Security Labs in OPNET IT Guru

Enginyeria i Arquitectura La Salle

Universitat Ramon Llull

Barcelona 2004

Security Labs in OPNET IT Guru

Authors:

Cesc Canet

Juan Agustín Zaballos

Translation from Catalan:

Cesc Canet

Overview

This project consists in practical networking scenarios to be done with OPNET IT Guru Academic Edition, with a particular interest in security issues.

The first two parts are a short installation manual and an introduction to OPNET. After that there are 10 Labs that bring into practice different networking technologies. Every Lab consists in a theoretical introduction, a step-by-step construction of the scenario and finally Q&A referring to the issues exposed.

Lab 1: ICMP Ping, we study Ping traces and link failures.

Lab 2: Subnetting and OSI Model, we study tiers 1,2 and 3 of the OSI model, and the Packet Analyzer tool to observe TCP connections.

Lab 3: Firewalls, we begin with proxies and firewalls. We will deny multimedia traffic with a proxy, and study the link usage performance.

Lab 4: RIP explains the RIP routing protocol, and how to create timed link failures and recoveries.

Lab 5: OSPF compares RIP. We study areas and Load Balancing.

Lab 6: VPN studies secure non-local connections. A Hacker will try to access into a server that we will try to protect using virtual private networks.

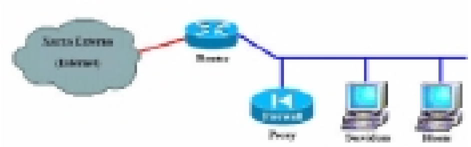
Lab 7: VLAN creates user logical groups with Virtual LANs. Studies One-Armed-Router interconnections.

Lab 8: Dual Homed Router/Host, **Lab 9: Screened Host/Subnet. DMZ** and **Lab 10: Collapsed DMZ** explains the static routing tables, ACLs, proxies and internal vs. perimetric security. Lab 10 is 100% practical, we want you to create it on your own, a piece of cake if you did the other Labs!

Lab 9: Screened Host / Subnet (DMZ)

Screened Host

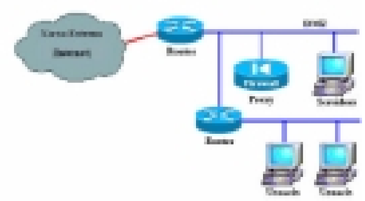
- Filtering at Layer-3 (packets) and Layer-5 (application)
- Packet filtering is performed by routers
- A Firewall (aka bastion host) at the internal network acts as a proxy and establishes external and internal connections
- Perimetrical security (incoming/outgoing messages)
- The router is used to limit the quantity of traffic to the bastion host, rejecting certain packets specified at the router's security policy



L9.1 Screened Host

Screened Subnet (DMZ)

- Perimetrical and internal security.
- The same router of Screened Host (external firewall) protects the server against external attacks.
- An additional router (internal firewall) protects the server against internal attacks.
- As a result we have a Demilitarized Zone (DMZ). All the traffic accessing this area has crossed a router (the external network traffic as well as the internal network traffic).
- Connections controlled by the proxy depend on the security level we want to obtain.



L9.2 Screened Subnet (DMZ)

Lab Description

First we create an scenario using Screened Host, and then a second scenario starting from the first using Screened Subnet (DMZ). We will create an internal network with an FTP, HTTP and DB Server, and an internal network with a DB and FTP Server, and a HTTP Server. We want to protect the internal DB and FTP Server against two kinds of attacks: internal and external. Additionally we want to permit the traffic to the HTTP internal server.

At last, we will do a few questions about the perimetric security against the internal security; the packets rejected by the proxy with/without ACLs at the internal network router, and it will be studied how the proxy manages the connections at the internal network, by studying the ping traces.

Creating the Scenario

1. Open a new Project in OPNET IT Guru Academic Edition (**File→ New Project**) using the following parameters (use default values for the remainder):

   - **Project Name: <your_name>_Screened**
   - **Scenario Name: ScreenedHost**
   - **Network Scale: Office**

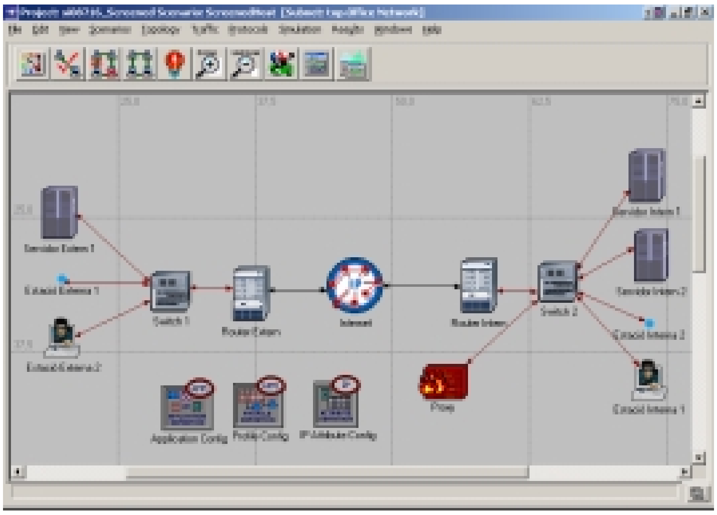
   Zoom + ZOOM the grid so we can maximize the scenario later if we need some more room

2. Deploy the following components on the scenario:

Qty	Component	Pallette	Description
1	ip_32_cloud	internet_toolbox	
1	Application Config	internet_toolbox	
1	Profile Config	internet_toolbox	
1	IP Attribute Config	internet_toolbox	
2	ethernet4_slip8_gtwy	internet_toolbox	
1	ethernet2_slip8_firewall	internet_toolbox	
2	ethernet16_switch	internet_toolbox	
4	Sm_Int_wkstn	Sm_Int_Model_List	
3	Sm_Int_Server	Sm_Int_Model_List	
	PPP_DS1	internet_toolbox	Links to Internet
	100BaseT	internet_toolbox	Remaining links

Figura L9.3 Components of our network

3. Place the components on the scenario as we can see in picture L9.2. Rename the nodes as seen in the picture, because we will refer to them by their name hereinafter. The Internal Station #1 can have its icon changed optionally, it will be a hacker in the internal network. External Station #2 will be a hacker in the external network as well.



L9.4 The completed scenario

4. Assigning IP addresses to all stations, interfaces and subinterfaces:
   Editing the Attributes for all stations and servers, we can change the IP address and network mask at **IP Host Parameters→Address** and **Subnet Mask**. For routers, **IP Routing Parameters→Interface Information→row *i*** will give us access to the same parameters for the interface IF *i*.

We will create 5 networks:

Interface	**Address/Subnet Mask**
Internal Network	213.180.1.0/24
External Network	194.179.95.0/24
Internet (to External Network)	190.50.50.0/24
Internet (to Internal Network)	190.40.40.0/24
Internal Router -Switch2-Proxy	190.30.30.0/24

L9.5 Networks in the scenario

We assign the addresses as seen in picture L9.6. We always use Subnet Mask 255.255.255.0.

Interface	**Address/Subnet Mask**
External Station #1	194.179.95.4/24
External Station #2	194.179.95.3/24
External Server #1	194.179.95.2/24
External Router – interface to Switch 1 (IF0)	194.179.95.1/24
External Router – interface to Internet (IF10)	190.50.50.1/24
Internet – interface to External Router (IF0)	190.50.50.2/24
Internet – interface to Internal Router (IF10)	190.40.40.1/24
Internal Router – interface to Internet (IF1)	190.40.40.2/24
Internal Router – interface to Switch 2 (IF0)	190.30.30.1/24
Internal Station #1	213.180.1.2/24
Internal Station #2	213.180.1.3/24
Internal Server #1	213.180.1.4/24
Internal Server #2	213.180.1.5/24
Proxy (IF0) – subinterface to Internal Network (IF0.1)	213.180.1.6/24
Proxy (IF0) – subinterface to Internal Router (IF0.2)	190.30.30.2/24

L9.6 Addresses for the network

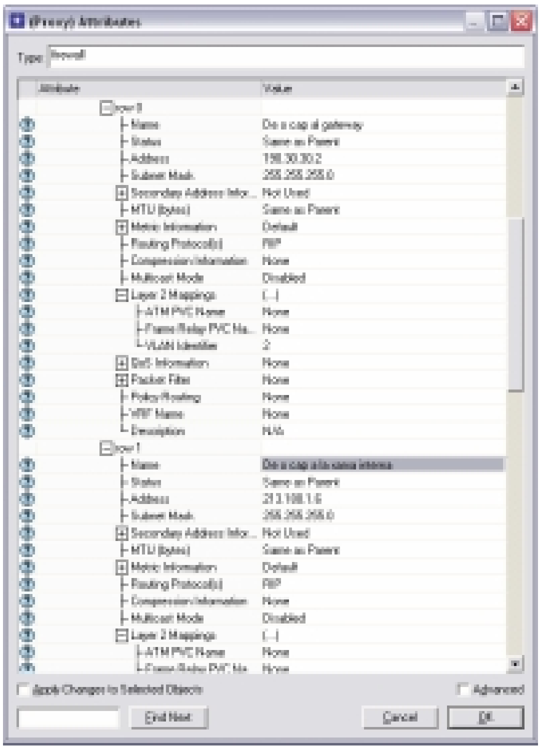
The values of the interface names depend on the device creation order.

The Proxy has two subinterfaces at the interface that is connected to Switch 2 (IF0). We can change it at the Proxy Attributes: **Interface Information→row**

i (*i* for the interface of Switch 2, *0* in our case)→**Subinterface Information→rows: 2**. Deploy both two subinterface branches and set the following parameters in both of them:

- **Name**: ***From/To Gateway*****, Address: 190.30.30.2, Subnet Mask: 255.255.255.0. Layer 2 Mappings→VLAN Identifier: 2** (so we have the same interface belonging to two networks simultaneously)
- **Name: *From/To Internal Network*, Address: 213.180.1.6, Subnet Mask: 255.255.255.0. Layer 2 Mappings→VLAN Identifier: 3**

We don't have to give an IP Address or Mask to the interface itself, we can set **Address: No IP Address** and **Subnet Mask: Auto Assigned**



(Proxy) Attributes

Type: firewall

Attribute	Value
⊟ row 0	
Name	De a cap al gateway
Status	Same as Parent
Address	190.30.30.2
Subnet Mask	255.255.255.0
⊞ Secondary Address Infor...	Not Used
MTU (bytes)	Same as Parent
⊞ Metric Information	Default
Routing Protocol(s)	RIP
Compression Information	None
Multicast Mode	Disabled
⊟ Layer 2 Mappings	(...)
ATM PVC Name	None
Frame Relay PVC Na...	None
VLAN Identifier	2
⊞ QoS Information	None
⊞ Packet Filter	None
Policy Routing	None
VRF Name	None
Description	N/A
⊟ row 1	
Name	De a cap a la xarxa interna
Status	Same as Parent
Address	213.180.1.6
Subnet Mask	255.255.255.0
⊞ Secondary Address Infor...	Not Used
MTU (bytes)	Same as Parent
⊞ Metric Information	Default
Routing Protocol(s)	RIP
Compression Information	None
Multicast Mode	Disabled
⊟ Layer 2 Mappings	(...)
ATM PVC Name	None
Frame Relay PVC Na...	None

□ Apply Changes to Selected Objects

□ Advanced

L9.7 Configuring the Proxy subinterfaces

5. Assigning a default gateway to stations and servers:

   We assign the default gateway of all stations and servers of network 213.180.1.0/24 pointing to the interface *From/To Internal Network* (213.180.1.6). This parameter is the one from **IP Host Parameters→Interface Information→Default Rout**e. We have to select **Internal Station #1, Internal Station #2, Internal Server #1, Internal Server #2** and change this **Attribute**. We check **Apply Changes To Selected Objects** to apply changes simultaneously on all nodes.

6. Configuring the Application Config control:

   Edit Attributes and set **Application Definitions: Default**.

7. Configuring the Profile Config control:

   Edit Attributes and create 3 profiles. Use default values for the remainder. The profiles are:

   - **HTTPProfile**, including the application **Web Browsing (Heavy HTTP 1.1)**
   - **FTPProfile**, including the application **File Transfer (Heavy)**
   - **DBProfile**, including the application **Database Access (Heavy)**

8. Assigning applications and services:

   We assign services supported by servers as seen in the table below:

Server	Services
External Server #1	File Transfer (Heavy), Web Browsing (Heavy HTTP 1.1), Database Access (Heavy)
Internal Server #1	Database Access (Heavy), File Transfer (Heavy)
Internal Server #2	Web Browsing (Heavy HTTP1.1)

L9.8 Services supported by servers

We have to change the **Attribute Application: Supported Services** on all servers.

9. Assigning profiles to the workstations:

   Assign the profiles supported by the workstations as seen in the table:

Station	Profiles
External Station #1	HTTPProfile
External Station #2	DBProfile, FTPProfile
Internal Station #1	FTPProfile, DBProfile
Internal Station #2	HTTPProfile, FTPProfile

L9.9 Station's profiles

We have to change the **Attribute Application: Supported Profiles** on all servers.

10. Assigning the Attribute Server Address on all servers:

Server	Server Address
External Server #1	SExt1HTTPFTPDB
Internal Server #1	SInt1FTPDB
Internal Server #2	SInt2HTTP

L9.10 Server Addresses of the servers

11. Assigning application demands:

We have to change the Attribute Application: Destination Preferences

Station	Symbolic Name	Actual Name
External Station #1	HTTP Server	SInt2HTTP
External Station #2	Database Server	SInt1FTPDB
	FTP Server	SInt1FTPDB
Internal Station #1	Database Server	SInt1FTPDB
	FTP Server	SInt1FTPDB
Internal Station #2	HTTP Server	SExt1HTTPFTPDB
	FTP Server	SExt1HTTPFTPDB

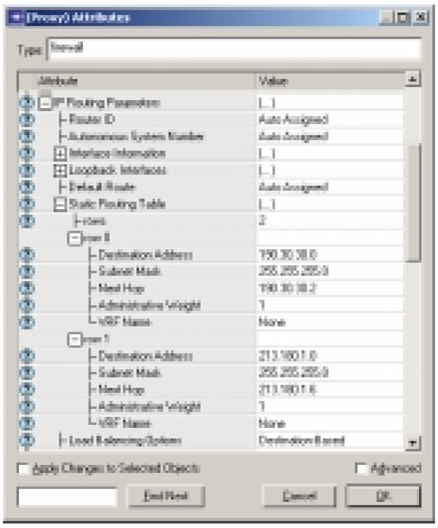
L9.11 Application Demands

12. Editing the static routing table and filtering rules of the Proxy:

We will do this device to:

- Receive IP packets of the internal network sent to Internet, and resend them to the gateway (Internal Router) to be sent to the Internet.
- Receive the IP packets that Internal Router sends from the Internet sent to the internal network and resend them to the final station of the internal network.
- In both cases, perform a proxy filtering (Layer 5).

The two first points will be achieved by editing the static routing table, accessible through **IP Routing Parameters→Static Routing Table**. At the following table we can see the routing table configured.

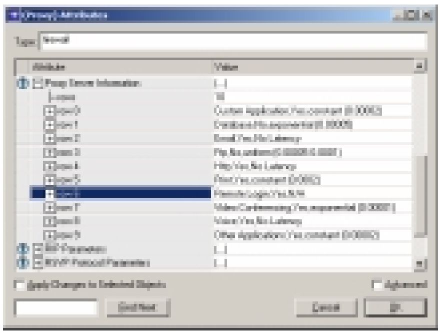


Type: firewall

Attribute	Value
IP Routing Parameters	(...)
Router ID	Auto Assigned
Autonomous System Number	Auto Assigned
Interface Information	(...)
Loopback Interfaces	(...)
Default Route	Auto Assigned
Static Routing Table	(...)
rows	2
row 0	
Destination Address	190.30.38.0
Subnet Mask	255.255.255.0
Next Hop	190.30.38.2
Administrative Weight	1
VRF Name	None
row 1	
Destination Address	213.180.1.0
Subnet Mask	255.255.255.0
Next Hop	213.180.1.6
Administrative Weight	1
VRF Name	None
Load Balancing Options	Destination Based

L9.12 Static Routing Table of the Proxy

We will configure the proxy as well in order to deny the traffic from the FTP and Database service from the internal network. We need to modify the Proxy Server Information hierarchy to have **Proxy Server Deployed: No** at Database, and permit the rest.



Type: firewall

Attribute	Value
Proxy Server Information	(...)
rows	10
row 0	Custom Application,Yes,constant (0.0002)
row 1	Database,No,exponential (0.0005)
row 2	Email,Yes,No Latency
row 3	Ftp,No,uniform (0.0005,0.0001)
row 4	Http,Yes,No Latency
row 5	Print,Yes,constant (0.0002)
row 6	Remote Login,Yes,N/A
row 7	Video Conferencing,Yes,exponential (0.0001)
row 8	Voice,Yes,No Latency
row 9	Other Applications,Yes,constant (0.0002)
RIP Parameters	(...)
RSVP Protocol Parameters	(...)

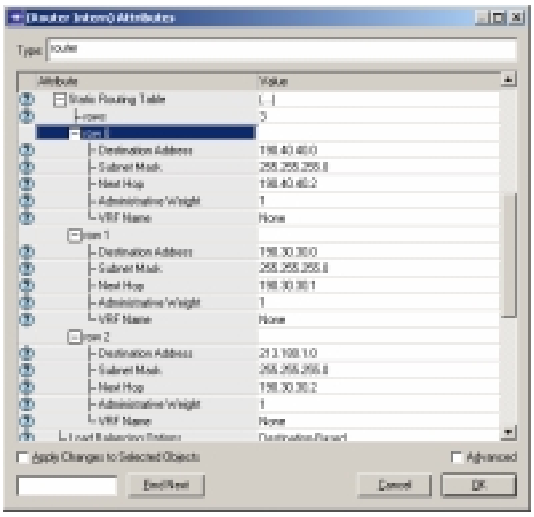
L9.13 Configuring the proxy

13. Editing the static routing table of Internal Router:

    We will make this device to:

    - Receive IP packets from the Proxy (coming from the internal network) and resend them to the Internet
    - Receive packets from the Internet with destination to the internal network, and resend them to the Proxy
    - In both cases, perform a layer-3 packet filtering with ACLs.
    - Reject packets received directly from the internal network (it is mandatory to go across the 2 routers for the in-out and out-in communication). This can be done with VLANs.

At picture L9.14 we can see the configuration of the static routing table, and at picture L9.15 the ACL configuration.



(Router Intern) Attributes

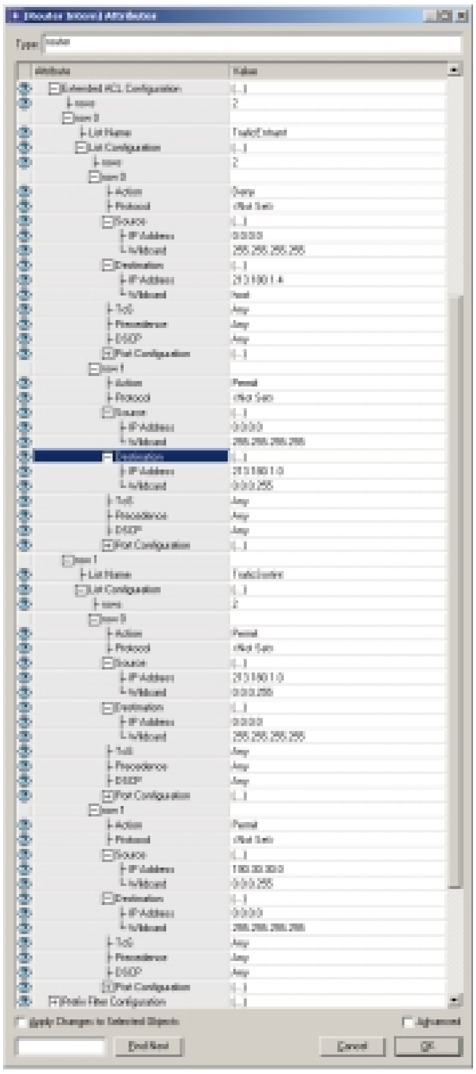
Type: router

Attribute	Value
Static Routing Table	(...)
rows	3
row 0	
Destination Address	198.40.40.0
Subnet Mask	255.255.255.0
Next Hop	198.40.40.2
Administrative Weight	1
VRF Name	None
row 1	
Destination Address	198.30.30.0
Subnet Mask	255.255.255.0
Next Hop	198.30.30.1
Administrative Weight	1
VRF Name	None
row 2	
Destination Address	213.108.1.0
Subnet Mask	255.255.255.0
Next Hop	198.30.30.2
Administrative Weight	1
VRF Name	None
Load Balancing Options	Destination-Based

☐ Apply Changes to Selected Objects ☐ Advanced

L9.14 Static Routing Table at Internal Router

We have to assign ACL tables to the interfaces: **IP Routing Parameters→Interface Information→row 1** (the one with the interface to Internet)**→Packet Filter→Send Filter: OutgoingTraffic** and **Receive Filter: IncomingTraffic**. For the internal network (IF0), we invert the order.



Attribute	Value
Extended ACL Configuration	(...)
rows	2
row 0	
List Name	TraficEntrant
List Configuration	(...)
rows	2
row 0	
Action	Deny
Protocol	(Not Set)
Source	(...)
IP Address	0.0.0.0
Wildcard	255.255.255.255
Destination	(...)
IP Address	213.180.1.4
Wildcard	host
ToS	Any
Precedence	Any
DSCP	Any
Port Configuration	(...)
row 1	
Action	Permit
Protocol	(Not Set)
Source	(...)
IP Address	0.0.0.0
Wildcard	255.255.255.255
Destination	(...)
IP Address	213.180.1.0
Wildcard	0.0.0.255
ToS	Any
Precedence	Any
DSCP	Any
Port Configuration	(...)
row 1	
List Name	TraficSortint
List Configuration	(...)
rows	2
row 0	
Action	Permit
Protocol	(Not Set)
Source	(...)
IP Address	213.180.1.0
Wildcard	0.0.0.255
Destination	(...)
IP Address	0.0.0.0
Wildcard	255.255.255.255
ToS	Any
Precedence	Any
DSCP	Any
Port Configuration	(...)
row 1	
Action	Permit
Protocol	(Not Set)
Source	(...)
IP Address	190.30.30.0
Wildcard	0.0.0.255
Destination	(...)
IP Address	0.0.0.0
Wildcard	255.255.255.255
ToS	Any
Precedence	Any
DSCP	Any
Port Configuration	(...)
Prefix Filter Configuration	(...)

L9.15 Internal Router ACL

14. Setting up the VLAN at the internal network:

For the Proxy to work with many subinterfaces in the same interface we need each subinterface to belong to a different network, and this can be done with VLANs. We create two simple VLANs, the first one with VLAN Identifier: 2 (network 190.30.30.0/24) and the second one with VLAN Identifier 3 (network 213.180.1.0/24).

We assign the VLAN Identifiers as seen in the following table to the internal network's interfaces. Remember that this parameter can be accessed through **IP Host Parameters→Interface Information→Layer 2 Mappings→VLAN Identifier** for the workstations; and **IP Routing Parameters→Interface Information→row *i*** (*i* for the interface)**→Layer 2 Mappings→VLAN Identifier** for routers.

Interface	**VLAN Identifier**
Internal Router -interface to Switch 2 (IF0)	3
Proxy – subinterface From/To gateway	3
Proxy –subinterface From/To Internal Network	2
Internal Station #1	2
Internal Station #2	2
Internal Server #1	2
Internal Server #2	2

L9.16 VLAN Identifiers

We assign also this parameters to *Switch 2* to configure the VLAN. The port values are the ones we had, and they depend on the creation order.

Port	**Port Type**	**Port VLAN Id.**	**Supported VLANs**
Interface to Internal Router (P0)	Access	2	2
Interface To Proxy (P13)	Trunk	1	1,2,3
Interface to Internal Station #1 (P1)	Access	3	3
Interface to Internal Station #2 (P10)	Access	3	3
Interface to Internal Server #1 (P11)	Access	3	3
Interface to Internal Server #2 (P12)	Access	3	3

L9.17 Configuring VLAN at Switch 2

This information is at **Switch Port Configuration→row *i*** (*i* for the interface)**→VLAN Parameters**.

We have to configure besides of this the parameter **VLAN Parameters→Supported VLANs** to support VLANs 1,2 and 3 (**Name: Default**, **Gateway** and **InternalNetwork** respectively), and **VLAN Parameters→Scheme: Port-Based VLANs**.

Setting up the simulation

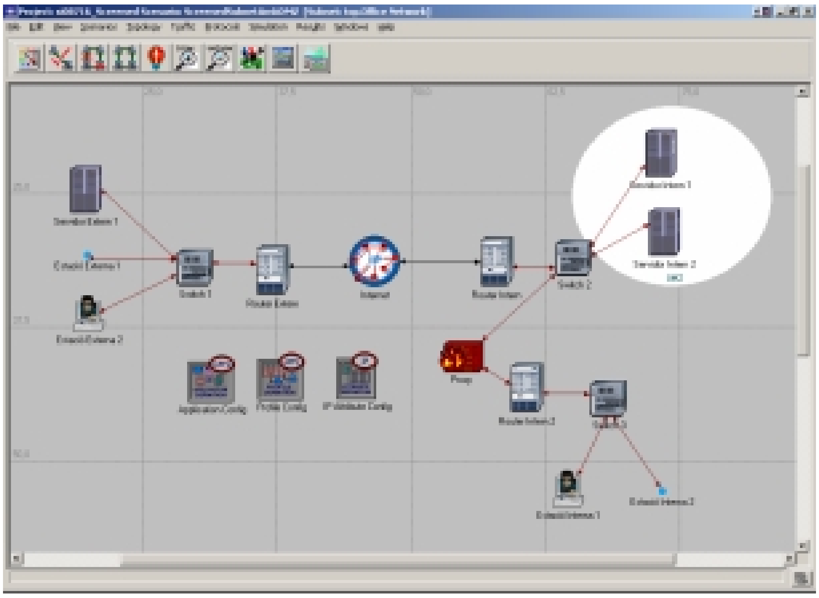
- Select the statistic **IP Traffic Dropped (packets/sec)** at **Proxy**. (**right click→Choose Individual Statistics**).
- This way we can see the amount of traffic rejected by the proxy.
- We click on **Configure/run simulation** , and set the parameter **Duration: 15 minute(s)**. We click on **OK** (don't start the simulation yet).

Creating the second scenario

1. Duplicate the scenario:

   From the Project Editor and with the scenario opened, **Scenarios→Duplicate Scenario…** Call the new scenario **Scenario Name: ScreenedSubnetWithDMZ**.

   The new scenario is the same as we have so far, but this time the internal stations will be connected to *Switch 2* through a ethernet_4_slip8_gtwy router (at internet_toolbox pallette), which will link them to the Proxy. The internal users will be at a switched LAN with ethernet16_switch (at internet_toolbox palette). The new link's wires will use 100BaseT (at Links palette). The servers layout will be the same as we have (DMZ).



L9.18 The scenario ScreenedSubnetWithDMZ

2. Assigning IP addresses again:

   Create the network 213.190.1.0/25, separated of 213.180.1.0 (only servers will be at here now). Now this network is called Demilitarized Zone (DMZ) because is isolated from external and internal attacks. Another network is created: 190.20.20.0/24, between *Internal Router #2* and *Proxy*.

The new IP addresses are:

Interface	**IP Address**
Internal Station #1	213.190.1.2
Internal Station #2	213.190.1.3
Internal Router #2 – interface to Switch 3 (IF0)	213.190.1.1
Internal Router #2 – interface to Proxy (IF1)	190.20.20.1
Proxy – interface to Internal Router #2 (IF1)	190.20.20.2

L9.19 New IP addresses

Once again the interfaces in brackets are the ones we had, but they can be different from yours depending on the creation order of the links on the grid.

3. Assigning an ACL to Internal Router #2:

The security policy of our network still being the same: we have to avoid access to Internal Server #1 (FTP and DB server). We will create an ACL at *Internal Router #1* using the information of picture L9.20, where:

- The *IncomingTrafficAtDMZ* list denies all traffic sent to *Internal Server #1* (213.180.1.4) and permits all the remaining traffic.
- The *OutgoingTrafficFromDMZ* denies outgoing traffic from Internal Server #1, but permits the remaining outgoing traffic.

List Name	**Action**	**Source**	**Destination**
IncomingTrafficToDMZ	Deny	*	213.180.1.4/host
	Permit	*	213.180.1.0/24
	Permit	*	*
OutgoingTrafficFromDMZ	Deny	213.180.1.4/host	*
	Permit	*	*

L9.20 ACL of Internal Router #2

4. Assigning ACLs to interfaces at Internal Router #2.

- Interface to Proxy (IF1). **Send Filter: IncomingTrafficToDMZ** , **Receive Filter: OutgoingTrafficFromDMZ**.
- Interface to Switch3 (IF0). **Send Filter: OutgoingTrafficFromDMZ, Receive Filter: IncomingTrafficToDMZ**.

5. Creation of the routing table of Internal Router #2, and modification of the routing tables of Internal Router #1 and Proxy.

   - For the Internal Router #2, **Destination: 190.20.20.0/24 Next Hop: 190.20.20.1; Destination: 213.190.1.0/24 Next Hop: 213.190.1.1** and **Default: 190.20.20.2**.
   - For the Proxy, we add a new entry: **Destination: 213.190.1.0/24 Next Hop: 190.20.20.1**.
   - For the Internal Router #1, we add a new entry: **Destination: 213.190.1.0/24 Next Hop: 190.30.30.2**.
   - Assignation of the default route to Internal Station #1 and Internal Station #2 pointing to 213.190.1.1.

6. Reprogramming the ACL of the Internal Router:

   We have to modify slightly the ACLs of the outgoing and incoming traffic to allow the traffic pass from/to the new networks we have just created, 213.190.1.0/24 (to the new internal network) and 190.20.20.0/24 (the router between Internal Router #2 and the Proxy). At picture L9.21 we can see the new ACLs we have to program at Internal Router (the remainder parameters are left with default values).

List Name	Action	Source	Destination
IncomingTraffic	Deny	*	213.180.1.4/host
	Permit	*	213.180.1.0/24
	Permit	*	213.190.1.0/24
	Permit	*	190.20.20.0/24
OutgoingTraffic	Permit	213.190.1.0/24	*
	Permit	190.20.20.0/24	*
	Permit	213.180.1.0/24	*
	Permit	190.30.30.0/24	*

L9.21 Adding up new conditions to the ACL

7. Executing the simulation:

   From the Project Editor, **Scenarios→Manage Scenarios**. We check all the scenarios with **<collected>** at the **Results** field and press **OK**.

Questions

Q1 At the scenario ScreenedHost, create a new ping from External Station #1 to Internal Server #2 with Ping Pattern: Record Route. Take a look at the ping trace at the Simulation Log. What do you observe?

Q2 Duplicate the scenario ScreenedHost and call the new scenario ScreenedHostQ2. Create a new ping from External Station #1 to Internal Station #1 (Record Route).

At the new scenario, change the default route of Internal Station #1 pointing to 190.30.30.1 (Internal Router – interface to Switch 2). Run the simulation and analyze the frame of the pings at Q1. Is it possible to avoid the Firewall this way?

Q3 Duplicate the scenario ScreenedHost and call the new scenario ScreenedHostQ3. Disable the ACLs we have programmed at Internal Router (the fastest way for doing so is to set *rows:0* at the field *IP Routing Parameters→Extended ACL Configuration*). Run the simulation and compare the statistic *IP→Traffic Dropped (packets/sec)* in the Proxy at the scenarios ScreenedHost and ScreenedHostQ3. What conclusions do you get?

Q4 Fill up the following table, taking the information from the Simulation Log of the traffic demands at Internal Server #1 (traffic from the DB or FTP). Write down if the destination is reached or not.

Scenario	**Internal Station #1**	**External Station #2**
ScreenedHost		
ScreenedSubnetAmbDMZ		

What can we say about the security in both schemes? (Remember that any of the two stations are allowed to use the services of FTP and Database at *Internal Server #1*, and *Internal Station #1* and *External Station #2* are hackers).

Answers

Q1 The interesting thing is to notice that all the traffic between the internal network and the external network go necessarily across the router and firewall.

```
IP Address     Hop Delay     Node Name
----------     ---------     ---------
194.179.95.4    0,00000      Office Network.External Station #1
190.50.50.1     0,00005      Office Network.External Router
192.0.0.1       0,00070      Office Network.Internet
190.30.30.1     0,00068      Office Network.Internal Router
213.180.1.6     0,00005      Office Network.Proxy
213.180.1.5     0,00005      Office Network.Internal Server #2
213.180.1.5     0,00001      Office Network.Internal Server #2
190.30.30.2     0,00004      Office Network.Proxy
192.0.0.2       0,00005      Office Network.Internal Router
190.50.50.2     0,00070      Office Network.Internet
194.179.95.1    0,00068      Office Network.External Router
194.179.95.4    0,00005      Office Network.External Station #1
```

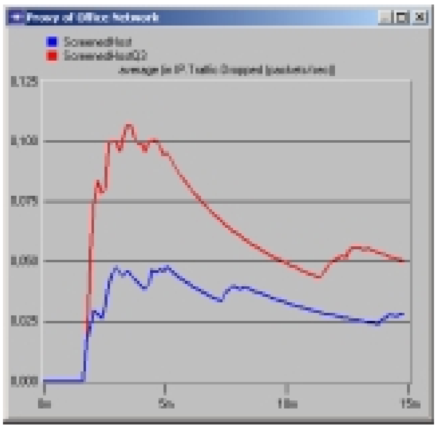
L9.22 Ping

Q2 It is impossible for an Internal Station to avoid the bastion host changing the default gateway.

```
IP Address     Hop Delay     Node Name
----------     ---------     ---------
194.179.95.4    0,00000      Office Network.Estació Externa 1
190.50.50.1     0,00006      Office Network.Router Extern
192.0.0.1       0,00137      Office Network.Internet
190.30.30.1     0,00068      Office Network.Router Intern
213.180.1.6     0,00005      Office Network.Proxy
213.180.1.2     0,00005      Office Network.Estació Interna 1
213.180.1.2     0,00001      Office Network.Estació Interna 1
190.30.30.2     0,00004      Office Network.Proxy
192.0.0.2       0,00005      Office Network.Router Intern
190.50.50.2     0,00070      Office Network.Internet
194.179.95.1    0,00068      Office Network.Router Extern
194.179.95.4    0,00005      Office Network.Estació Externa 1
```

L9.23 It is not possible to avoid the Proxy

Q3 We observe that the traffic load rejected by the proxy increases if the ACLs of the router are disabled because this traffic use to be rejected by the router, i.e., connections to the Internal Server #1.



L9.24 The ACL helps to reduce the load on the Proxy

Q4 The interesting thing is to compare the perimetric security offered by Screened Host with the perimetric security and internal security as well offered by DMZ.

Scenario	Internal Station #1	External Station #2
ScreenedHost	Yes	No
ScreenedSubnetAmbDMZ	No	No

L9.25 Internal attacks can be avoided only with DMZ