finjan®
Vital Security™
securing your web

Technical Brief

Load Balancing Configuration with NG-8040

Vital Security Release 8.4.x

January 2007

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA: San Jose 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	**Europe: UK** 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
USA: New York Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com	**Europe: Germany** Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
Israel/Asia Pacific Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	**Europe: Netherlands** Printerweg 56 3821 AD Amersfoort Netherlands Tel: +31 318 693 272 Fax: +31 318 693 274 salesne@finjan.com

Catalog name: Load Balancing Configuration with NG-8040: Q1 2007
Email: support@finjan.com
Internet: http://www.finjan.com

Contents

1 Introduction

The Finjan Vital Security NG-8040 is based on a Nortel Layer 2/7 switch appliance which is used as a Load Balancer and integrated into the Finjan Blade Center chassis.

Key features of Vital Security NG-8040 Load Balancer are:

- IP Load Balancing
- Gigabit Ethernet switch
- Layer 4/7 switching
- Redundant High Available Solution (2N)
- Enhanced security
- Enhanced health checks

Load Balancers consists of a virtual server (also referred to as vserver or VIP) which, in turn, consists of an IP address and port. The virtual server (VIP) is bound to a number of physical services running on the physical servers in a server farm. These physical services contain the physical server's IP address and port.

The following traffic flow occurs while using a load balancer: A client sends a request to the virtual server (load balancer). The load balancer selects a physical server in the server farm and directs this request to the selected physical server

Load Balancers also perform server monitoring (health checks) and maintains traffic/load statistics in order to ensure even balancing between the servers/services in the farm. In case of service failure, or server maintenance downtime, the load balancer will balance the traffic across the remaining servers/services that are up (healthy).

Load balancing is especially important for networks where it is difficult to predict the number of requests that will be issued to a server. A load balancer can be used to increase the capacity of a collection of servers beyond that of a single server. Therefore, load balancing is needed in a Vital Security environment comprising multiple Vital Security scanning servers and SSL appliances.

The Vital Security NG-8040 Load Balancer is integrated into the blade center chassis to enable traffic load balancing without the need of an external switch. Balancing the network traffic among multiple Servers is used to increase the traffic capacity of the system working as a server farm beyond that of a single server. It also increases the system availability by enabling service through any of the other servers in the farm in case one of the servers in that farm failed, making a server failure transparent to the end-user.

NOTE: This document is relevant for VSOS 8.4.x.

2 Overview

This document describes 3 basic topologies for load balancing using a Vital Security NG-8040 switch in a Blade center:

1. Load Balance two Vital Security NG scanning servers.
2. Load Balance multiple Vital Security NG Scanning Servers with SSL.
3. Load Balance multiple Vital Security NG Scanning Servers (with no SSL) while working in Transparent Mode

In topologies 1 and 2 above, the assumption is that the client's browsers are configured to directly access the switch's IP which acts as a proxy. This IP will be the virtual IP for all scanners. The switch will than load balance the traffic among the services, either regular scanning servers or scanning servers with SLL.

3 Load Balancing Two Vital Security Scanning Servers on a Blade Center

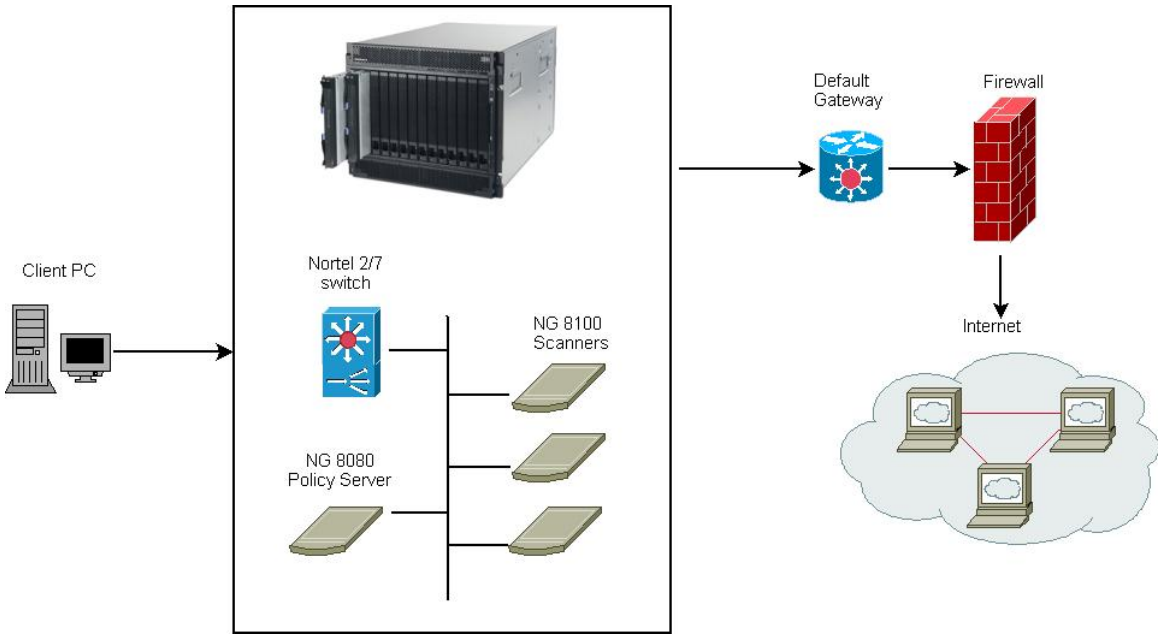
This section describes the configuration of the Nortel L2-7 switch to work with the Vital Security environment on a flat network (one subnet comprising as many scanners as required).

The switch configuration enables redirection of traffic to the blades.

A health check test does a 3-way handshake with each of the scanning servers every 10 seconds. If the scanning servers do not answer after 2 consecutive Health checks, the failed scanning server will be disabled by the switch.

3.1 Set Up Instructions

The example that follows is based on the setup shown below.



3.2 Requirements

A basic installation of a Policy Server[1] and multiple scanning servers is required.

Each scanning server in this configuration is accessed through the proxy virtual IP. In addition the switch itself should have an IP from the same subnet.

NOTE: This configuration also supports the HA-PS solution.

[1] A single or active/standby Policy Server configuration can be used in this topology

3.3 Switch configuration

In the following example, the switch configuration comprises of the following addresses:

Vital Security scanning server 1: **10.194.150.11**

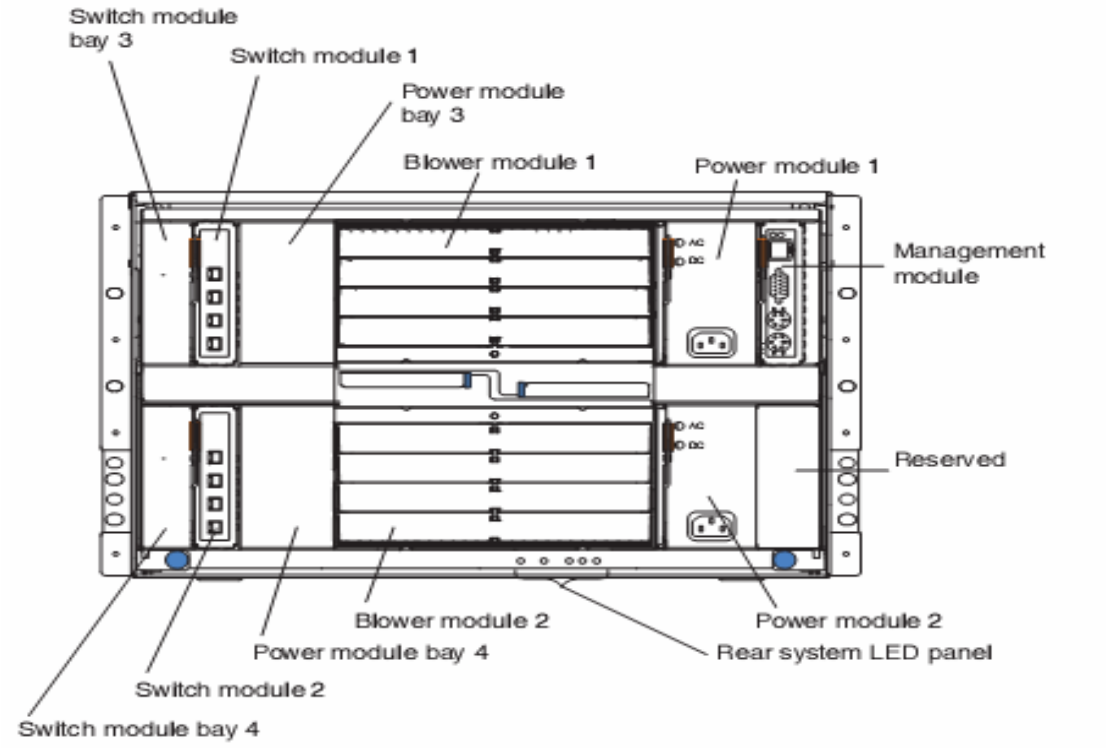
Vital Security scanning server 2: **10.194.150.12**

Default gateway: **10.194.0.1**

Switch IP address: **10.194.150.200**

Proxy Virtual IP: **10.194.150.87**

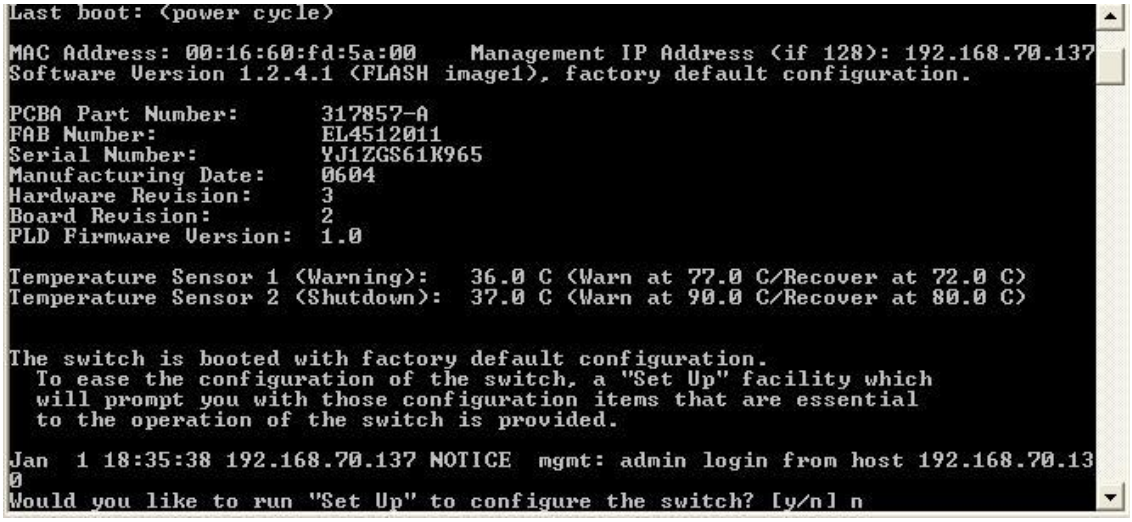
NOTE: All of the commands in the switch configuration can be copied and pasted to the switch except for the ones which require IP changes.



NOTE: The IP of the switch is set by default to 192.168.70.127 – 192.168.70.130, depending on the location of the switch on the chassis, such that the default IP on place holder number 1 is 192.168.70.127.

⇨ To log in to the switch

1. Log in to the switch via telnet using the "admin" password. The switch is booted with factory default configuration. The following is displayed:



2. Type n (i.e. do not run the "Set up" to configure the switch).
3. Ensure that the switch configuration is empty by typing the following command:

   /cfg/dump

   A clean configuration will give the following result:

   ```
   script start "Nortel Networks Layer2-7 GbE Switch Module" 4  /****
   /* Configuration dump taken  0:03:20 Thu Jan  1, 2070
   /* Version 21.0.1.1,  Base MAC address 00:13:0a:4d:13:00
   /
   script end  /****
   ```

4. If this result is not displayed, restore the configuration to default from the Blade Center management module on the I/O Module configuration screen (see Paragraph 6.2).

⇨ To add IP of switch

- Add the IP of the switch and set the default gateway by typing the following:

```
/c/l2/stg 1/off
/c/l3/if 1
    ena
    addr 10.194.150.200
    mask 255.255.0.0
    broad 10.194.255.255
/c/l3/gw 1
    ena
    addr 10.194.0.1
/c/slb/adv
    direct ena
```

⇨ To configure the multiple Vital Security scanning servers on the switch

- For Vital Security scanning server configuration on the switch, type the following

```
/c/slb/real 1
        ena
        rip 10.194.150.11
        inter 10
        retry 2
        name "Vital Security NG scanning server 1 IP address"
/c/slb/real 2
        ena
        rip 10.194.150.12
        inter 10
        retry 2
        name "Vital Security NG scanning server 2 IP address"
/c/slb/group 1
        add 1
        add 2
        metric minmisses
```

NOTE: This will add 2 scanning servers with IPs 10.194.150.11 and 10.194.150.12 to the configuration, combined as a group called group 1.

⇨ To create the virtual IP:

- To create the virtual IP for the load balancing and set its services, type the following:

```
/c/slb/virt 1
        ena
        vip 10.194.150.87
/c/slb/virt 1/service 8080
        group 1
/c/slb/virt 1/service 2121
        group 1
        pbind clientip
        dbind ena
```

To set the switch internal ports to work in the correct mode:

- To set the switch internal ports to work in the correct mode type the following:

NOTE: Type only the required internal ports on which scanning blades are installed, i.e. if blades are in slots 1-5, then only INT1-INT5 should be defined.

```
/c/slb/port INT1
        server ena
/c/slb/port INT2
        server ena
/c/slb/port INT3
        server ena
/c/slb/port INT4
        server ena
/c/slb/port INT5
        server ena
/c/slb/port INT6
        server ena
/c/slb/port INT7
        server ena
/c/slb/port INT8
        server ena
/c/slb/port INT9
        server ena
/c/slb/port INT10
        server ena
/c/slb/port INT11
        server ena
/c/slb/port INT12
        server ena
/c/slb/port INT13
        server ena
/c/slb/port INT14
        server ena
/c/slb/port EXT1
        client ena
```

To save the configuration

- To save the configuration type the following

```
apply
save
```

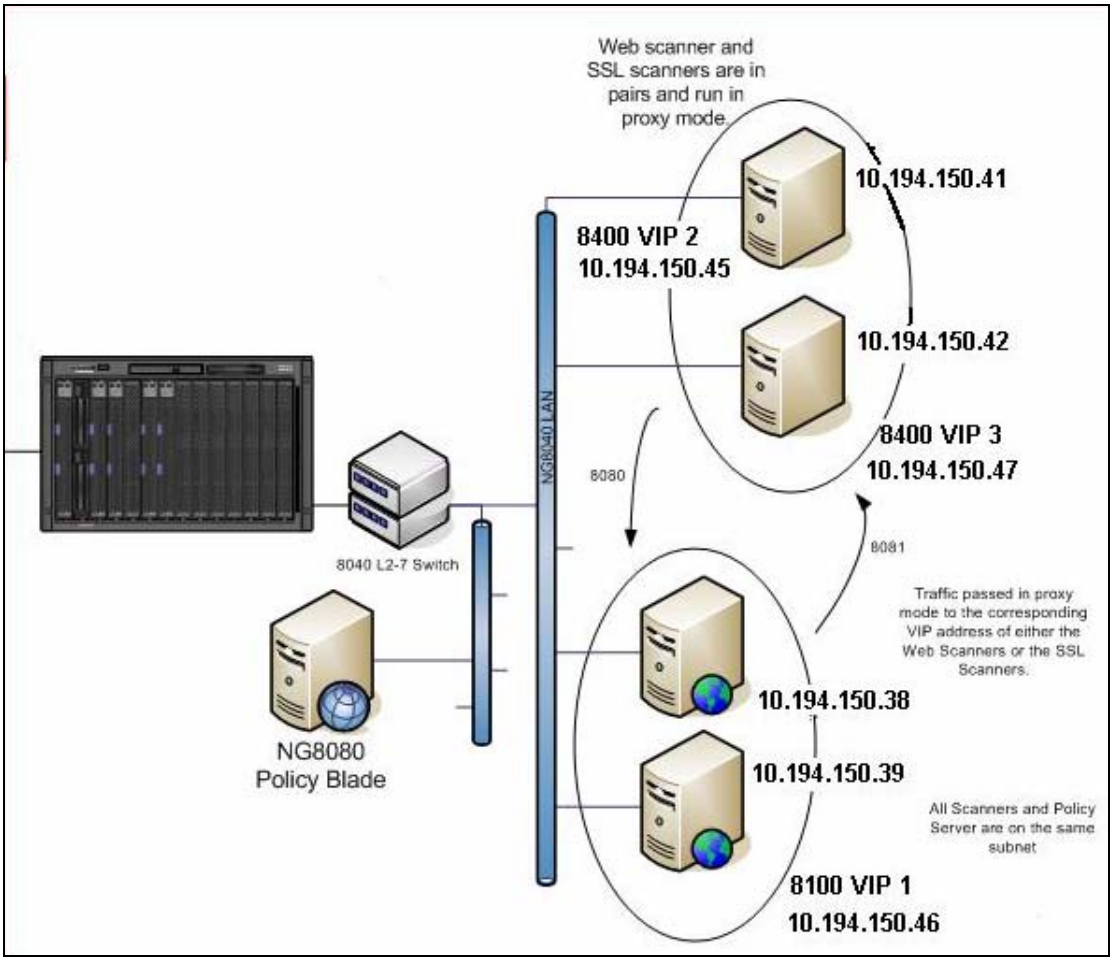
NOTE: It is recommended to save the configuration regularly while entering command lines.

4 Load Balancing multiple Vital Security Scanning Servers with SSL on a Blade Center

The following topology configuration handles the option of load balancing the traffic on multiple[2] Vital Security scanning servers with additional load balancing of SSL traffic over multiple SSL appliances.

4.1 Setup Instructions

The example that follows is based on the setup shown below.



[2] One or more

4.2 Configuring the Load Balancer to match the LAN

For the purposes of this configuration, assume that in the Telnet session you will be working on the network 10.194.XXX.XXX.

The switch must have an IP route to all of the real servers that receive switching services.

⇨ **To configure the load balancer to match the LAN (i.e. to have a LAN IP)**

1. To configure the load balancer to match the LAN, type the following:

   /c/l3/if 1

   This will create a new interface (1) for the load balancer which is on the same network as the LAN.

2. Type the following:

   mask 255.255.0.0

   addr 10.194.50.7

   vlan 1

   ena

4.3 Port Setup

The instructions listed below are relevant to every external port (EXT) in the switch that has an Ethernet line (network cable) attached. There may be 1-4 external ports depending on the number of external ports connected to the switch. Each port relates to an Ethernet interface on each blade (eth0-eth3). This is supported by hardware on the blades themselves (by default only eth0 and eth1 are available and both are enabled). It is also necessary to configure all 14 internal ports, as the traffic may come from any blade (i.e. blade servers 1-14).

To set up the ports

- To set up the ports, type the following:

NOTE: Type only the required internal ports on which scanning blades are installed, i.e. if blades are in slots 1-5 on the chassis, then only INT1-INT5 should be defined. Similarly, only the EXT ports which are connected on the switch and used for incoming traffic to the scanning blades should be configured.

```
/c/slb/port INT1
        client ena
        server ena
    /c/slb/port INT2
        client ena
        server ena
    /c/slb/port INT3
        client ena
        server ena
    /c/slb/port INT4
        client ena
        server ena
    /c/slb/port INT5
        client ena
        server ena
    /c/slb/port INT6
        client ena
        server ena
    /c/slb/port INT7
        client ena
        server ena
    /c/slb/port INT8
        client ena
        server ena
    /c/slb/port INT9
        client ena
        server ena
    /c/slb/port INT10
        client ena
        server ena
    /c/slb/port INT11
        client ena
        server ena
    /c/slb/port INT12
        client ena
        server ena
    /c/slb/port INT13
        client ena
        server ena
    /c/slb/port INT14
        client ena
        server ena
```

```
/c/slb/port EXT1
   client ena
   server ena
   proxy ena
/c/slb/port EXT2
   client ena
   server ena
   proxy ena
/c/slb/port EXT3
   client ena
   server ena
   proxy ena
/c/slb/port EXT4
   client ena
   server ena
   proxy ena
```

4.4 Creating the Real Servers

Configuration is necessary in order to introduce the entire network to the load balancer. The real servers in any given real server group must have an IP route to the switch that performs the load balancing functions. This IP routing is easily accomplished by placing the switches and servers on the same IP subnet.

To create a Real Server

- To create a Real Server, type the following

```
/c/slb/real 2
   ena
   rip 10.194.150.41
   name "SSL Appliance 1 IP address"
/c/slb/real 3
   ena
   rip 10.194.150.42
   name "SSL Appliance 2 IP address"
/c/slb/real 4
   ena
   rip 10.194.150.38
   name "Vital Security NG scanning server 1 IP address"
/c/slb/real 5
   ena
   rip 10.194.150.39
   name "Vital Security NG scanning server 2 IP address"
```

NOTE: 10.194.150.41 and 10l.194.150.42 are the SSL appliance IPs and , 10.194.150.38 and 10.194.150.39 are the NG-8100 appliance IPs.

4.5 Creating the Group and adding servers to each group

⇨ **To create a group which combines similar scanning servers together**

- To create a group which combines similar scanning servers together, type the following:

```
/c/slb/group 1
  add 2
  add 3
/c/slb/group 2
  add 4
  add 5
```

NOTE: Group 1 is the group of SSL scanning servers, group 2 is the group of HTTP scanning servers.

4.6 Creating the Virtual Server

The Virtual Server is the Load Balancer address that the Client's browser points to as a proxy. The following configuration will provide the right group of scanning servers for each service.

⇨ **To create a virtual server**

- To create a virtual server, type the following:

```
/c/slb/virt 1
        ena
        vip 10.194.150.45
/c/slb/virt 1/service 8080
        group 1
/c/slb/virt 2
        ena
        vip 10.194.150.46
/c/slb/virt 2/service 8080
        group 2
/c/slb/virt 3
        ena
        vip 10.194.150.47
/c/slb/virt 3/service 8081
        group 1
```

NOTE: 10.194.150.45 and 10.194.150.46 are the HTTPS LB VIP on port 8080, 10.194.150.47 is the HTTP LB VIP on port 8081 for the loopback, group 1 is the group of SSL scanning servers and group 2 is the group of HTTP scanning servers,

4.7 Enabling two or more IPs to use the same port

This example includes both 10.194.150.45 and 10.194.150.46 (virtual IP addresses/virtual proxies) using port 8080 (this is configured in the browser as the proxy settings). In order to enable using the same port by two different IPs, Direct Mode must be enabled.

To enable Direct Mode

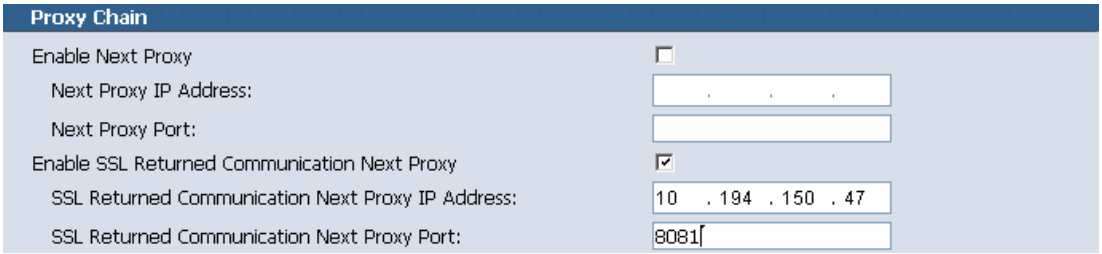
- To enable Direct Mode, type the following:

```
/c/slb/adv
        direct ena
```

4.8 Configuration in Vital Security

To configure Vital Security:

1. Navigate in the Management Console to **Settings-> Devices-> Scanning Server-> HTTP-> Proxy Chain**.

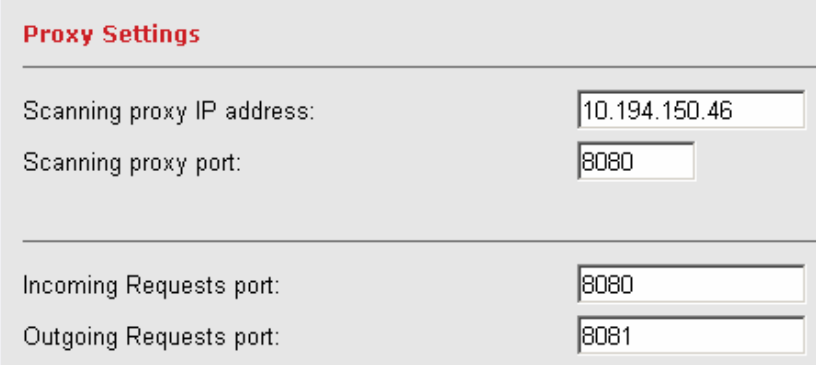


2. Check the **Enable SSL Returned Communication Next Proxy** in order to add a Next Proxy specifically for SSL Traffic. Enter the relevant IP Address and Port.

4.9 Configuration of the SSL Appliance

⇨ **To configure the SSL Appliance:**

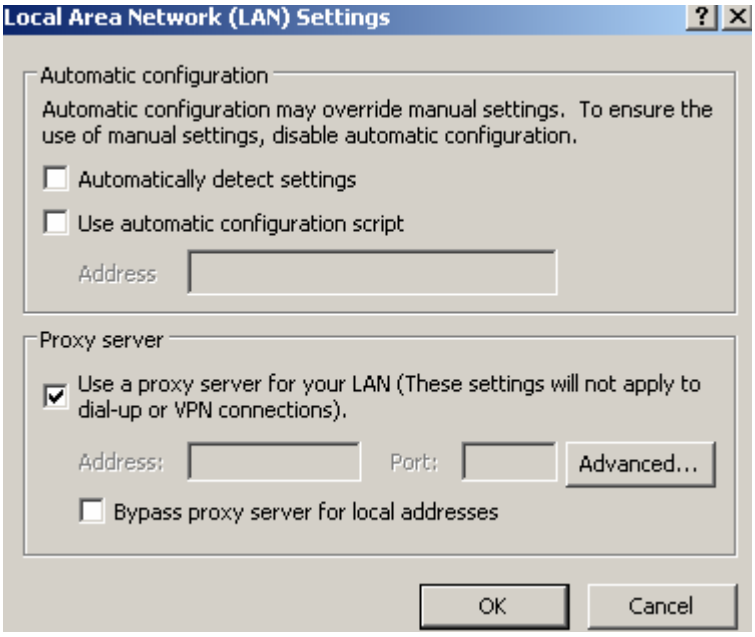
- On the SSL web configuration screen, navigate to **Scanners-> Proxy Settings** and enter the required proxy settings**.**



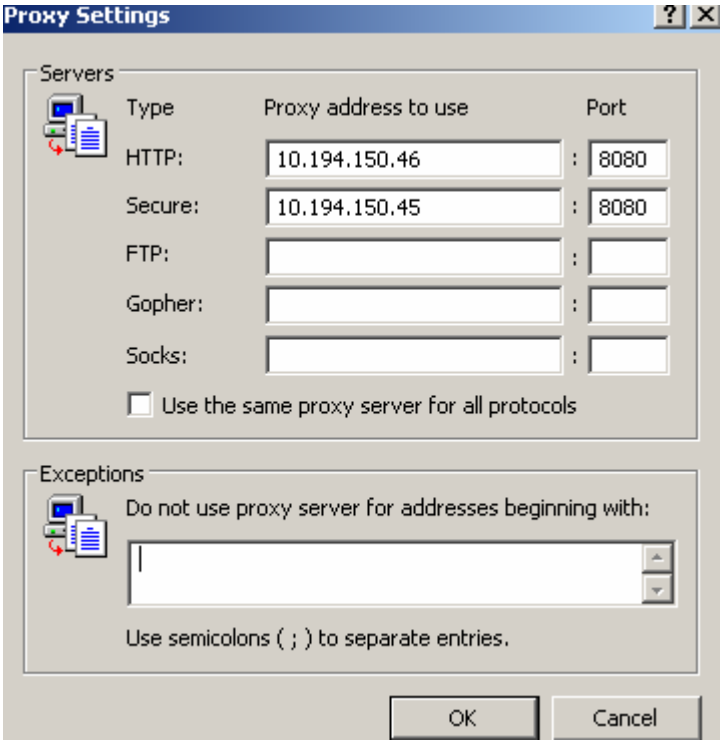
4.10 Client's Browser Configuration

⇨ **To configure the Browser:**

1. Navigate in the Internet Explorer to **Tools-> Internet Options-> Connections-> LAN Settings.**



2. Select the Proxy Server option and click **Advanced**. The proxy Settings screen is displayed.



3. Type in the HTTP proxy address and port as well as the secure proxy address and port and click **OK**.

NOTE: This IP is the virtual IP of the switch which was previously configured.

5 Load Balancing multiple Vital Security Scanning Servers without SSL on a Blade Center while working in Transparent Mode

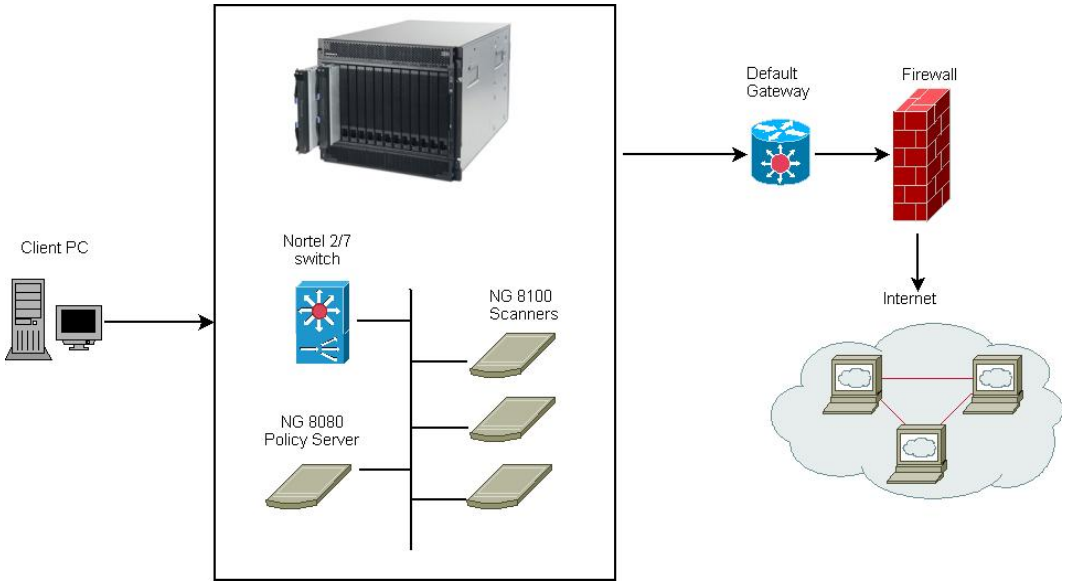
This section describes the configuration of the Nortel L2-7 switch to work with the Vital Security environment in transparent mode on a flat network (one subnet).

The suggested switch configuration will enable the switch to redirect traffic to the scanning server blades.

A health check test does a 3-way handshake with each of the scanning servers every 10 seconds. If the scanning servers do not answer after 2 consecutive health checks, they are disabled by the switch and traffic will not be send to it until it will respond again.

5.1 Setup Instructions

The example that follows is based on the setup shown below.



5.2 Requirements

A basic installation of one Policy Server and numerous Scanning Servers is required. Each scanning server in the configuration is analogous to a “real server”. In addition the switch itself should also have an IP from the same subnet.

NOTE: This configuration also supports the HA-PS solution.

5.3 Switch configuration

The switch configuration example described below uses the following addresses:

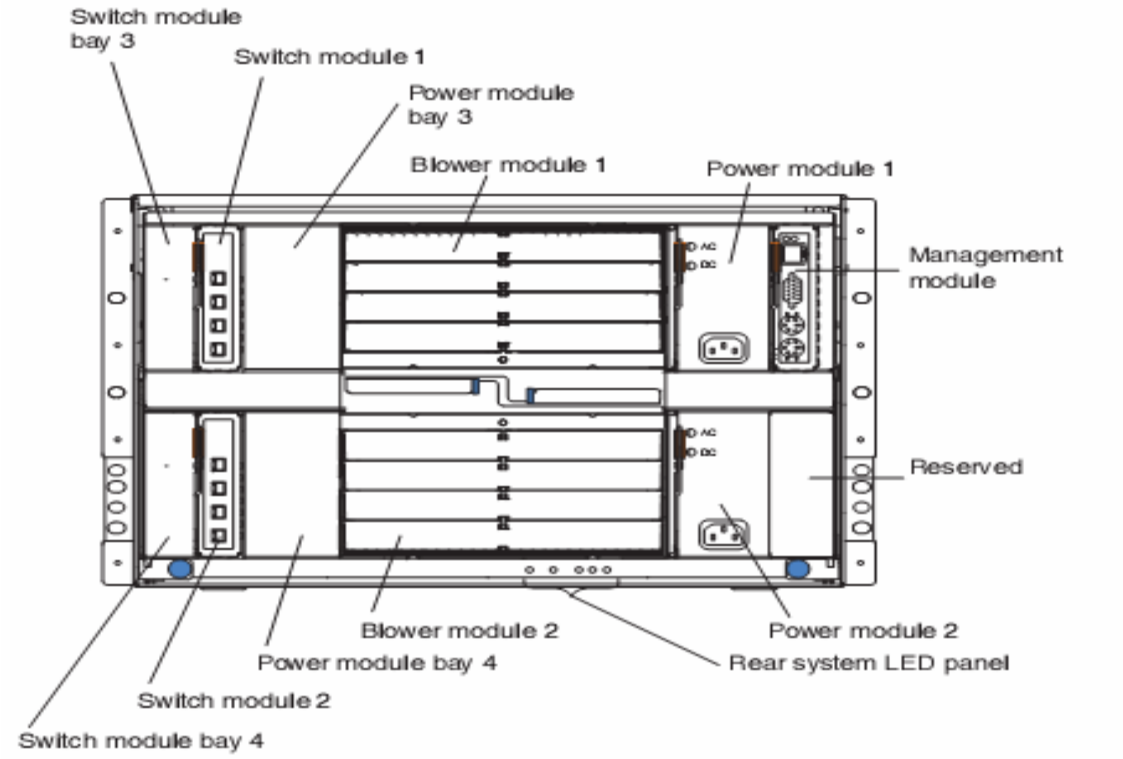
NG scanning server 1: **10.194.150.210**

NG scanning server 2: **10.194.150.211**

Default gateway: **10.194.0.1**

Switch IP address: **10.194.150.200**

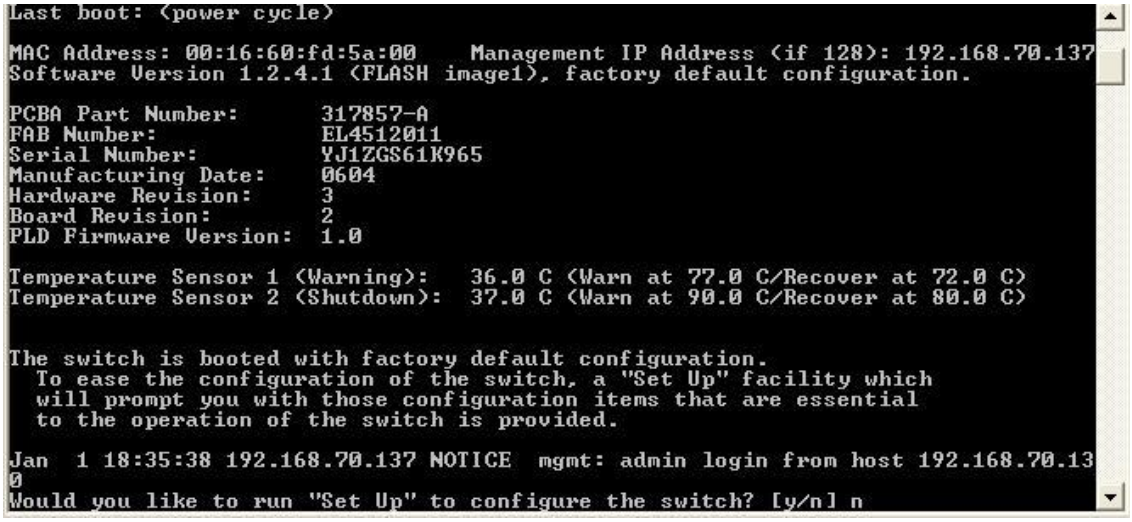
NOTE: All of the commands in the switch configuration can be copied and pasted to the switch except for the ones which require IP changes.



NOTE: The IP of the switch by default is 192.168.70.127 – 192.168.70.130, depending on the location of the switch on the chassis, such that the default IP on place holder number 1 is 192.168.70.127.

⇨ To log in to the switch

1. Log in to the switch via telnet using the "admin" password. The switch is booted with factory default configuration. The following is displayed:



2. Type n (i.e. do not run the "Set up" to configure the switch).
3. Ensure that the switch configuration is empty by typing the following command:

```
/cfg/dump
```

A clean configuration will give the following result:

```
script start "Nortel Networks Layer2-7 GbE Switch Module" 4  /****
/* Configuration dump taken  0:03:20 Thu Jan  1, 2070
/* Version 21.0.1.1,  Base MAC address 00:13:0a:4d:13:00
/
script end  /****
```

4. If this result is not displayed, restore the configuration to default from the chassis management module on the I/O Module configuration screen (see paragraph 6.2).

⇨ To add IP of switch and set the default GW

- Add the IP of the switch and set the default GW by typing the following:

```
/c/l3/if 1
    ena
    addr 10.194.150.200
    mask 255.255.0.0
    broad 10.194.255.255
/c/l3/gw 1
    ena
    addr 10.194.0.1
/c/slb/adv
    direct ena
```

⇨ To configure the Vital Security NG scanning servers on the switch

- For Vital Security NG scanning server configuration on the switch, type the following:

NOTE: The Vital Security scanning server 1 and Vital Security scanning server 2 IP addresses must be inserted, as well as the Vital Security Scanning server group.

```
/c/slb/real 1
    ena
    rip 10.194.150.210
    inter 10
    retry 2
    name "Vital Security NG scanning server 1 IP address"
/c/slb/real 2
    ena
    rip 10.194.150.211
    inter 10
    retry 2
    name "Vital Security NG scanning server 2 IP address"
/c/slb/group 1
    metric hash
    health tcp
    add 1
    add 2
    name "Vital Security NG Scanning servers group"
```

⇨ To set filters to direct the HTTP & FTP traffic to the scanning servers

1. To set the filters to direct the HTTP & FTP traffic to the scanning servers type the following:

```
/c/slb/filt 20
    name "filter http traffic"
    ena
    action redir
    proto tcp
    dport http
    group 1
    rport 0
    vlan any
/c/slb/filt 20/adv
    thash both
/c/slb/filt 21
    ena
    action redir
    proto tcp
    dport ftp
    group 1
```

```
        rport 0
        vlan any
/c/slb/filt 21/adv
        thash both
/c/slb/filt 22
        ena
        action redir
        proto tcp
        dport ftp-data
        group 1
        rport 0
        vlan any
/c/slb/filt 22/adv
        thash both
/c/slb/filt 30
        name "any other traffic redirect"
        ena
        action redir
        proto tcp
        group 1
        rport 0
        vlan any
/c/slb/filt 30/adv
        thash both
```

2. Enable all the defined filters on the switch external port by typing the following:

```
/c/slb/port EXT1
        filt ena
        add 20-22
        add 30
```

Note: EXT1 – EXT4 are the NICs connection on the switch such that EXT1 is the upper one.

To save the configuration

- To save the configuration type the following

```
apply
save
```

NOTE: It is recommended to save regularly while entering command lines.

To setup transparent proxy in the Vital Security Web Appliance, please refer to the Management Console Reference Guide , section 8.4.6.3.

6 Appendix A – Resetting the Switch Configuration to Default Settings

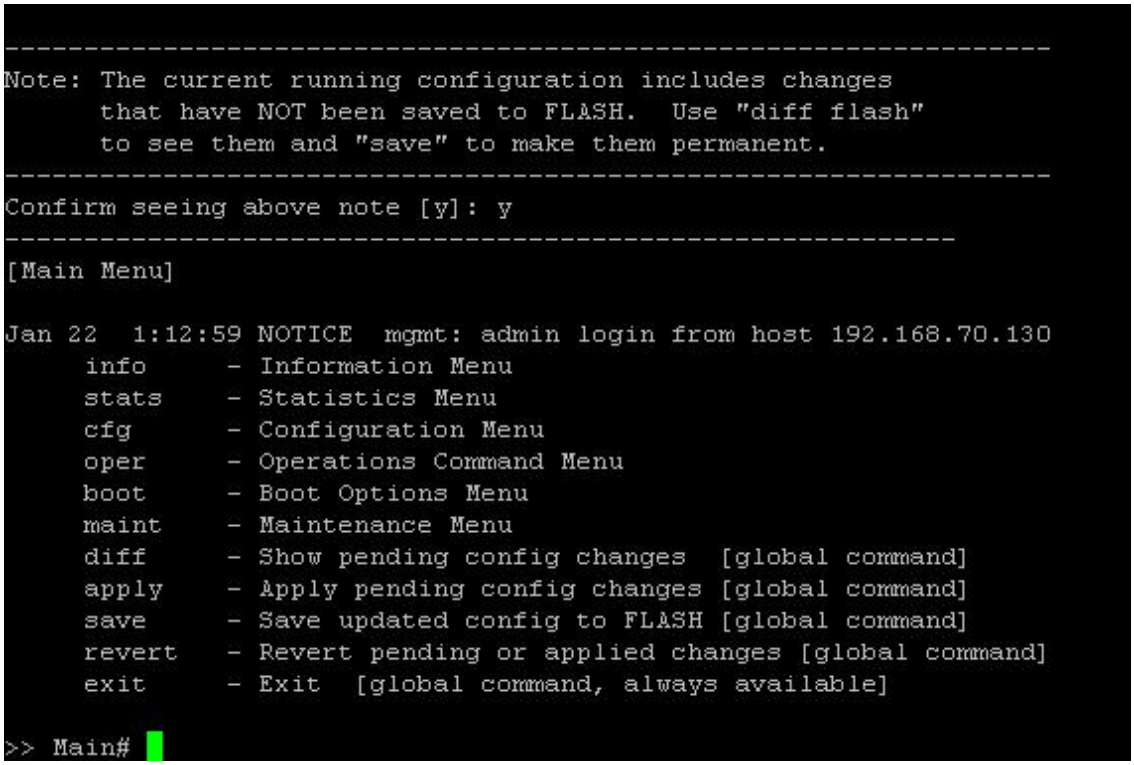
There are 2 methods for resetting the L2/7 configuration to factory defaults:

- Using the switch CLI
- Using the Blade Center Management Module

6.1 Restore Default Settings using CLI

⇨ **To restore the switch to default "factory" settings:**

1. Log in to the switch (as described in Paragraph 3.3 - To log in to the switch).
2. Navigate in the Main Menu to the Boot Options Menu.

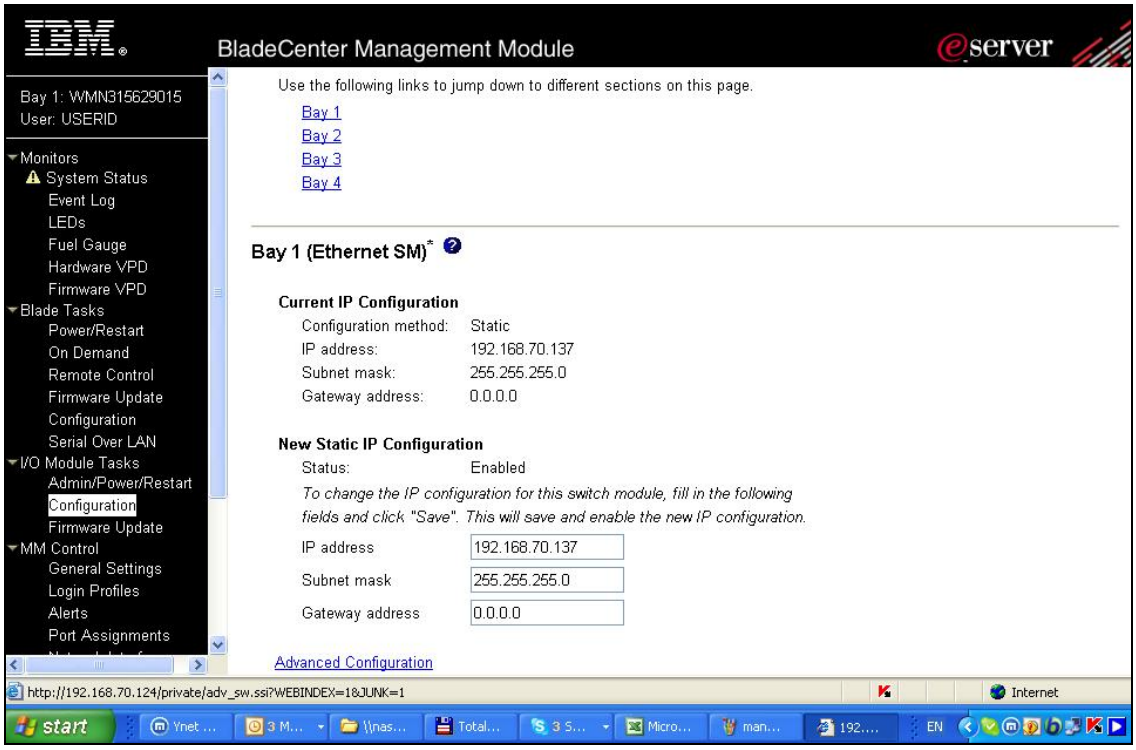


3. Select config block to use on next boot.
4. Type "factory" and press Enter.
5. Type "reset" and press Enter – this will prompt for confirmation. Confirm to reset the switch to the default configuration.

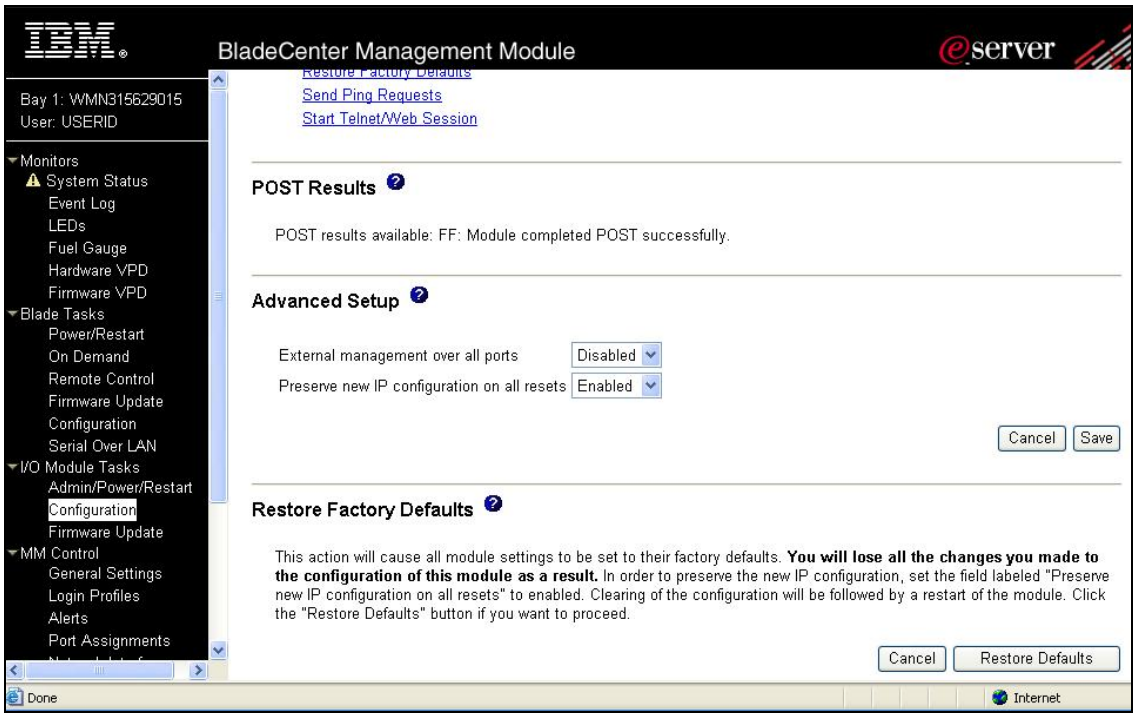
6.2 Restore Default Settings using the Blade Center Management Module

⇨ **To restore the switch to default "factory" settings:**

1. Enter IP to log in to the Blade Center Management Module. At the Welcome screen click on Continue.
2. In the Blade Center Management Module, navigate on the left hand side to **I/O Module Tasks** -> **Configuration** and select the required switch Bay (1-4).



3. Click the **Advanced Configuration** link. The **Restore Factory Defaults** section is displayed.



4. Click **Restore Defaults** and confirm. This resets the switch and loads it with the default settings.

7 Appendix B – Troubleshooting Commands

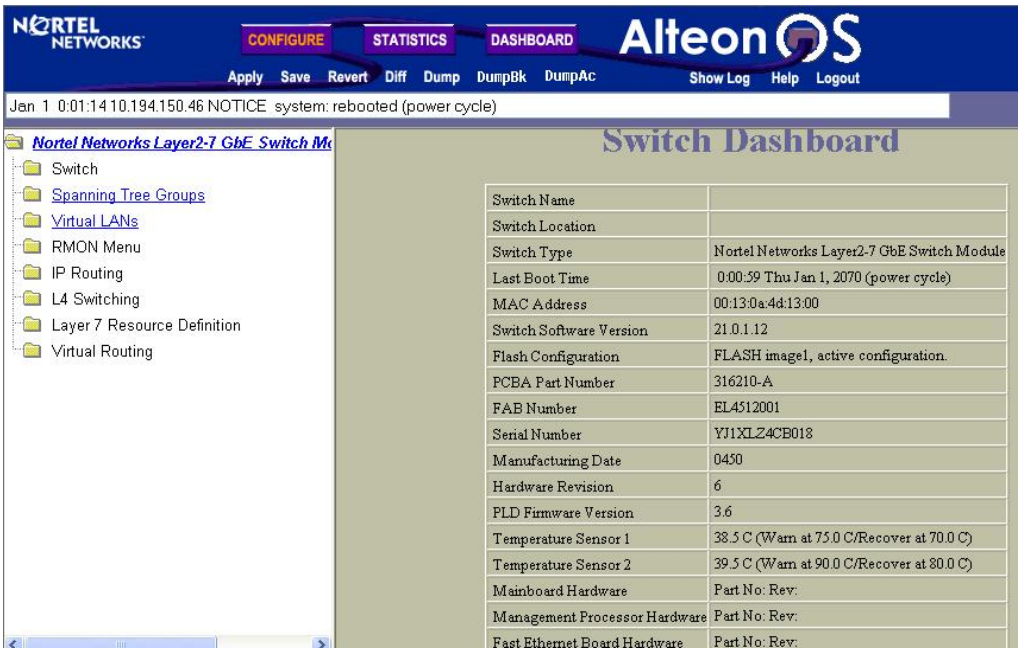
The following Vital Security NG-8040 troubleshooting commands are available:

Command	Description
/info/l3/dump	This command will display the following: ♦ Interfaces status – which physical IP's are configured and their status. ♦ Default Gateways status – Which Gateways are defined and their status. ♦ Current IP port settings. ♦ VRRP status. ♦ ARP and Routing information. Other options that are not related to the example configurations described in this document.
/info/slb/real	This command will display all the defined real servers (scanning servers) and all related configuration aspects (group, services, virtual servers, etc).
/info/slb/virt	This command will display all the defined virtual servers and all related configuration aspects.
/info/slb/filt	This command will display all the defined filters and their related configuration aspects.
/info/slb/dump	This command will display all the above 'slb' options and additional information which is not related to the example configurations described in this document.
/stats/l3/dump	This command displays all Layer 3 statistics.
/stats/slb/dump	This command displays all 'slb' statistics.

The above information can also be viewed using the HTML based GUI of the switch as shown in the following example:

⇨ To view the IP Interface Configuration information

1. Enter the IP address of the switch and at the login screen type the username ("admin") and password ("admin").
2. Click on **DASHBOARD** and then on the **Nortel Networks Layer2-7 GbE Switch Menu.**



3. Navigate in the **Nortel Networks Layer2-7 GbE Switch Menu** to **IP Routing** > **IP Interfaces** to view the IP Interface Configuration Information.