

CheckPoint Software Technologies LTD.ä

How to Configure Firewall-1 With Connect Control

(Load-Balance across multiple servers)

Event: Partner Exchange Conference

Date: October 10, 1999

Revision 1.0

Author: Victor Bojorquez

Credits:

Load Balancing

Description:

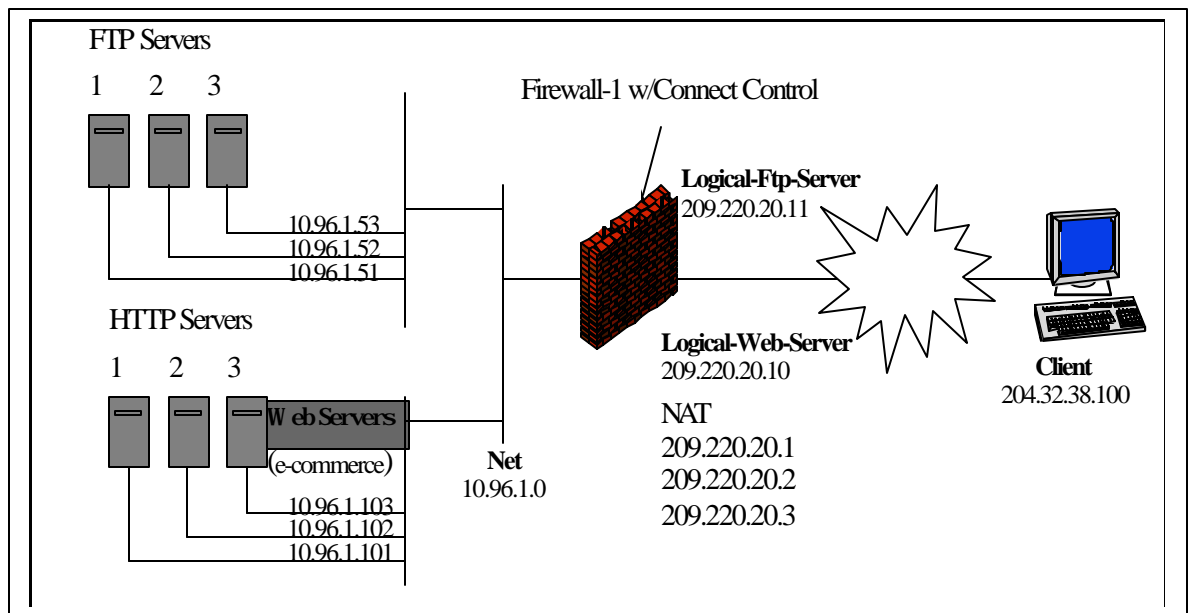
Load Balancing allows several servers in one network to share and distribute the load among themselves, while being protected by FireWall-1. This reduces the load to any one server and helps the security engineer manage network traffic from FireWall-1.

Overview:

In this example, we will configure Load-Balancing with the Round Trip algorithm. The network that the servers are located on is a non-routable network. Therefore, Static Network Address Translation will be required.

When a client initiates communication with a Logical Server, *HTTP redirects* sends HTTP redirects to direct the communication to the proper physical server, via the load-balancing daemon. The daemon notifies the client that subsequent connections should be directed to the IP address of the (physical) server, rather than the IP address of the logical server. The remainder of the session is conducted without the load-balancing daemon's intervention.

Load Balance with Web Servers and FTP Servers



Goal of the Demo:

- Demonstrate the Load Balancing features of FireWall-1.
- Demonstrate how to create an HTTP logical Server
- Describe how an FTP logical server performs load-balancing

Load Balancing Components:

- Connect Control Module
- Load Balancing daemon (LHTTPD)
- Load Balancing algorithm

Connect Control Module

The Connect Control Module is the FireWall-1 Module containing the load balancing algorithm. This algorithm determines which server will receive a request.

Load Balancing Daemon:

This daemon resides on the firewalled server. Its purpose is to redirect requests to make a Web browser initiate a new connection to a physical server's IP address. Once a client has established a connection and the load balancing daemon has determined that the incoming packet must be load balanced, the remainder of the client's communication is done without the load balancing daemons intervention.

Load Balancing Algorithms

Whenever the FireWall Module sees a request to a logical server's IP address, the FireWall-1 load-balancing algorithm determines which physical server will receive the request. There are five load balancing algorithms from which to choose.

1. Server Load – determines the load of each physical server (requires load-measuring agent on each physical server)
2. Round Trip
3. Round Robin
4. Random
5. Domain – chooses the physical server closest to the client based on domain name. (HTTP only)

HTTP Redirect example:

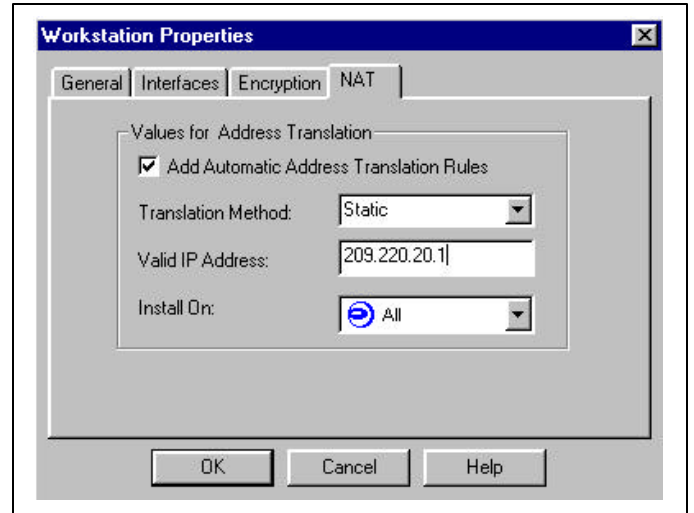
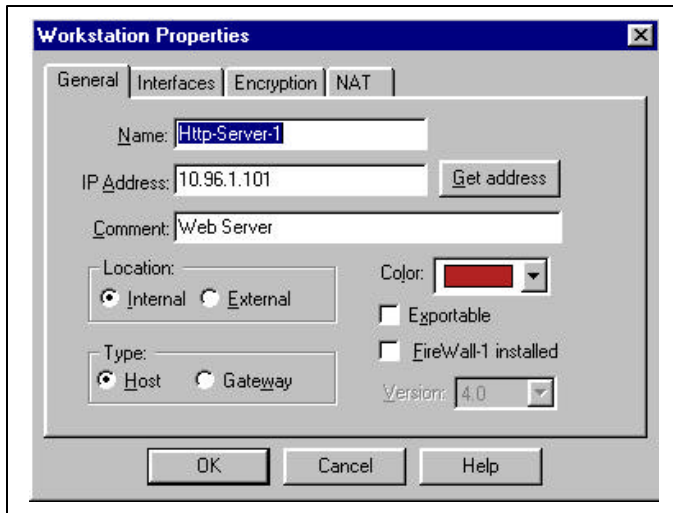
1. FireWall-1 detects an HTTP request to a logical server and redirects the request to the load-balancing daemon.
2. The daemon notifies the client that the request is being redirected to the destination physical server.
3. The rest of the session is conducted between the client and the destination server, without the intervention of the load-balancing daemon.

Configuration:

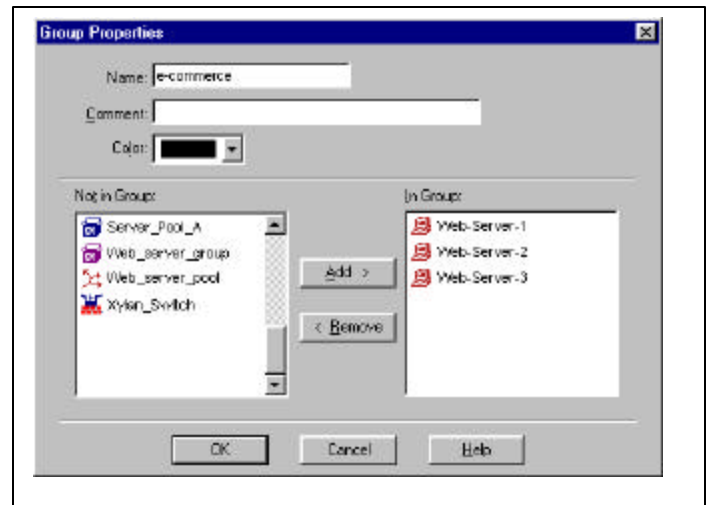
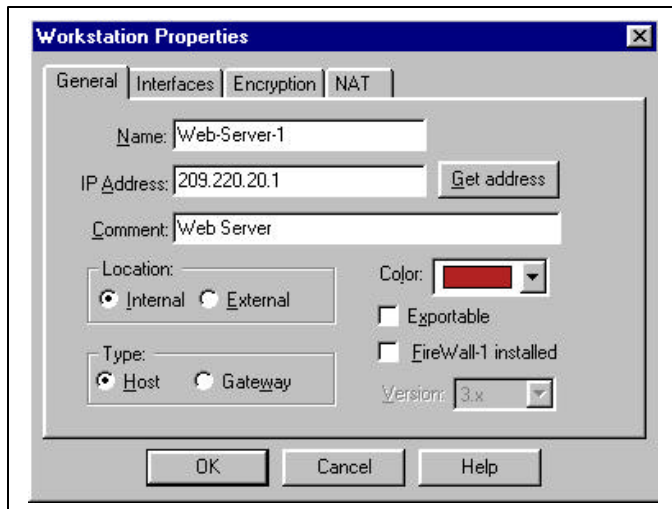
1. Define Workstation Properties for Http-Servers 1,2, and 3 with static NAT
2. Define Workstation Properties for external Servers
3. Define a group network object consisting of physical servers that will be providing the given service.
4. Define a Network object for the Logical Server
5. Define properties of Logical Server.
6. Add rules to rule base

Configuration Details:

1. Define Workstation Properties for Http-Servers-1,2 and 3 with static NAT

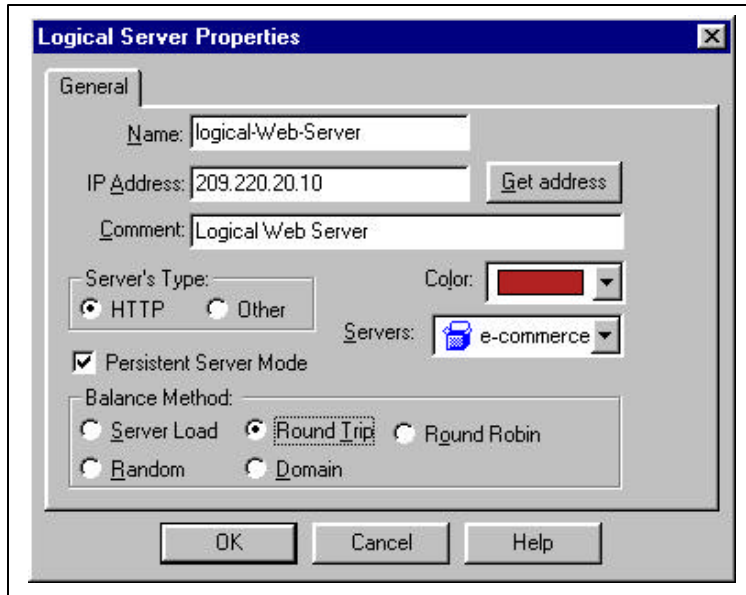


2. Define Workstation Properties for Http-Servers 1,2 and 3 using their translated address
Note: Although the NAT entries were configured for each Server, an entry must be made for reference for the Logical Web Server to send the correct address in the *HTTP redirect*.
3. Define a group network object consisting of physical servers that will be providing the given service.

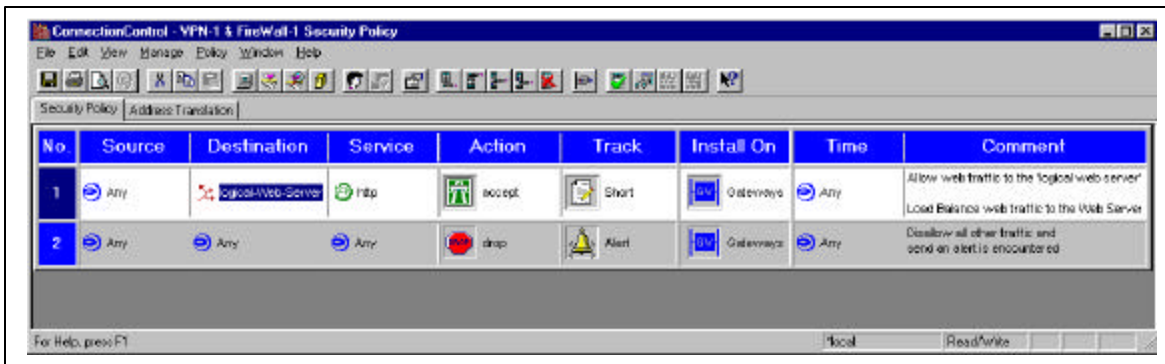


4. Define a Network object for the Logical Server
5. Define properties of Logical Server

Note: Persistent Server Mode allows a session to retain its load-balancing method until the session has ended. An example of this is loading multiple Web pages from one site. Because each page is from the same site, FireWall-1 does not require a new session to re-establish the original load-balancing algorithm.



6. Add rule to rule base



+++++

In the Logical Server Properties screen, you can choose Other as the server type. Choose Other when a server is an FTP (or other) server.

FTP load balancing is different from HTTP load-balancing . When Other is chosen under Server's type, load-balancing is performed with automatic address translation.

FTP example:

1. The Client sends a packet to the firewall; the packet is sent to the FTP logical server, using the IP address 209.220.20.11.

2. The load-balancing daemon ensures the packet is load balanced. The kernel translates the packet to the physical server's IP address 10.96.1.51.
3. The kernel translates the reply packet from 10.96.1.51 to 209.220.20.11 using backward address translation.

Appendix A - Troubleshooting Tips

The most common problem is with setting static routes for static NAT entry. Be sure to set the correct ARP entry. To configure the correct ARP entries use the following syntax.

Unix

On the gateway, link the IP address for each server to the external address of the gateway's external interface.

```
#arp -s 209.220.20.1 <MAC Address> pub
```

```
set static route
```

```
#route add 209.220.20.1 10.96.1.101
```

NT

Create a text file named local.arp in the \$FWDIR\state directory

```
<MAC Address> <IP Address>
```

```
set static route
```

```
route -p add 209.220.20.1 10.96.1.101
```