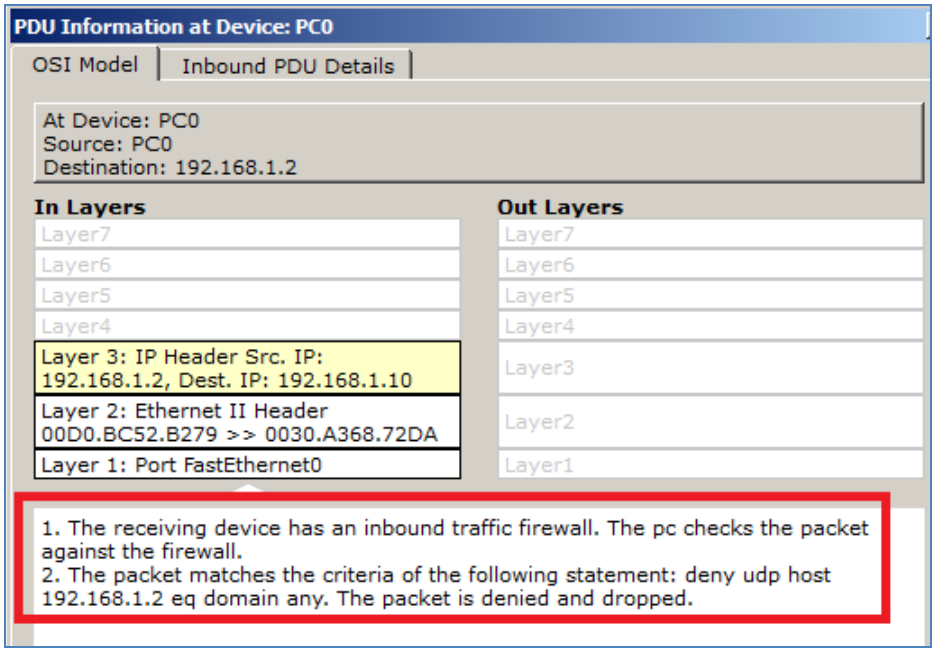
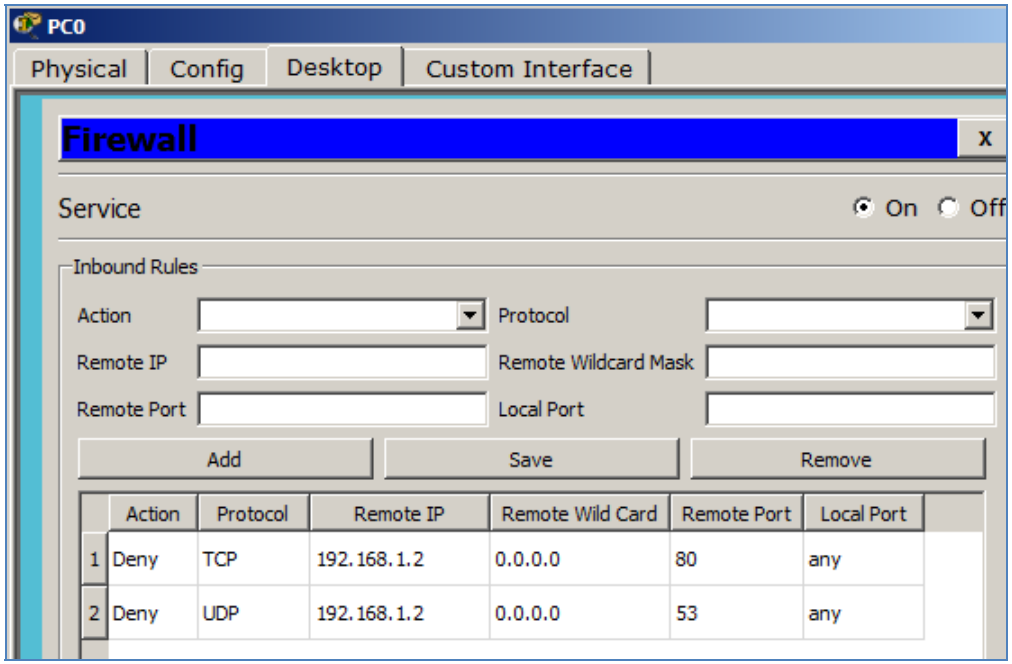

Esempio pilota su "Personal Firewall con Packet Tracer":
Impedire a uno dei PC di una rete, la navigazione verso un server web locale.
Rete privata di classe C
192.168.1.0
IP: .10
DNS: .2
PC-PT
PC0
.2
Server-PT
ServerLocale
Switch-PT
Switch0
IP: .11
DNS: .2
PC-PT
PC1
Regole sul Personal Firewall di PC0:
Tipo Prot. IP Remoto Id Mask Porta Rem. Porta Loc.
1. DENY TCP 192.168.1.2 0.0.0.0 80 any
2. DENY UDP 192.168.1.2 0.0.0.0 53 any
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type
5.917 -- PC0 DNS
5.918 PC0 Switch0 DNS
5.919 Switch0 ServerLoc... DNS
5.920 ServerLocale Switch0 DNS
5.921 Switch0 PC0 DNS
Reset Simulation
Constant Delay
Captured to:
5.921 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters - Visible Events
DNS, HTTP
Edit Filters
Show All/None


PC0
Physical
Config
Desktop
Custom Interface
Web Browser
X
<
>
URL
http://serverlocale
Go
Stop
Host Name Unresolved


PDU Information at Device: PC0
OSI Model
Inbound PDU Details
At Device: PC0
Source: PC0
Destination: 192.168.1.2
In Layers
Out Layers
Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.2, Dest. IP: 192.168.1.10
Layer 2: Ethernet II Header 00D0.BC52.B279 >> 0030.A368.72DA
Layer 1: Port FastEthernet0
Layer3
Layer2
Layer1
1. The receiving device has an inbound traffic firewall. The pc checks the packet against the firewall.
2. The packet matches the criteria of the following statement: deny udp host 192.168.1.2 eq domain any. The packet is denied and dropped.


PC0
Physical
Config
Desktop
Custom Interface
Firewall
X
Service
On
Off
Inbound Rules
Action
Protocol
Remote IP
Remote Wildcard Mask
Remote Port
Local Port
Add
Save
Remove
Action
Protocol
Remote IP
Remote Wild Card
Remote Port
Local Port
1
Deny
TCP
192.168.1.2
0.0.0.0
80
any
2
Deny
UDP
192.168.1.2
0.0.0.0
53
any