



FBLOS FortiBalancer 8.2

WebUI Handbook

All Rights Reserved

Copyright©2000-2011 Fortinet, Inc., 1090 Kifer Road Sunnyvale, CA 94086, USA. All rights reserved.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and compilation. No part of this document may be reproduced in any form by any means without prior written authorization of Fortinet, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

Fortinet, Inc., reserves the right to change any products described herein at any time, and without notice. Fortinet, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Fortinet, Inc. The use and purchase of this product does not convey a license to any patent copyright, or trademark rights, or any other intellectual property rights of Fortinet, Inc.

Warning: Modifications made to the Fortinet units, unless expressly approved by Fortinet, Inc., could void the user’s authority to operate the equipment.

Declaration of Conformity

We, Fortinet, Inc., 1090 Kifer Road Sunnyvale, CA 94086, 1-866-992-7729; declare under our sole responsibility that the product(s) Fortinet, Inc., FortiBalancer Appliance complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Warning: This is a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. In a residential area, operation of this equipment is likely to cause harmful interference in which case the user may be required to take adequate measures or product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Foreword

Related Documents

FBLOS FortiBalancer 8.2 CLI Handbook

FBLOS FortiBalancer 8.2 User Guide

Contacting Fortinet

Please use the following information to contact us at Fortinet:

Website: Please go to <http://www.fortinet.com/>

Telephone: Please go to <https://support.fortinet.com/>

Address: 1090 Kifer Road Sunnyvale, CA 94086, USA

Conventions

The CLI commands mentioned in this handbook will adhere to these general conventions:

Style	Convention
Bold typeface	The body of a CLI command is in Boldface.
<i>Italic</i>	CLI parameters are in Italic.
< >	Parameters in angle brackets < > are required.
[]	Parameters in square brackets [] are optional. Subcommand such as “ no ”, “ show ” and “ clear ”.
{ x y ... }	Alternative items are grouped in braces and separated by vertical bars. One should be selected.
[x y ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.

This handbook will introduce the WebUI operations with the WebUI screenshots and lower-case letter symbols combined, as follows:

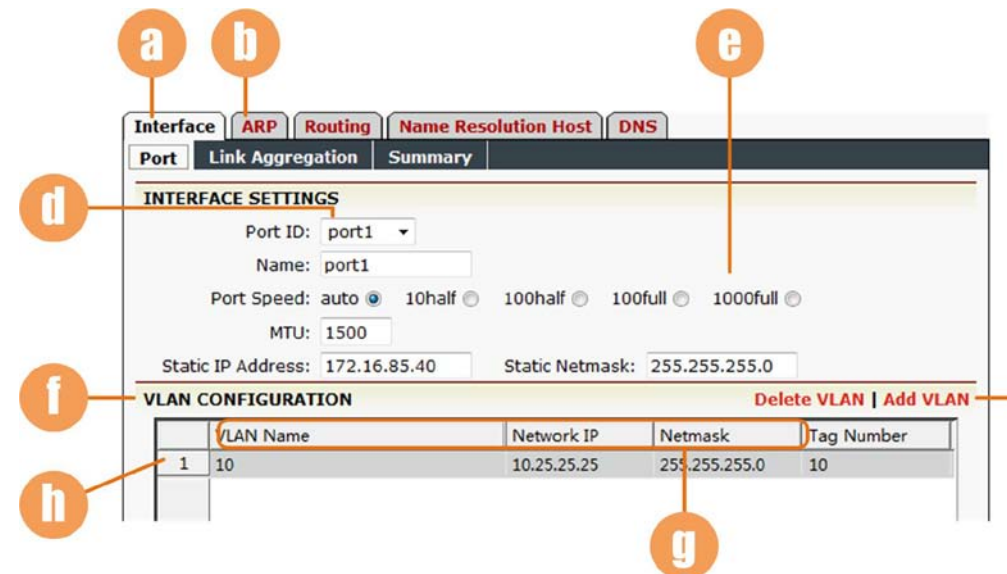


Table of Contents

All Rights Reserved.....	II	Configuration Window	9
Declaration of Conformity.....	II	Using the FortiBalancer WebUI	10
Foreword.....	III	Configuring with the WebUI	11
Related Documents.....	III	Home Page.....	12
Contacting Fortinet.....	III	Basic Information.....	12
Conventions	IV	Flight Deck.....	13
Table of Contents.....	V	Quick Starts	14
Web User Interface Introduction.....	1	System Configuration.....	17
Enabling the WebUI Function	2	General Settings	17
Connecting to the FortiBalancer Appliance	2	Host Settings.....	17
Enabling the WebUI Function via CLI	2	Date/Time.....	17
Using the WebUI Function.....	4	NTP.....	18
Supported Browsers.....	4	Basic Networking	19
Accessing the WebUI	5	Interface	19
Logging in the FortiBalancer WebUI	6	ARP	24
Understanding the FortiBalancer WebUI	7	Routing.....	25
Top Bar.....	8	Name Resolution Host.....	32
Side Bar	8	DNS	33

Advanced Networking.....	34	Virtual Services.....	59
NAT.....	34	Virtual Services	60
IPv6	36	All Policy Statistics.....	73
IP Region	39	Policy Order Templates.....	73
IP Pool	40	Virtual Service Global Setting	74
Port Forwarding.....	41	Check Lists	75
Clustering	43	Health Checker	75
Virtual Clusters.....	44	Health List.....	76
Fast Failover	46	Health Imports	77
Discreet Backup Mode.....	46	Groups	79
Statistics.....	47	Groups.....	80
WebWall.....	48	Groups Setting	83
Access Control.....	48	Application Setting.....	84
Attacking Packet Filter.....	50	SIP NAT.....	84
Monitoring	51	Direct Forward.....	85
Interface Statistics.....	51	Monitoring	86
NAT Translation Tables.....	52	Status.....	86
Server Load Balance	53	Virtual Service Statistics	87
Real Services.....	53	Group Statistics.....	87
Real Services	54	Real Service Statistics	87
Health Check Setting	57	Proxy.....	88

Compression	88	Global Load Balance	126
Setting.....	88	General Settings.....	127
Type.....	89	Records	128
Statistics	90	Topology	132
Caching Proxy.....	91	Methods.....	137
Global URL Filter.....	91	Bandwidth	142
HTTP Settings	93	DPS.....	144
Cache Settings	97	IANA	148
DNS Cache Settings.....	100	Statistics	149
SSL.....	101	Report.....	150
Global Settings	101	Monitoring	151
SSL Errors.....	104	SDNS	151
Virtual Hosts	105	Pool SNMP Statistics	151
Real Hosts	114	Admin Tools.....	152
Monitoring.....	119	System Management.....	152
Cache	119	System Info.....	152
Advanced Load Balance.....	120	Access Control.....	154
InBound Settings	121	Update.....	155
OutBound Settings.....	122	Shutdown/Reboot.....	156
Statistics	124	License	156
Report	125	Config Management	157

View	157	Interfaces	186
Backup	158	Statistics	187
Load	159	QoS Interface Statistics	187
Clear	160		
Synchronization	161		
Synchronization Sdns	164		
Command Timeout	165		
Graph	166		
Logging	166		
SNMP	170		
Statistics	173		
Graph Monitoring	175		
Troubleshooting	179		
Tools	179		
Debug Monitor	181		
Support Access	182		
User Management	183		
User Management	183		
QoS Configuration	184		
QoS	184		
QoS Entries	185		

Web User Interface Introduction

The FortiBalancer Web User Interface (WebUI) is designed to maximize the functionality and performance of the FortiBalancer appliance by allowing administrators to configure and control key functions of the FortiBalancer appliance. This WebUI Guide covers the functional elements of the graphical interface as well as basic setup steps.

This WebUI Guide is one of the three documentation resources available to administrators from Fortinet, Inc. The other two are the CLI Handbook and User Guide. The CLI Handbook is a resource tool that instructs administrators on detailed CLI operations of the FortiBalancer appliance. The User Guide is a more in-depth configuration strategy resource for complex FortiBalancer appliance deployments.

The three documents as well as current release notes and installation guides are available on the Documentation CD that accompanies the FortiBalancer appliance or from Fortinet, Inc. directly.

Enabling the WebUI Function

Connecting to the FortiBalancer Appliance

To use the WebUI function, first we should connect the client PC to the FortiBalancer appliance.

Put the FortiBalancer appliance onto the rack properly. Attach the power cord to the power supply, and turn on the power by pressing the power button.

Connect one end of the Console cable to the serial port of the client PC, and the other end to the serial port of the FortiBalancer appliance. Then, run the terminal software on the client PC to access the FBLOS via the Console connection.

Enabling the WebUI Function via CLI

To access the FBLOS via the terminal software, please first make certain that your terminal software is set as follows:

Setting	Value
Emulation	VT 100
Baud	9600
Number of Bits	8
Parity	No
Stop Bits	1
Flow Control	No

Enabling the WebUI Function via CLI (Continue)

After the above settings are finished, you can access the FBLOS CLI interface via the terminal software.

In the CLI interface, you will be first prompted for the user name and password (default to admin and admin). Once you log in successfully, the FBLOS will show the prompt “FBL>”. Enter the command “**enable**” to go to “Enable” mode, and the FBLOS will show “FBL#”. Continue to enter the command “**configure terminal**” to go to “Config” mode, and the FBLOS will show “FBL(config)#”.

Then, execute the following commands to complete necessary network settings and enable the WebUI function:

Command	Operation
ip address {system_ifname mnet_ifname vlan_ifname bond_ifname} <ip_address> <netmask>	This command is used to set the IP address and netmask of the system interface, MNET interface, VLAN interface or bond interface.
webui ip <ip_address>	This command is used to set the WebUI IP address.
ip route default <gateway_ip>	This command is used to set the default gateway IP address.
webui {on off}	This command is used to enable or disable the WebUI function.

Example:

```
FBL>enable
FBL#config terminal
FBL(config)#ip address outside 10.3.70.100 255.255.255.0
FBL(config)#webui ip 10.3.70.100
FBL(config)#ip route default 10.10.0.1
FBL(config)#webui on
FBL(config)#exit
```

Using the WebUI Function

Supported Browsers

The FortiBalancer appliance WebUI supports the following browsers:



Microsoft Internet Explorer (Recommended)



Mozilla Firefox



Google Chrome



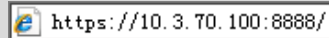
Opera

Note: It is highly recommended to use the Microsoft Internet Explorer (IE) browser for accessing the FortiBalancer WebUI. This handbook will introduce the WebUI operations in the IE browser.

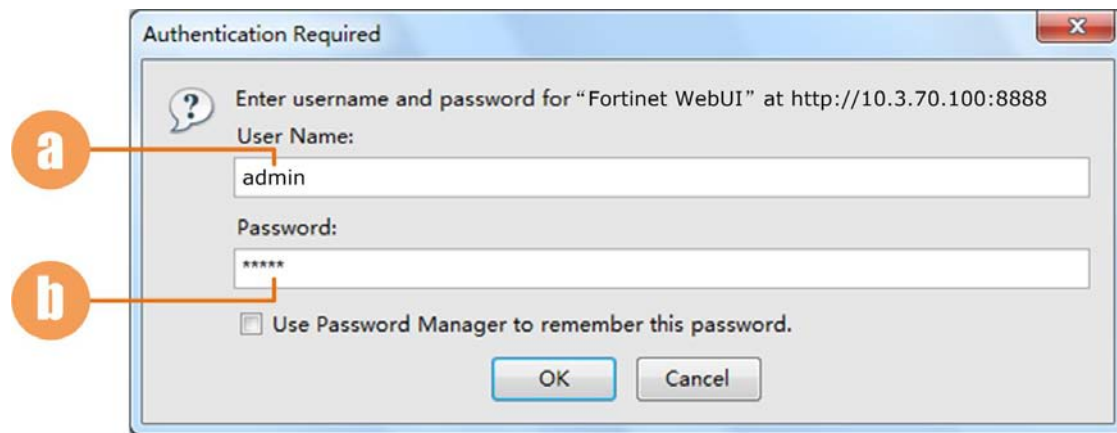
Accessing the WebUI

To access the FortiBalancer appliance, enter the configured WebUI IP address into the browser. Please note that this is a secure connection and therefore should be entered as an **HTTPS** address.

Example:

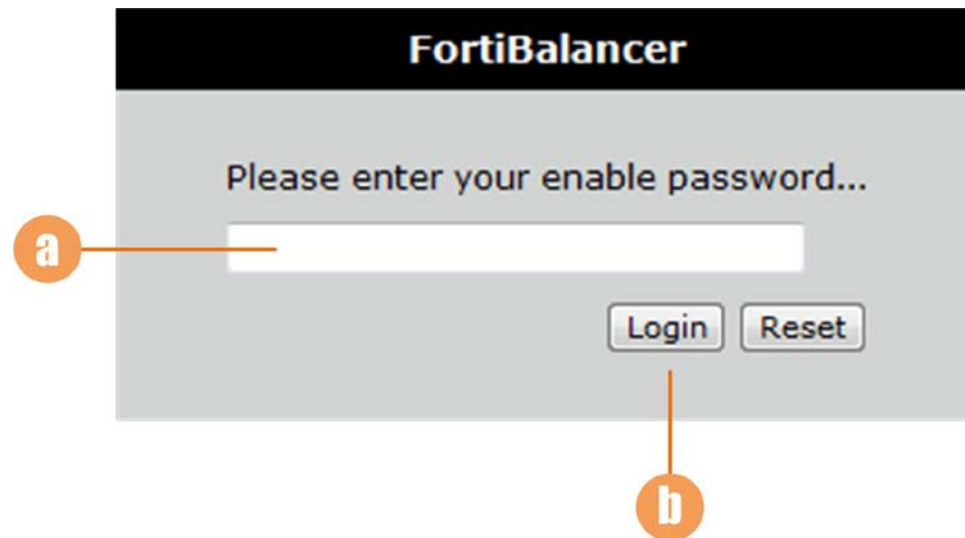


If the FortiBalancer appliance is correctly configured and the WebUI is turned on (see the example on the previous page), you will be prompted for the user name **[a]** and password **[b]**. Input the user name and password correctly. By default, the user name is admin and the password is admin. Click on “OK” when finished.



Logging in the FortiBalancer WebUI

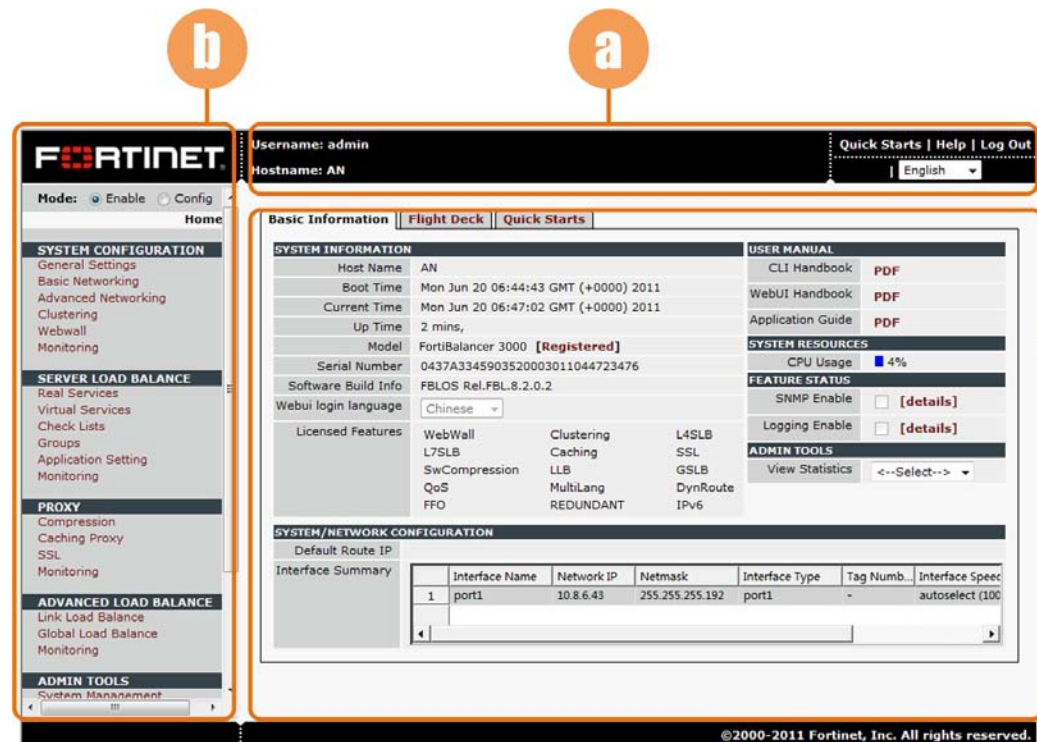
After the step of user registration, the FortiBalancer appliance will prompt you for an Enable level password. Enter the enable password correctly in the text field [a] (default to **null**), and click on the “Login” button [b]. Then, you will be taken to the FortiBalancer WebUI.



Understanding the FortiBalancer WebUI

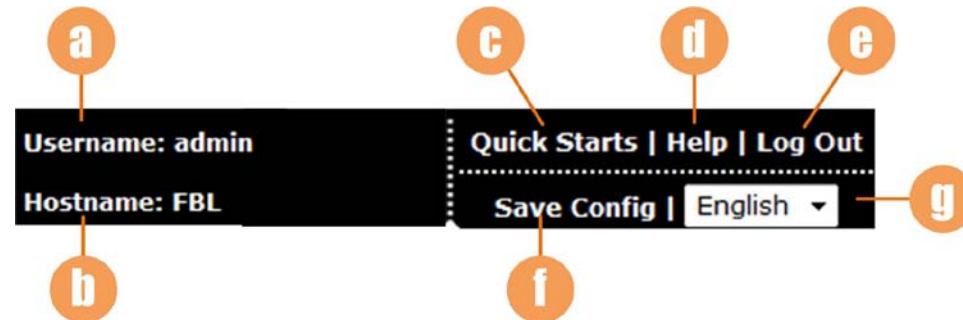
The FortiBalancer WebUI turns an ordinary browser window into an extraordinary configuration and management tool for the FortiBalancer appliance.

Illustration separates and labels the FortiBalancer WebUI's three active portions of the interface: top bar [a], sidebar [b], and configuration window [c].



Top Bar

The top bar displays basic static information such as user's name [a], FortiBalancer appliance host name [b] and four basic hyperlinks: Quick Starts [c], Help [d], Log Out [e] and Save Config [f]. Users can also set the WebUI display language via the selector [g].

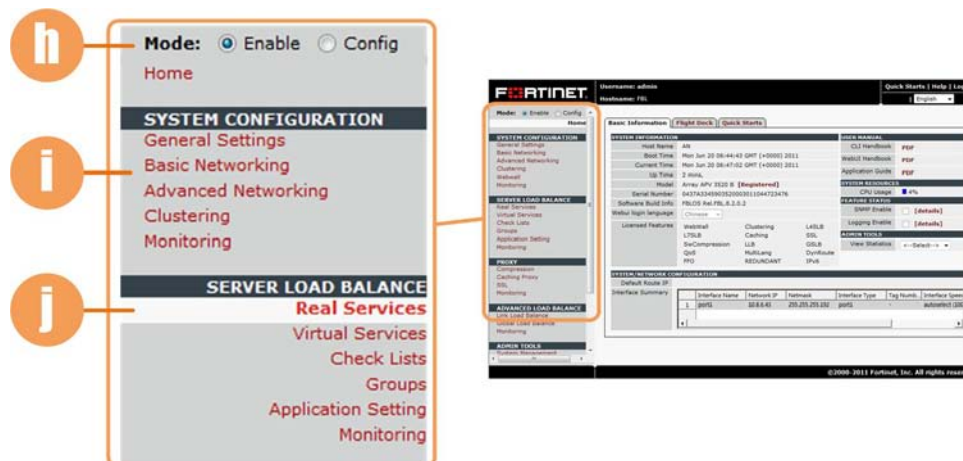


Side Bar

The side bar serves as the principal navigational tool for the Web interface. With this sidebar, administrators can perform desired configuration management and general setup about the FortiBalancer appliance.

Administrators can switch between the Enable and Config modes via the radio buttons [h]. Features are presented in groups [i], depending on site and user specifics as well as licensed features.

To configure a specific feature, click on the link, A white strip [j] will indicate your location within each feature group.



Configuration Window

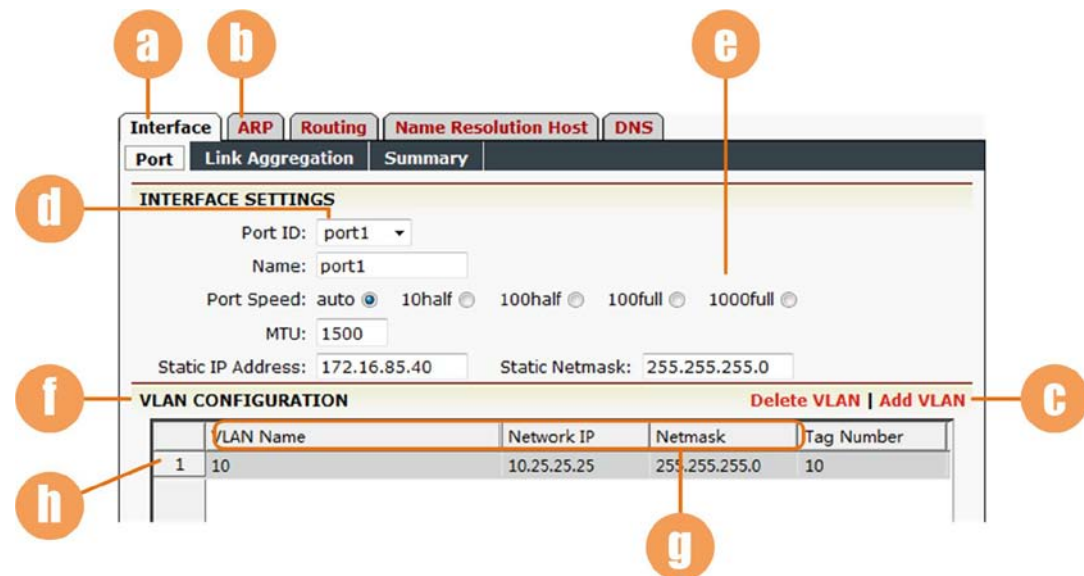
Though individual features will have slightly differing elements for specific configuration windows and tasks, these basic elements remain universal for the WebUI.

There are foreground tabs [\[a\]](#) and background tabs [\[b\]](#) for configuration navigation. Current tabs will be displayed with white backgrounds [\[a\]](#). During configuration you may go through multiple pages under a given tab; to return to the top level, click on the tab [\[a\]](#) again for the desired feature or function.

Some configuration pages may have action links [\[c\]](#) for adding, deleting, saving, canceling or otherwise applying key configuration data. The text of the links will outline the actions to be taken.

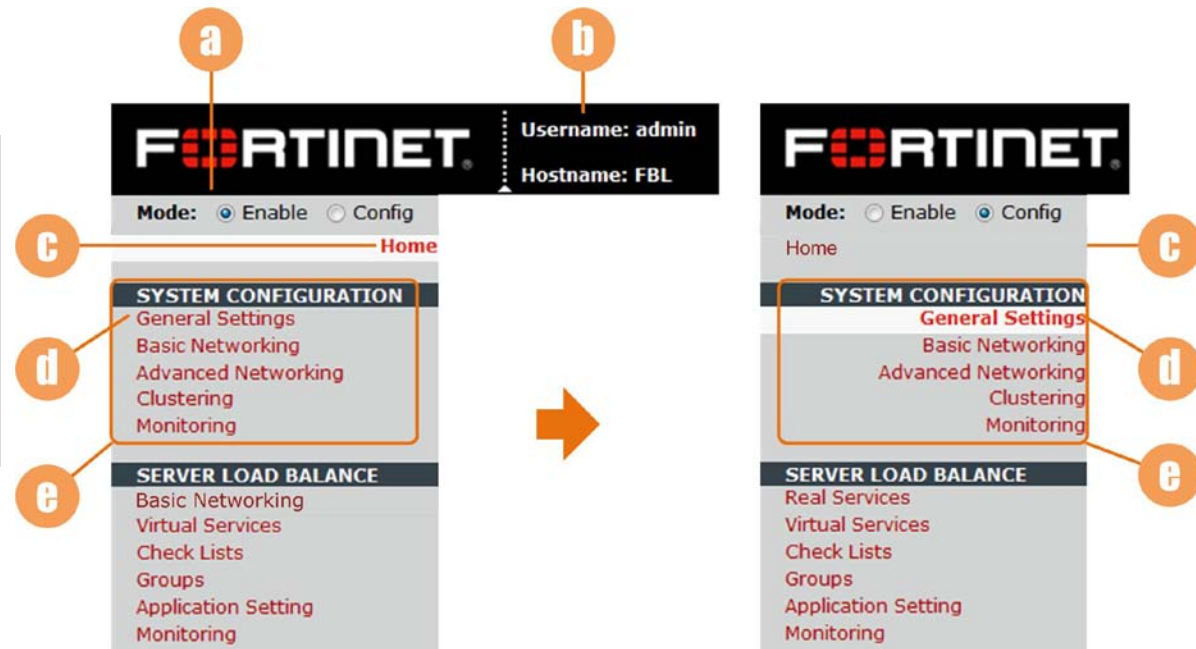
Most configured information will be entered through labeled data entry fields [\[d\]](#) or assigned via radio buttons [\[e\]](#).

You will find active tables [\[f\]](#) with sort options [\[g\]](#) available for displaying critical information. Some tables are sort-ready [\[h\]](#).



Using the FortiBalancer WebUI

When you log into the WebUI, please note that you are first in the **Enable** mode [a]. Also note the default username “admin” and default FortiBalancer appliance hostname “FBL” are displayed [b] within the top bar. Finally, notice that the feature link **Home** [c] is right justified and framed with a white bar. Whenever a feature link like **General Settings** [d] is selected, all related features in the feature group [e] will become right justified with the selected feature singled out with the white bar [d] and the previously selected feature link [c] returns to the left side of the sidebar.



Configuring with the WebUI

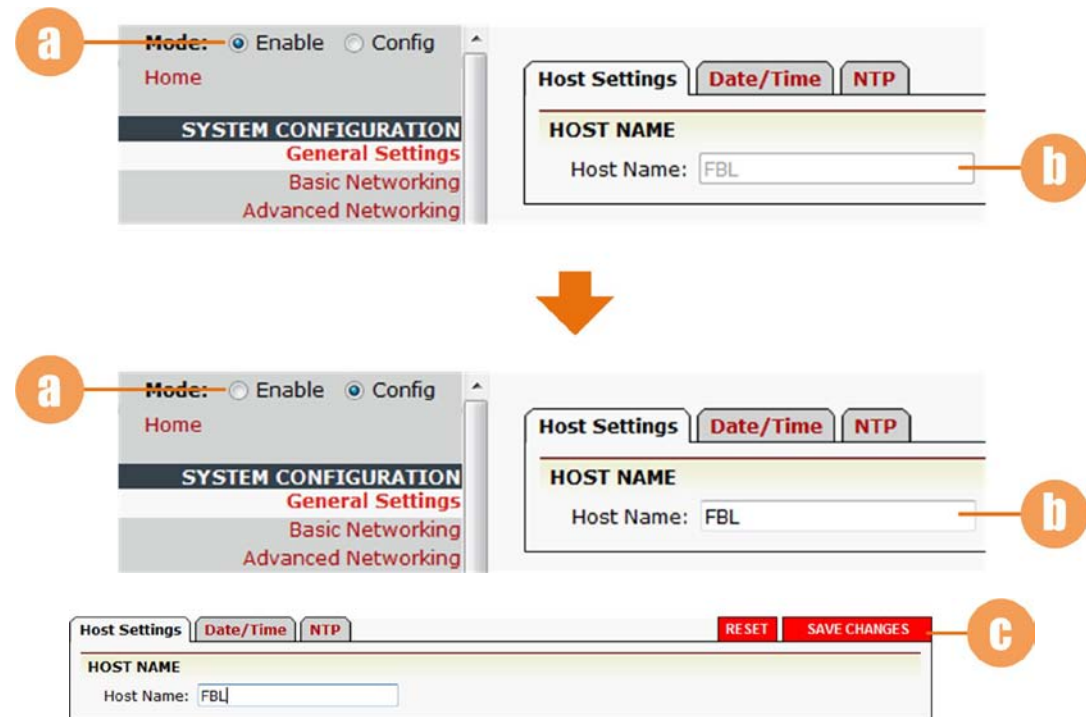
The FortiBalancer appliance offers two levels or modes for the configuration and access to the FBLOS.

The first level is **Enable** mode. Users in this mode have access to a majority of view only operations, such as some statistics pages.

The second level is **Config** mode. It is at this level that the user can make changes to any part of the FortiBalancer appliance configuration. The configuration mode can be accessed by only one user at one time.

To switch between the **Enable** to the **Config** mode, simply click on the radio button [a]. Once in **Config** mode all data fields will be available for configuration [b] for all licensed features.

When changes are made to the existing configuration, “RESET” and “SAVE CHANGES” buttons [c] will appear within the configuration window. You can click on either of them as desired.



Home Page

When you log into the WebUI, the FortiBalancer appliance will display a general status **Home** page. This home page will vary based on appliance model and licensed features.

Basic Information

The home page will have tabs **[a]**: **Basic Information**, **Flight Deck** and **Quick Starts**.

The **Basic Information** will present several pieces of useful information including current system information **[b]**, a list of licensed features **[c]**, available user manuals **[d]**, current resource allocation **[e]**, feature status (enabled/disabled) **[f]** and general network configuration data **[g]**.

On this page, Fortinet will invite you to register your product. By clicking on the “Register Now” button **[h]**, you will be directed to the Fortinet official website to complete the registration. After you finish registration, the button will be displayed as “Registered”.

The screenshot shows the 'Basic Information' tab selected. The page is divided into several sections:

- Basic Information** (Tab **a**): Contains system details like Host Name (FBL), Boot Time, Current Time, Up Time, Model (FortiBalancer 3000), Serial Number, and Software Build Info (FBLOS Rel.FBL.8.2.0.2). A **[Register Now]** button **[h]** is present.
- SYSTEM INFORMATION** (Section **b**): A table listing system details.
- USER MANUAL** (Section **d**): Links to CLI Handbook, WebUI Handbook, and Application Guide, all in PDF format.
- SYSTEM RESOURCES** (Section **e**): Shows CPU Usage at 10%.
- FEATURE STATUS** (Section **f**): Shows status for SNMP Enable and Logging Enable, with links to details.
- ADMIN TOOLS** (Section **f**): Includes a 'View Statistics' button and a dropdown menu.
- SYSTEM/NETWORK CONFIGURATION** (Section **g**): Shows Default Route IP (172.16.85.1) and an Interface Summary table.

Interface Name	Network IP	Netmask	Interface Type	Tag Number	Interface
1 port1	172.16.85.40	255.255.255.0	port1	-	autose

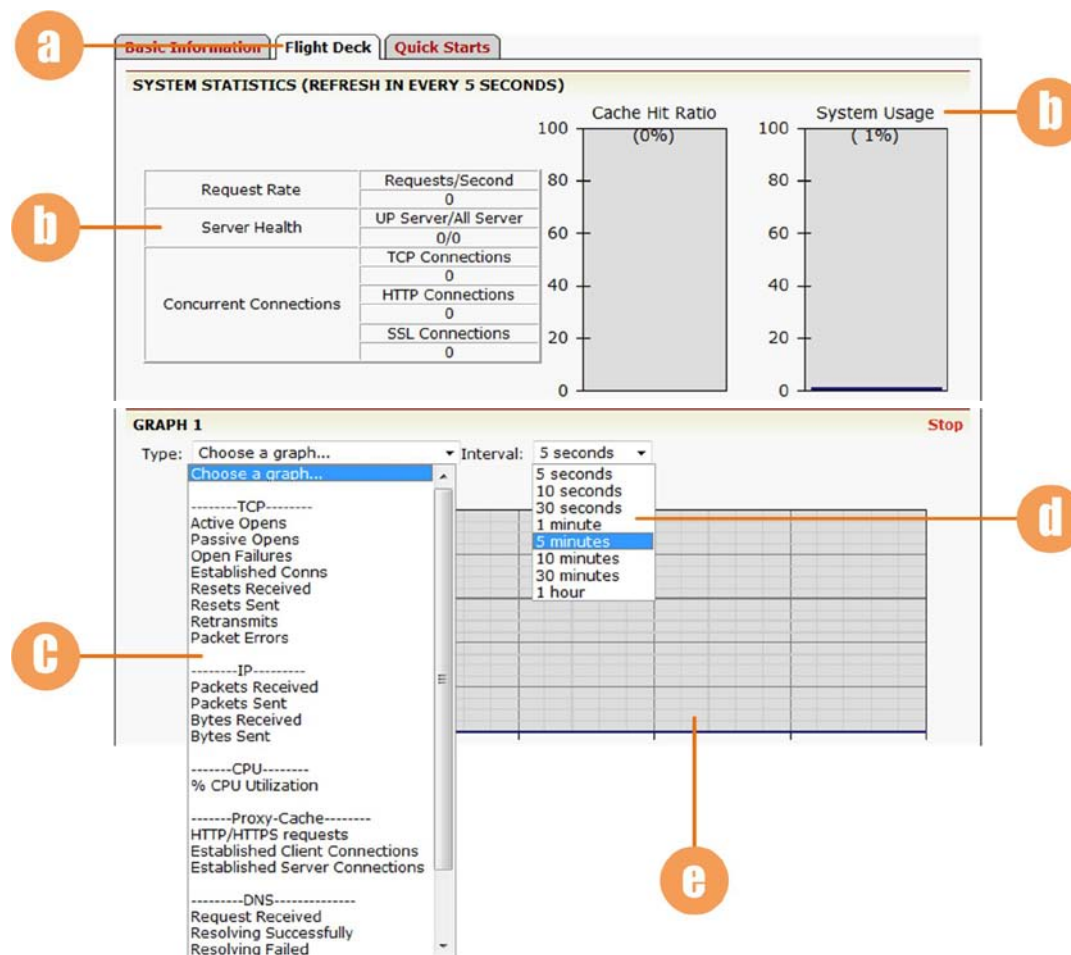
Flight Deck

The **Flight Deck** allows you to supervise system statistics and watch parameter tendency by dynamic graphs.

Make certain that you are in Config mode, and have clicked on the feature link “**Home**” from the sidebar. Click on the “**Flight Deck**” tab, the configuration window will display a panel where there are system statistics and graphs [a].

You can check the Request Rate, Server Health, Concurrent Connections, Cache Hit Ratio and System Usage from System Statistics panel [b].

To view dynamic system parameters by graphs, you can select parameter type [c] and set update interval [d]. The tendency graph will be instantaneously updated [e].



Quick Starts

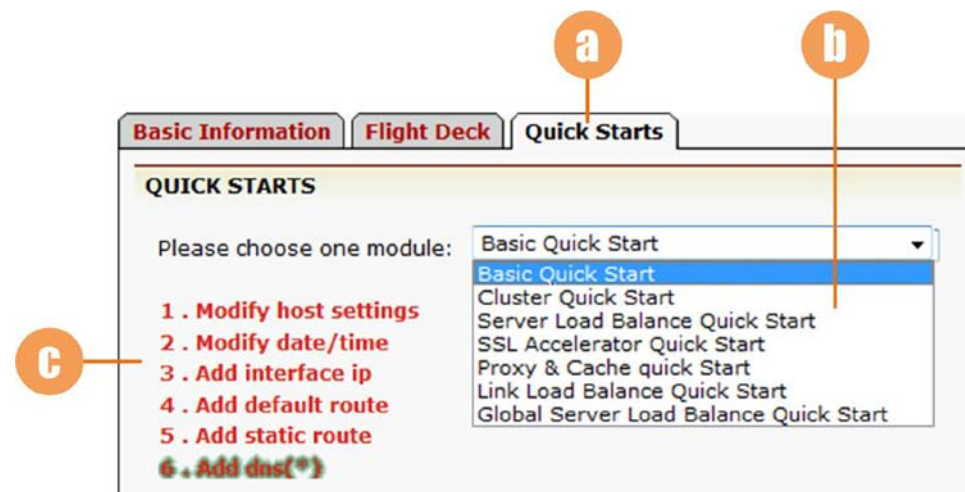
In order to make the total configuration easier and more convenient for FortiBalancer appliance users, we set up “Quick Starts” to guide users to directly complete desired configurations.

To perform quick start configuration, **make certain that you are in Config mode** and have selected the tab “Quick Starts” [\[a\]](#).

Select the “Basic Quick Start” module from the selector [\[b\]](#), and the configuration window will present 6 steps to carry out basic configurations [\[c\]](#).

You may notice the action links are in two colors in the configuration page. The red ones represent the steps that have already been finished, while the green ones indicate you have not configured them yet. Click on the action links according to the numbers of collective steps.

Next, we will take **Basic Quick Start** as an example to illustrate the operation steps of quick starts.



Quick Starts (Continue)

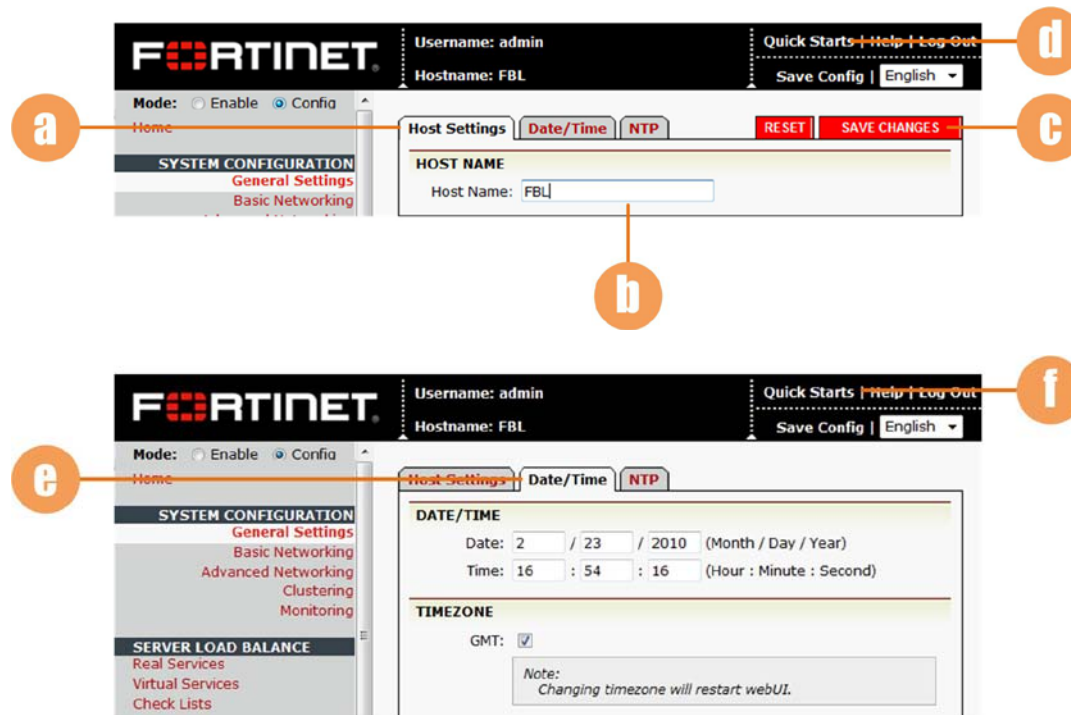
Basic Quick Start:

Click on the action link “1. Modify host settings”, WebUI will guide you to the **Host Settings** configuration page [a]. Fill in the blank with host name [b], click on the button “Save Changes” [c], and then click on the action link “Quick Starts” on the upper right side [d], the configuration window will return to the **Quick Starts** panel (see the former page).

Click on the action link “2. Modify date/time”. For details about configuring this page [e], please refer to the “General Settings” section in the “System Configuration” chapter.

After configuring the Date/Time, click on “Quick Starts” [f] to go back to the Quick Starts main panel in order to perform further tasks.

“3. Add interface ip”, “4. Add default route”, “5. Add static route” and “6. Add dns” action links are all from System Configuration/Basic Networking. Remember to click on the action link “Quick Starts” if you have finished one step and want to move on to another.



Quick Starts (Continue)

You can follow the similar operation steps to Basic Quick Start to complete the following configurations.

Cluster Quick Start [a]:

Please refer to **System Configuration>Clustering** to know more about how to “1. Add cluster” and “2. Enable cluster”.

Server Load Balance Quick Start [b]:

Please refer to **Service Load Balance>Virtual Services** in this handbook.

SSL Accelerator Quick Start [c]:

Please refer to **Proxy>SSL** in this handbook.

Proxy & Cache Quick Start [d]:

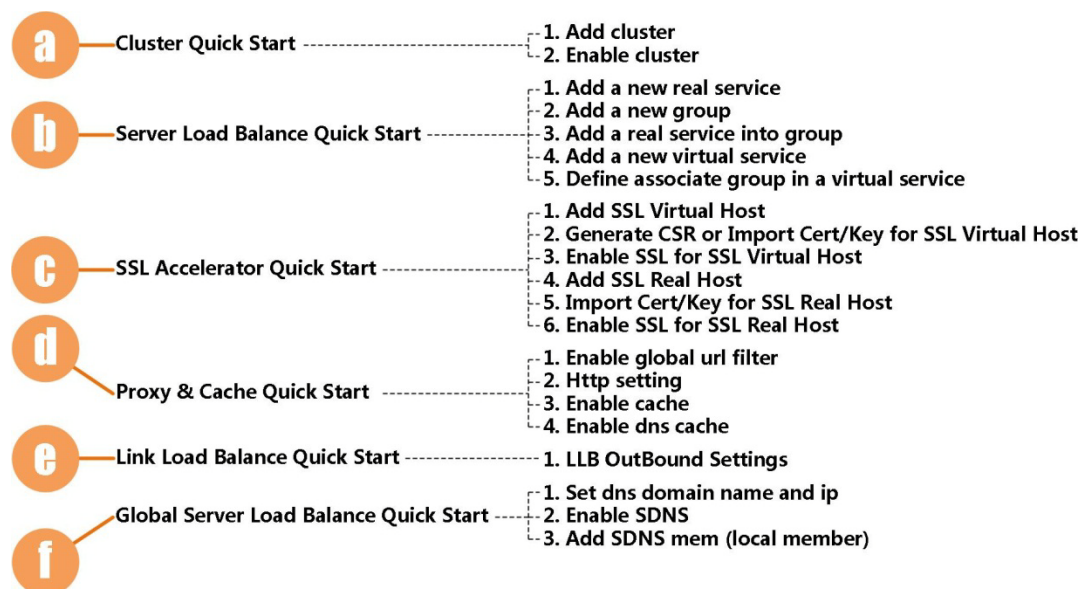
Please refer to **Proxy>Caching Proxy** in this handbook.

Link Load Balance Quick Start [e]:

Please refer to the “**Link Load Balance**” section in the “**Advanced Load Balance**” chapter in this handbook.

Global Server Load Balance Quick Start [f]:

Please refer to **Advanced Load Balance>Global Load Balance** in this handbook.



System Configuration

General Settings

Host Settings

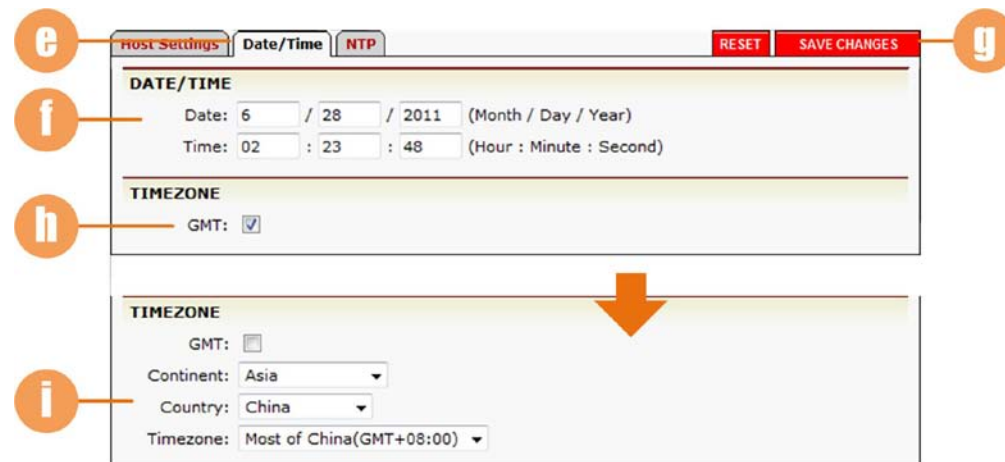
Make certain you are in Config mode, click “General Settings” [a].

On the “Host Settings” page [b], enter the host name for the FortiBalancer appliance [c], and click on the “SAVE CHANGES” button [d] to save your settings.



Date/Time

Click on the “Date/Time” tab [e]. Enter the date and time as desired [f], and click on “SAVE CHANGES” [g]. The FortiBalancer appliance has the default time zone set to GMT [h]. To change this time zone, un-select the time zone box, and configure the time zone properly via the three selectors [i]. Then, remember to click on the “SAVE CHANGES” button [g].



NTP

Click on the “NTP” tab [a]. You can enable NTP by selecting the check box [b]. (Remember to save your setting [c].) Before you enable NTP, you need to first add an NTP Server. Click on the action link “Add” [d], supply the IP address and version number of the NTP server [e]. Click on the action link “Save” [f]. The newly added server will be displayed in the sort ready table [g].

With the NTP function enabled, you can view the NTP statistics in the box [h].

The screenshot shows the Fortinet web interface for NTP configuration. The top navigation bar includes tabs for Host Settings, Date/Time, and NTP (highlighted with callout 'a'). To the right of the tabs are buttons for RESET and SAVE CHANGES (callout 'c'). Below the tabs is the NTP SETTINGS section, which includes an 'Enable NTP' checkbox (callout 'b'). Underneath is the NTP SERVERS table (callout 'g'), which has an 'Add' link (callout 'd'). The table contains one entry with ID 1, IP 210.72.145.44, and version 4. Below the table is the 'ADD NTP SERVER' form (callout 'e'), which has input fields for 'NTP Server IP' and a dropdown for 'NTP Server Version' (set to 4). The form has buttons for Cancel, Save & Add Another, and Save (callout 'f'). At the bottom is the 'VIEW NTP STATISTICS' section (callout 'h') displaying a text-based summary of the NTP server's status and statistics.

	NTP Server	NTP Version
1	210.72.145.44	4

```

ntp server 210.72.145.44 4
ntp on
time since restart:    0
time since reset:     0
packets received:     3
packets processed:    0
current version:      0
    
```

Basic Networking

Make certain you are in Config mode and click “Basic Networking” [a].

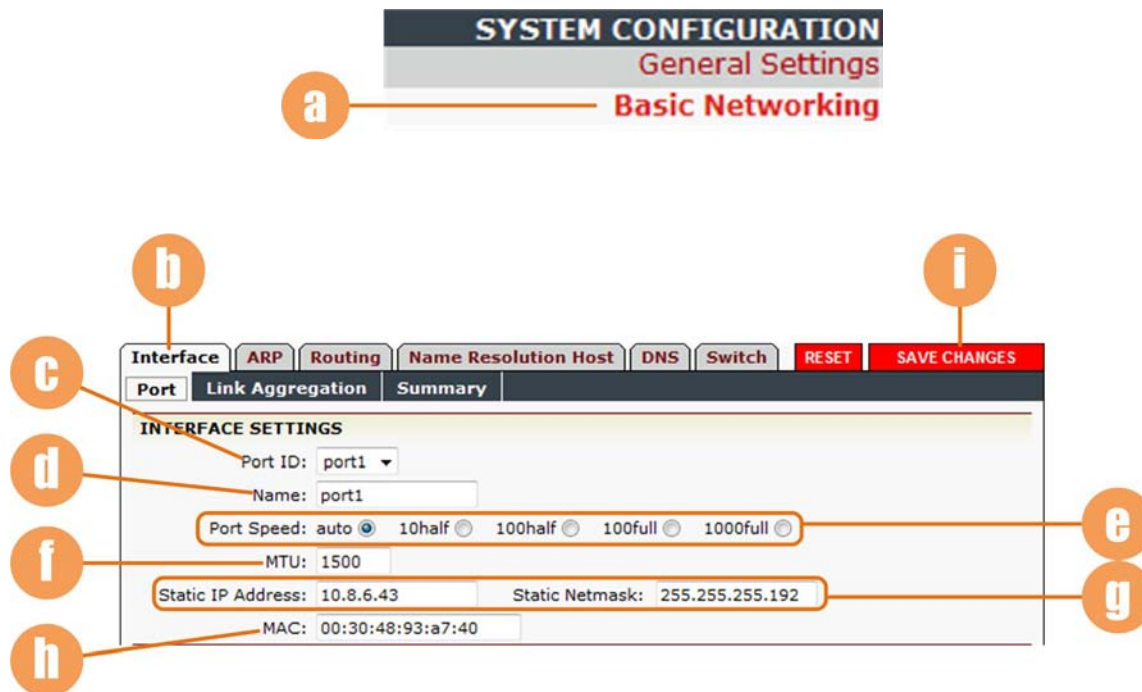
Interface

To complete the interface settings, select the tab “Interface” and its sub tab “Port” [b].

Port

To perform interface settings, select port ID via the selector [c], supply its name [d], set the port speed via the radio buttons [e], supply the MTU value [f] and supply the static IP address and static netmask [g]. Besides, you can change the MAC address of the system interface [h].

After confirming the input information, click on the “SAVE CHANGES” button [i] to save your settings.



Interface (Continue)

Port (Continue)

To add VLAN, click on the action link “Add VLAN” [\[a\]](#). In the new configuration window, supply the VLAN name, IP address and netmask, and VLAN ID [\[b\]](#), and click on the action link “Save” [\[c\]](#). The new VLAN will appear in the sort ready table [\[d\]](#).

To add MNET, click on the action link “Add MNET” [\[e\]](#). In the new configuration window, supply the MNET name, IP address and netmask [\[f\]](#), and click on the action link “Save” [\[g\]](#). The new MNET will appear in the sort ready table [\[h\]](#).

The diagram illustrates the configuration process for VLAN and MNET. It consists of two main sections: VLAN CONFIGURATION and MNET CONFIGURATION, each with an associated 'ADD' form.

VLAN CONFIGURATION:

- Table:** A table with columns: VLAN Name, Network IP, Netmask, and Tag Number. A callout [\[d\]](#) points to the table.
- Action Link:** A callout [\[a\]](#) points to the "Add VLAN" link in the top right corner.
- Form:** An orange arrow points from the table to the "ADD VLAN" form. The form includes:
 - Port Name:
 - VLAN Name:
 - Network IP:
 - Netmask:
 - Tag Number: (1 - 4094)
- Action Links:** Callout [\[c\]](#) points to the "Save" link in the bottom right corner of the form.

MNET CONFIGURATION:

- Table:** A table with columns: MNET Name, Network IP, and Netmask. A callout [\[h\]](#) points to the table.
- Action Link:** A callout [\[e\]](#) points to the "Add MNET" link in the top right corner.
- Form:** An orange arrow points from the table to the "ADD MNET" form. The form includes:
 - Port Name:
 - MNET Name:
 - Network IP:
 - Netmask:
- Action Links:** Callout [\[g\]](#) points to the "Save" link in the bottom right corner of the form.

Interface (Continue)

Link Aggregation

Select the “Link Aggregation” sub tab [a].

First select the Bond ID via the selector, and supply the name of the bond interface [b]. Then, supply the IP address and netmask of the bond interface [c]. Click on the “SAVE CHANGES” button to save your settings [d].

To add a system interface into the bond interface, click on the action link “Add Bond” [e]. In the new window, select a desired system interface, set it as the primary or backup interface of the bond [f], and click on “Save” [g]. The configuration will be displayed in the sort ready table [h].

The screenshot displays the Fortinet web interface for configuring a bond interface. The top navigation bar includes tabs for Interface, ARP, Routing, Name Resolution Host, and DNS, along with a red 'SAVE CHANGES' button. The 'Link Aggregation' sub-tab is selected. The 'INTERFACE SETTINGS' section contains fields for Bond ID (bond1), Name (bond1), Bond Speed (auto), and MTU (1500). Below these are fields for Static IP Address and Static Netmask. A table lists the System Interface Name and Interface Type. An 'Add Bond' link is present. A modal window titled 'ADD BOND' is open, showing fields for Bond Name (bond1), Interface Name (port1), and Interface Type (Primary selected). A large orange arrow points from the 'Add Bond' link to the 'ADD BOND' modal window. Various steps are labeled with letters a through g in orange circles.

Interface (Continue)

Link Aggregation (Continue)

The FortiBalancer appliance supports configuring MNET or VLAN on bond interface. The bond interface configuration must be performed before configuring MNET/VLAN on it.

To add VLAN, click on the action link “Add VLAN” [\[a\]](#). In the new window, supply the VLAN name, IP address and netmask, and VLAN ID [\[b\]](#), and click on “Save” [\[c\]](#). The new VLAN will appear in the sort ready table [\[d\]](#).

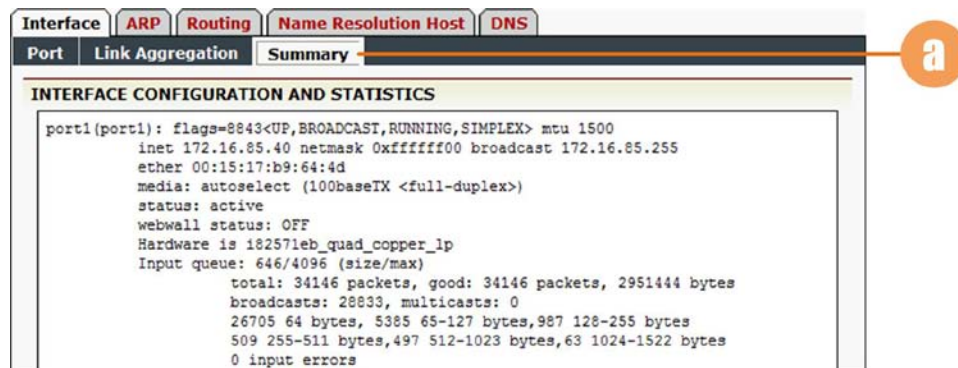
To add MNET, click on the action link “Add MNET” [\[e\]](#). In the new window, supply the MNET name, IP address and netmask [\[f\]](#), and click on “Save” [\[g\]](#). The new MNET will appear in the sort ready table [\[h\]](#).

The screenshot displays two configuration windows from the Fortinet management interface. The top window is titled "VLAN CONFIGURATION" and features a table with columns: VLAN Name, Network IP, Netmask, and Tag Number. An orange callout 'a' points to the "Add VLAN" link in the top right corner. Below this table is the "ADD VLAN" form, which includes input fields for Bond Name (pre-filled with "bond1"), VLAN Name, Network IP, Netmask, and Tag Number (with a range of 1-4094). An orange callout 'b' points to the VLAN Name field. An orange callout 'c' points to the "Save" button. An orange arrow points down to the second window, titled "MNET CONFIGURATION". This window also has a table with columns: MNET Name, Network IP, and Netmask. An orange callout 'e' points to the "Add MNET" link in the top right corner. Below is the "ADD MNET" form, with input fields for Bond Name (pre-filled with "bond1"), MNET Name, Network IP, and Netmask. An orange callout 'f' points to the MNET Name field. An orange callout 'g' points to the "Save" button. An orange callout 'h' points to the MNET Name field in the table above. Orange callouts 'd' and 'c' are also present on the left side of the VLAN CONFIGURATION window, pointing to the table and the "Add VLAN" link respectively.

Interface (Continue)

Summary

To view current setup and statistics, click on the sub tab “Summary” [\[a\]](#).



The screenshot shows the Fortinet web interface with the 'Interface' tab selected. The 'Summary' sub-tab is active, displaying the 'INTERFACE CONFIGURATION AND STATISTICS' for 'port1'. The configuration details are as follows:

```
port1(port1): flags=8843<UP,BROADCAST,RUNNING,SIMPLEX> mtu 1500
inet 172.16.85.40 netmask 0xfffff00 broadcast 172.16.85.255
ether 00:15:17:b9:64:4d
media: autoselect (100baseTX <full-duplex>)
status: active
webwall status: OFF
Hardware is 182571eb_quad_copper_lp
Input queue: 646/4096 (size/max)
  total: 34146 packets, good: 34146 packets, 2951444 bytes
  broadcasts: 28833, multicasts: 0
  26705 64 bytes, 5385 65-127 bytes, 987 128-255 bytes
  509 255-511 bytes, 497 512-1023 bytes, 63 1024-1522 bytes
  0 input errors
```

An orange circle with the letter 'a' is positioned to the right of the screenshot, corresponding to the link in the text above.

ARP

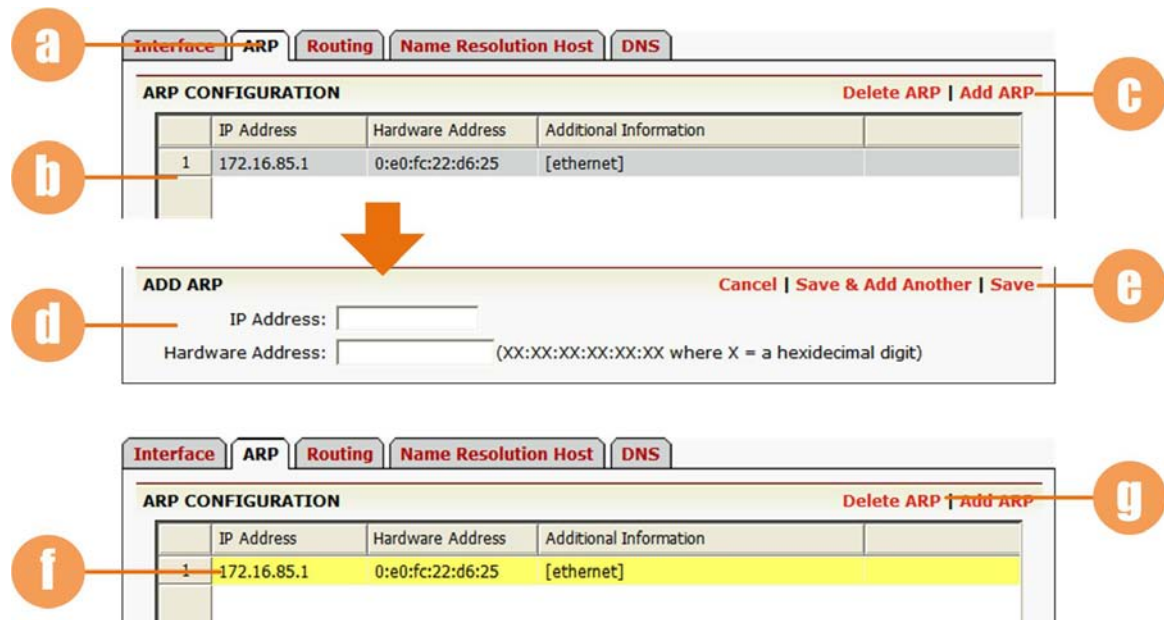
Extreme care should be taken when altering the ARP table. Administrators should not clear ARP entries for IP addresses that are already assigned to establish.

Click on the “ARP” tab [a] and the main window will display an ARP table.

The table contains sort-ready columns [b]. To add an ARP table entry, click on the “Add ARP” action link [c]. A new configuration window will appear.

Enter appropriate IP and hardware address in the data fields [d]. Click on the desired action link [e].

To remove an ARP entry, select the desired entry from the displayed list [f] and click on “Delete ARP” action link [g]. A new window will appear, click “OK” to delete ARP entry, click “cancel” to keep the ARP entry.



Routing

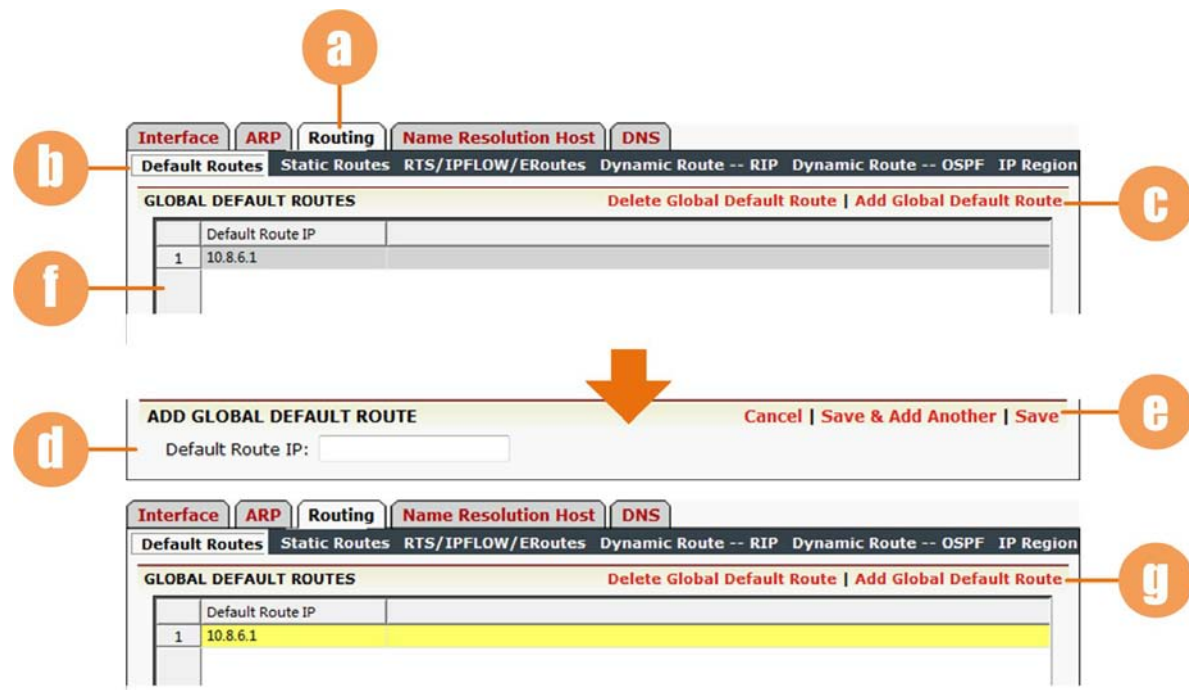
Make certain you are in **Config mode** and have selected the “**Routing**” tab [a]. Six sub tabs are displayed [b].

Default Routes

Verify and/or change the default route. To add a global default route, click on the action link [c] and the configuration window will present configuration field for the route.

Supply the destination IP in the field [d]. Click on the desired action link [e] to continue. Configured routes are displayed in the table [f].

To remove a global default route, simply select the destination from the displayed list and click on the “Delete Global Default Route” action link [g]. A new window will appear, click “OK” to delete ARP entry, click “cancel” to keep the ARP entry.



Routing (Continue)

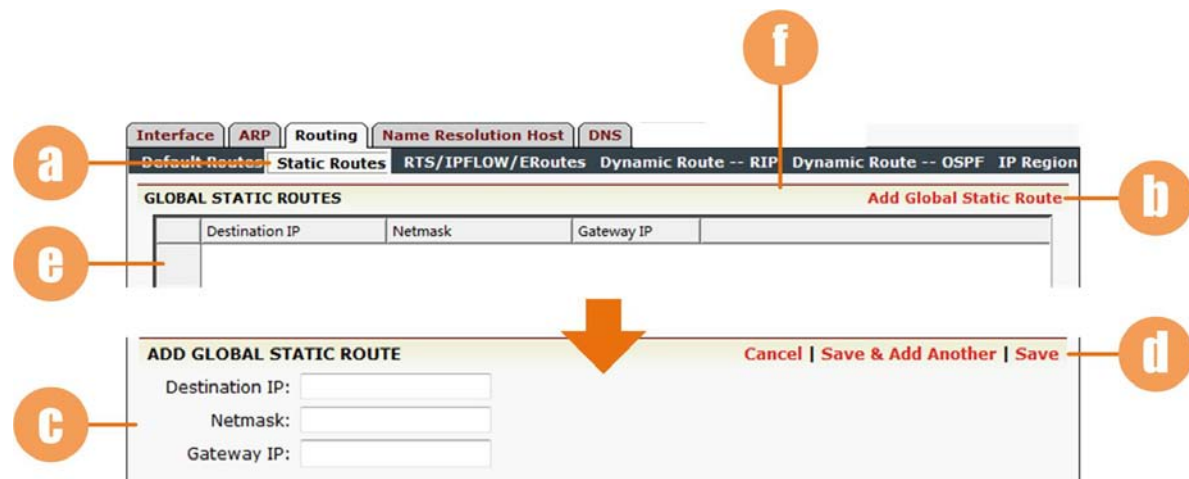
Static Routes

Select the “**Static Routes**” sub tab to add a static route [a].

Click on the action link “Add Global Static Route” [b], and the configuration window will present data fields for adding a static route.

Supply the destination IP, netmask and gateway IP [c], and click on the desired action link to continue [d]. Configured routes will be displayed in a sort ready table [e].

To remove a global static route, click on the action link “Delete Global Static Route” [f]. A new window will appear, click “OK” to delete ARP entry, click “cancel” to keep the ARP entry.



Routing (Continue)

RTS/IPFLOW/ERoute

Make certain that you select the “RTS/IPFLOW/ERoutes” sub tab [\[a\]](#).

Enable RTS functionality via the selector, and supply the desired expiration time [\[b\]](#). To turn on the RTS function, the option “on all” means RTS records all external senders that send packets to the unit, and all the packets will be sent back along the route which they came from. “on gateway” means RTS records external senders as configured gateways, and only the packets coming from these gateways will be sent back along the route which they came from.

Select the check box to enable IPFLOW, and supply the expiration time and priority [\[c\]](#).

To add an eroute, click on the action link “Add” [\[d\]](#), and then the configuration window will display text fields for adding an eroute [\[e\]](#).

Fill in these fields, and click on the desired action link to continue [\[f\]](#). If the eroute is added successfully, it will be displayed in the table [\[g\]](#).

Interface **ARP** **Routing** **Name Resolution Host** **DNS**

Default Routes **Static Routes** **RTS/IPFLOW/ERoutes** **Dynamic Route -- RIP** **Dynamic Route -- OSPF**

RTS SETTINGS

Enable RTS: **on all** [off](#) [on all](#) [on gateway](#)

RTS Expires in: 60 Seconds

IPFLOW SETTINGS

Enable IPFLOW: ☐

IPFLOW Expires in: 60 Seconds

IPFLOW Priority: 1000 (0 - 1999)

ERoutes [Add](#)

Name	Priority	Source Ip/Mask:Port	Destination Ip/Mask:Port	Protocol

ADD ERROUTE [Cancel](#) [Save & Add Another](#) [Save](#)

Name:

Priority: (1001 - 1999)

Source IP:

Source NetMask:

Source Port:

Destination IP:

Destination NetMask:

Destination Port:

Protocol: **any**

Gateway:

Weight: 1 (Default is 1)

Routing (Continue)

RTS/IPFLOW/Eroutes (Continue)

You can also check the following items:

NON-Eroutes [\[a\]](#).

RTS Statistics [\[b\]](#).

IPFLOW Statistics [\[c\]](#).

Eroute Statistics [\[d\]](#).

a

NON-EROUTES

	Name	Priority	Source Ip/Mask:Port	Destination Ip/Mask:Port	Protocol
1	interface	2000	0.0.0.0/0.0.0.0:0	127.0.0.1/255.255.255.255:0	any
2	interface	2000	0.0.0.0/0.0.0.0:0	10.3.0.0/255.255.0.0:0	any

b

RTS STATISTICS

Clear

Rts Statistics:
0 rts hits
0 source MAC matched

c

IPFLOW STATISTICS

Clear

Ipflow Statistics:
0 ipflow hits

d

EROUTE STATISTICS

Clear

Eroute Statistics:
0 eroute, 0 lookup, 0 fail

Routing (Continue)

Dynamic Route--RIP

Select the “**Dynamic Route--RIP**” sub tab [a]. You can enable RIP by selecting the check box [b]. If you enable the RIP, you need to further specify the version of RIP via the selector [c]. Then, click on “SAVE CHANGES” button [d] when it appears.

Click on the action link “Add” [e] and a new configuration page will be presented. Supply the destination IP address and netmask [f] properly and click on the “Save” action link [g]. Then, the added information will be displayed in the table [h]. You can clear RIP settings by clicking on the “Clear” button [i].

After you set the RIP network properly, the information of the routes dynamically detected will be displayed in the table [j].

Dynamic Route -- RIP

RIP SETTINGS

Enable RIP: ☒ [b]

Version: 2 [c]

Clear RIP: [Clear](#) [i]

RIP NETWORK

Destination IP	Netmask

[Add](#) [e]

RIP NETWORK

Destination IP: [f]

Netmask: [f]

[Cancel](#) | [Save & Add Another](#) | [Save](#) [g]

RIP ROUTES

Destination IP	Netmask	Gateway IP

[j]

Routing (Continue)

Dynamic Route--OSPF

Select the “**Dynamic Route--OSPF**” sub tab [a]. You can enable OSPF by selecting the check box [b]. Then, click on “**SAVE CHANGES**” button [c] when it appears.

Click on the action link “**Add**” [d] and a new configuration page will be presented. Supply the destination IP address, netmask and area ID [e] properly and click on the “**Save**” action link [f]. Then, the added information will be displayed in the table [g]. You can clear OSPF settings by clicking on the “**Clear**” button [h].

After you set the OSPF network properly, the information of the routes dynamically detected will be displayed in the table [i].

Dynamic Route--OSPF

Enable OSPF: ☒ [b]

Clear OSPF: [Clear](#) [h]

[Delete](#) | [Add](#) [d]

	Destination IP	Netmask	Area ID
1	10.3.10.0	255.255.255.0	10
2	10.3.20.0	255.255.255.0	20

[Cancel](#) | [Save & Add Another](#) | [Save](#) [f]

OSPF NETWORK

Destination IP:

Netmask:

Area ID: (0 - 4294967295)

OSPF ROUTES

	Destination IP	Netmask	Gateway IP
--	----------------	---------	------------

Routing (Continue)

IP Region

Select the “**IP Region**” sub tab [a]. To set the route for IP region, select the desired IP region file name via the selector, and supply the gateway IP, priority and weight [b] properly and click on the “Add” action link [c]. Then, the added information will be displayed in the table [d]. You can clear IP region route settings by clicking on the “Clear” button [c].

Clicking on the action link “IP Region Table” and “IP Region Proximity” [e] will direct you to the related configuration pages.

IP REGION ROUTE Add | Delete | Clear

Name: asdfs
 Gateway: 10.8.6.1
 Priority: 1999
 Weight: 1

	Name	Gateway	Priority	Weight
1	predefined_cernet	10.8.6.1	1999	1

IP Region Table | IP Region Proximity

Name Resolution Host

Make certain you are in **Config mode** and have selected the **"Name Resolution Host"** tab [a]. To add a new host, click on the action link **"Add Network Host"** [b].

Within the supplied configuration window, supply the host name and the host IP address in the text fields [c]. Once completed, click the next desired action link [d].

All added hosts will be displayed in a sort enabled table [e] for editing.

To delete a host, select the host name from the table [e] and click on the desired action link [f]. A new window will appear, click **"OK"** to delete ARP entry, click **"cancel"** to keep the ARP entry.

The diagram illustrates the process of adding and managing a Name Resolution Host through the Fortinet configuration interface. It consists of three main screenshots with numbered callouts (a-f) indicating specific actions.

Step 1: Main Configuration Window
 Screenshot (a) shows the **Interface** tab selected, with sub-tabs for **ARP**, **Routing**, **Name Resolution Host**, and **DNS**. The **Name Resolution Host** tab is active. Below the tabs is a table titled **NETWORK HOSTS** with columns **Host Name** and **Host IP**. The table contains one entry: **Sample** with IP **10.3.0.6**. To the right of the table are two action links: **Delete Network Host** and **Add Network Host**. Callout (a) points to the **Name Resolution Host** tab, and callout (b) points to the **Add Network Host** link.

Step 2: Add Network Host Form
 An orange arrow points from the **Add Network Host** link in the first screenshot to the second screenshot. Screenshot (c) shows the **ADD NETWORK HOST** form. It contains two text input fields: **Host Name:** and **Host IP:**. To the right of the form are three action links: **Cancel**, **Save & Add Another**, and **Save**. Callout (c) points to the **Host Name** field, and callout (d) points to the **Save** link.

Step 3: Updated Network Hosts Table
 An orange arrow points from the **Save** link in the second screenshot to the third screenshot. Screenshot (e) shows the **NETWORK HOSTS** table after the new host has been added. The table now contains two entries: **Sample** (10.3.0.6) and **sample** (10.3.0.6). The **sample** entry is highlighted in yellow. To the right of the table are the same two action links: **Delete Network Host** and **Add Network Host**. Callout (e) points to the **sample** entry in the table, and callout (f) points to the **Add Network Host** link.

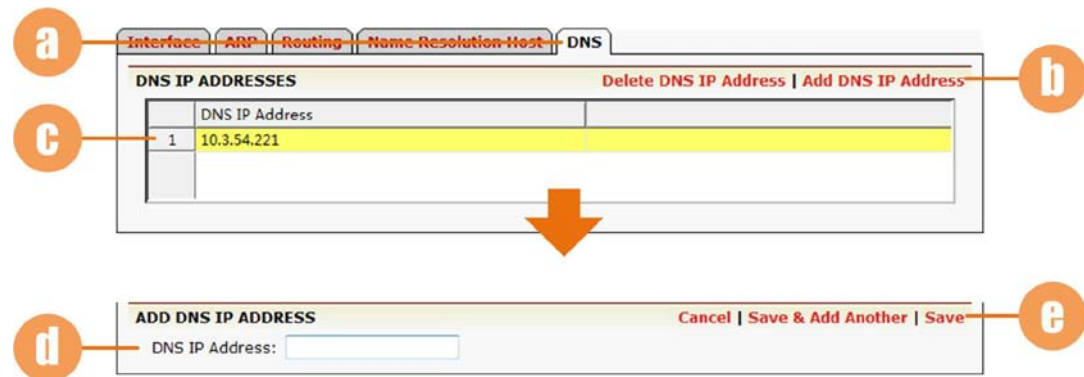
DNS

Make certain you are in **Config mode** and have selected the “DNS” tab [a].

From this configuration page, you may edit or assign DNS IP addresses by clicking on the action links [b].

Enter DNS IP address in dotted IP format [d] and click on the desired action link [e].

To delete a DNS, select the DNS address from the table [c] and click on the desired action link [b]. A new window will appear, click “OK” to delete ARP entry, click “cancel” to keep the ARP entry.



Advanced Networking

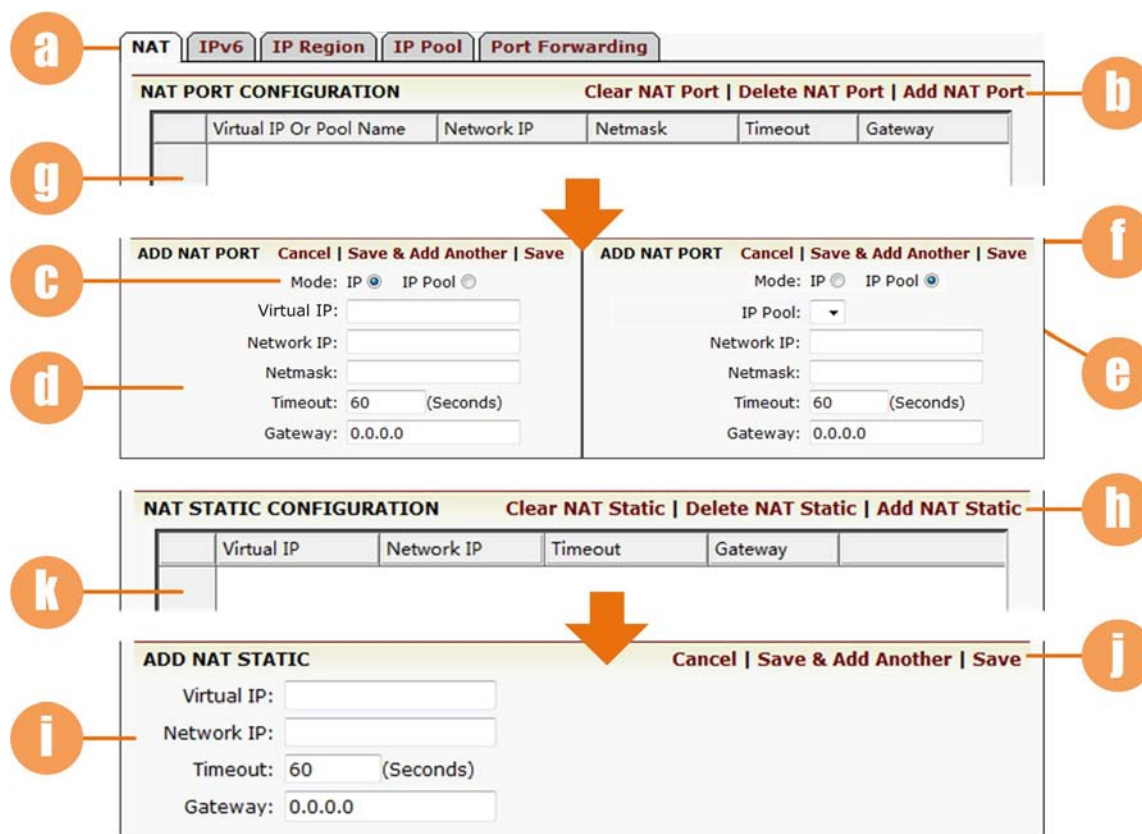
NAT

NAT converts the address behind the FortiBalancer appliance into one IP address for the Internet and vice versa. NAT also keeps individual IP addresses hidden from the Internet.

Make certain you are in Config mode, and have selected the “Advanced Networking” feature link from the sidebar, and further selected the “NAT” tab [\[a\]](#). The configuration window displays the sort enabled table of previously setup NATs.

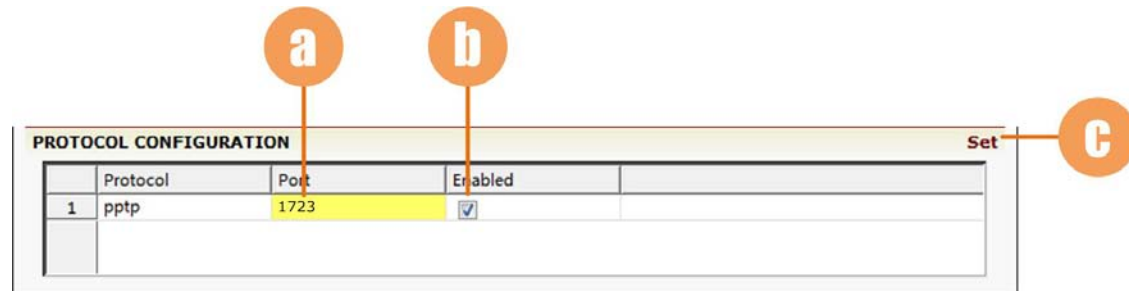
To create an NAT port configuration, click on the “Add NAT Port” action link [\[b\]](#). The configuration window will present some new fields. First, select the “IP” or “IP Pool” mode via the radio buttons [\[c\]](#), and then supply the required virtual IP/IP pool name, network IP, netmask, timeout length (defaults to 60 seconds) and gateway IP [\[d\]](#). If “IP Pool” mode is selected, you should first select desired IP pool name via the selector [\[e\]](#). Then, click on “Save” [\[f\]](#), and the created NAT port configuration will be displayed in the table [\[g\]](#). You can double click on an item in the table to edit the timeout value.

To create static NAT, click on “Add NAT Static” action link [\[h\]](#). The window will present four text fields [\[i\]](#), where you can supply the virtual IP, network IP, timeout length (defaults to 60 seconds) and gateway IP. Then, click on “Save” [\[j\]](#), and the created static NAT configuration will be displayed in the table [\[k\]](#). You can double click on an item in the table to edit the timeout value.



NAT (Continue)

To enable the PPTP protocol or change its port number, you can double click on the Port column to change the PPTP port [\[a\]](#), and click the “Enable” check box to enable the PPTP protocol [\[b\]](#). At last, click on the “Set” button to save your changes [\[c\]](#).



The screenshot shows the 'PROTOCOL CONFIGURATION' table. It has four columns: 'Protocol', 'Port', 'Enabled', and an empty column. The first row is highlighted in yellow and contains the values '1', 'pptp', '1723', and a checked checkbox. Above the 'Port' column, there is an orange circle with the letter 'a' and a line pointing to the '1723' value. Above the 'Enabled' column, there is an orange circle with the letter 'b' and a line pointing to the checked checkbox. To the right of the table, there is a 'Set' button with an orange circle containing the letter 'c' and a line pointing to it.

	Protocol	Port	Enabled	
1	pptp	1723	☒	

IPv6

Fortinet IPv6 implementation includes two parts currently: IPv6 routing and NAT-PT (Network Address Translation-Protocol Translation).

Select the “**IPv6**” tab [\[a\]](#), and the window displays the “Addresses” sub tab by default [\[b\]](#).

Addresses

This page allows you to set the IPv6 addresses for system interfaces. First, specify the interface name via the selector, and further input the desired IPv6 address and prefix length in the text fields [\[c\]](#).

Then, click on the “Set” action link [\[d\]](#). The configuration will be displayed in the sort ready table [\[e\]](#). **Note:** Only one address can be configured on each interface.

You can also click on the “Delete” action link to delete a configuration item in the table or “Clear” to delete all the configurations [\[d\]](#).

The screenshot shows the Fortinet web interface for IPv6 configuration. The top navigation bar includes tabs for NAT, **IPv6** (selected), IP Region, IP Pool, and Port Forwarding. Below this, the sub-tabs are **Addresses** (selected), Routing, and NATPT. The main content area is titled "IPv6 ADDRESS" and contains the following elements:

- Interface Name:** A dropdown menu currently showing "port1".
- IPv6 Address:** A text input field.
- Prefix Length:** A text input field with a range indicator "(1 - 128)".
- Action Links:** "Set", "Delete", and "Clear" buttons located at the top right of the configuration area.
- Table:** A table with 4 columns: "Interface Name", "IPv6 Address", and "Prefix Length". It contains 4 rows of data for interfaces port1, port2, port3, and port4.

Callouts in the image point to the following elements:

- a:** The "IPv6" tab in the top navigation bar.
- b:** The "Addresses" sub-tab.
- c:** The "Interface Name" dropdown, "IPv6 Address" field, and "Prefix Length" field.
- d:** The "Set", "Delete", and "Clear" action buttons.
- e:** The table displaying the IPv6 address configurations.

	Interface Name	IPv6 Address	Prefix Length
1	port1		
2	port2		
3	port3		
4	port4		

IPv6 (Continue)

Routing

Select the “**Routing**” tab [\[a\]](#).

First, you can configure the default IPv6 gateway. Input the default gateway address in the text field (should be a global unicast IPv6 address) [\[b\]](#), and click on the “Set” action link to save your configuration [\[c\]](#).

Then, you can set the IPv6 static route. Input the destination address, prefix length and gateway IP address (the destination address and gateway address should be global unicast IPv6 addresses) in the text fields [\[d\]](#) and click on the “Add” action link [\[e\]](#). The configuration will be displayed in the sort ready table [\[f\]](#).

Routing

DEFAULT ROUTE [Set](#) [Delete](#)

Default Route:

STATIC ROUTES [Add](#)

Destination:

Prefix Length: (1 - 128)

Gateway:

Destination	Prefix Length	Gateway

IPv6 (Continue)

NATPT

Select the “NATPT” tab [\[a\]](#).

First, you can activate the NATPT translation by selecting the “Enable NATPT” check box and setting the IPv6 prefix [\[b\]](#), and then click on the “Set” action link [\[c\]](#) to save your configuration.

To set a dynamic IPv6-to-IPv4 translation rule, you can input the IPv4 address, start port and end port in the text fields [\[d\]](#), and click on the “Set” action link [\[e\]](#) to save your configuration.

To set a static IPv4-to-IPv6 translation rule, you can input the IPv4 addresses and IPv6 address in the text fields [\[f\]](#), and click on the “Add” action link [\[g\]](#). The configuration will be displayed in the sort ready table [\[h\]](#).

The window also displays the NAT-PT translation table [\[i\]](#).

The screenshot shows the Fortinet web interface for NATPT configuration. The top navigation bar includes tabs for NAT, IPv6, IP Region, IP Pool, and Port Forwarding. The 'NATPT' tab is selected, and the 'NATPT' sub-tab is active. The interface is divided into several sections:

- IPv6 NATPT SETTINGS**: Contains an 'Enable NATPT' checkbox and a 'Prefix' text field. A 'Set' link is on the right.
- NATPT IPv6 TO IPv4 SETTINGS**: Contains an 'IPv4 Address' text field, 'Start Port' and 'End Port' text fields (both with a range of 1025 - 65535), and 'Set' and 'Delete' links.
- NATPT IPv4 TO IPv6 SETTINGS**: Contains an 'IPv4 Address' text field, an 'IPv6 Address' text field, and an 'Add' link.
- NATPT TRANSLATIONS**: A table with columns for Protocol, Local Address(src), Local Address(dst), and Remote Address.

Callouts a-i point to specific elements: a points to the NATPT tab, b points to the Prefix field, c points to the Set link in the IPv6 NATPT settings, d points to the IPv4 Address field in the IPv6 to IPv4 settings, e points to the Set link in the IPv6 to IPv4 settings, f points to the IPv4 Address field in the IPv4 to IPv6 settings, g points to the Add link in the IPv4 to IPv6 settings, h points to the NATPT TRANSLATIONS table, and i points to the table header.

IP Region

Make certain you are in **Config mode** and have selected the “**IP Region**” tab [\[a\]](#).

To import an existing IP region table via a local file, you can select the radio button “**Local File**” [\[b\]](#), and specify the location of the local file [\[c\]](#).

To import an existing IP region table via FTP, you can select the radio button “**FTP**” [\[e\]](#), and specify the server address [\[f\]](#).

To import an existing IP region table via HTTP, you can select the radio button “**HTTP**” [\[g\]](#), and specify the server address [\[h\]](#).

After confirming the supplied information, click on the action link “**Import**” to import the IP region table [\[d\]](#). The name of the IP region table files imported successfully will be displayed in the table [\[i\]](#).

To remove an IP region table file, simply select the desired file name from the displayed list and click on the “**Delete**” action link [\[d\]](#). A new window will appear, click “**OK**” to delete the file, or click “**cancel**” to cancel the deletion.

Double click on an IP region table file in the table, and the contents of the files will be displayed [\[j\]](#).

Clicking on the action link “**IP Region Route**” and “**IP Region Proximity**” [\[k\]](#) will direct you to the related configuration pages..

The screenshot shows the Fortinet web interface for the IP Region configuration. The tabs at the top are NAT, IPv6, IP Region (selected), IP Pool, and Port Forwarding. Below the tabs, there are three sections for importing IP region tables: Local File, FTP, and HTTP. Each section has a Name field, a URL field, and an Import button. A table below shows the list of imported IP region tables. At the bottom, there are links for IP Region Route and IP Region Proximity.

Callouts:

- a**: IP Region tab
- b**: Local File radio button
- c**: Local File field
- d**: Import button
- e**: FTP radio button
- f**: FTP URL field
- g**: HTTP radio button
- h**: HTTP URL field
- i**: Table of imported IP region tables
- j**: Double-click on a table entry
- k**: IP Region Route and IP Region Proximity links

	Name	
1	asadf	
2	predefined_cernet	
3	predefined_cnc	
4	predefined_ct	

IP Region Route | IP Region Proximity

Subnet	Country	Description
58.116.0.0/14	CN	China Education and Research Network
58.128.0.0/13	CN	China Education and Research Network
58.154.0.0/15	CN	China Education and Research Network
58.192.0.0/12	CN	China Education and Research Network
59.64.0.0/12	CN	China Education and Research Network
110.64.0.0/15	CN	China Education and Research Network
111.114.0.0/15	CN	China Education and Research Network
111.116.0.0/15	CN	China Education and Research Network

IP Pool

Make certain you are in **Config mode** and have selected the “**IP Pool**” tab [\[a\]](#).

To set an IP pool, you can input the pool name, start IP and end IP of the IP segment to be added into the IP pool in the text fields [\[b\]](#), and click on the “Add” action link [\[c\]](#) to save your configuration..

The configuration will be displayed in the IP pool list table [\[d\]](#). You can also click on the “Delete” action link to delete a configuration item in the table or “Clear” to delete all the configurations [\[e\]](#).

The screenshot shows the Fortinet configuration interface for the IP Pool tab. The interface includes a top navigation bar with tabs for NAT, IPv6, IP Region, IP Pool, and Port Forwarding. The IP Pool tab is selected. Below the navigation bar, there is an 'ADD IP POOL' section with three input fields: Pool Name, Start IP, and End IP. To the right of these fields is an 'Add' button. Below the 'ADD IP POOL' section is an 'IP POOLS LIST' table. The table has columns for Pool Name, Start IP, and End IP. The first row of the table contains the data: Pool1, 10.8.6.47, and 10.8.6.49. To the right of the table is a 'Delete | Clear' button. Callouts a-e point to specific elements: 'a' points to the IP Pool tab, 'b' points to the input fields, 'c' points to the 'Add' button, 'd' points to the first row of the IP POOLS LIST table, and 'e' points to the 'Delete | Clear' button.

Pool Name	Start IP	End IP
Pool1	10.8.6.47	10.8.6.49

Port Forwarding

Port Forwarding allows the FortiBalancer appliance to transparently forward traffic destined for one IP and port to another port on the network. All related network servers should point to the appliance for their gateway routes to take full advantage of port forwarding.

Make certain you are in Config mode, and have selected Advanced Networking from the sidebar, and further selected the “Port Forwarding” tab [\[a\]](#).

TCP/UDP

Select the sub tab “TCP/UDP” [\[b\]](#). The configuration window displays two sort enabled tables of previously setup TCP and UDP port forwarding schemes.

To set up port forwarding, click on “Add TCP Entry” for TCP [\[c\]](#) or “Add UDP Entry” for UDP [\[d\]](#). The configuration window will present several text fields [\[e\]](#), where you can supply the local IP address and port, the remote IP and port as well as the timeout length in seconds (the configuration fields are the same for UDP and TCP; only TCP configuration is pictured here.). Choose the appropriate action link [\[f\]](#).

To delete schemes, simply select the configuration from the table and click on “Delete TCP Entry/Delete UDP Entry” [\[c\]/\[d\]](#) respectively. You can double click on a configuration in the table to go to the timeout value edit page.

Port Forwarding Configuration Interface

TCP PORT FORWARDING

	Local IP	Local Port	Remote IP	Remote Port	Timeout

UDP PORT FORWARDING

	Local IP	Local Port	Remote IP	Remote Port	Timeout

ADD UDP ENTRY

Local IP:

Local Port:

Remote IP:

Remote Port:

Timeout:

Cancel | Save & Add Another | Save

Port Forwarding (Continue)

Mode

You may set the FortiBalancer appliance for transparent (default) or You may set the FortiBalancer appliance for transparent (default) or non-transparent port forwarding.

Select the sub tab “**Mode**” [a]. The configuration window displays two radio buttons to set the transparent mode or non-transparent mode [b] for port forwarding. This will affect TCP/UDP Port Forwarding.

Select the desired mode and click the “**SAVE CHANGES**” button [c] to save the settings.

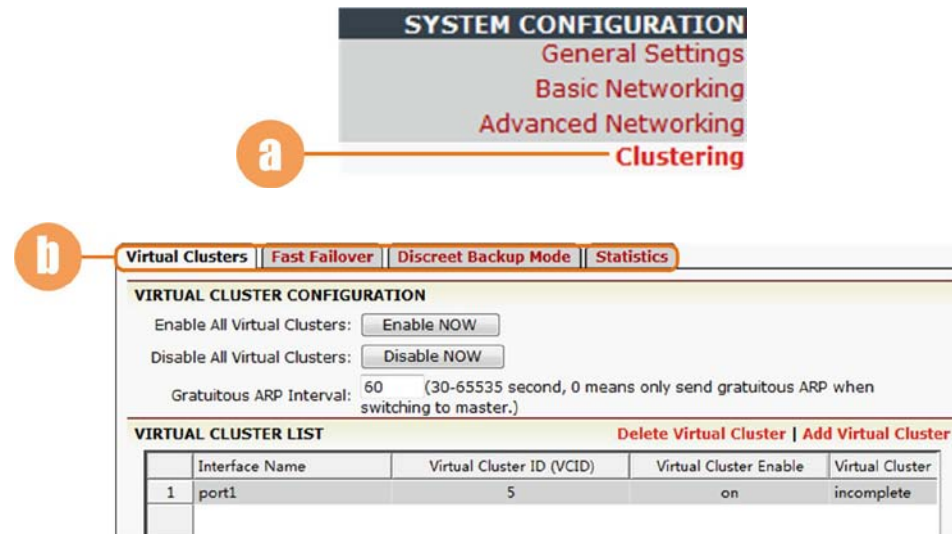


Clustering

The Fortinet Clustering Technology allows you to maintain high availability within local sites. Virtual Clustering provides high availability to SLB VIPs for the outside interface and for redundant gateways via the inside interface.

Make certain you are in **Config mode** and have selected “**Clustering**” from the sidebar [\[a\]](#).

You can see four tabs in the configuration window: Virtual Clusters, Fast Failover, Discreet Backup Mode, and Statistics [\[b\]](#). Note that to use the Fast Failover (FFO) function you have to first get the FFO license. Otherwise, the Fast Failover and Discreet Backup Mode tabs will not be displayed on the WebUI.



The screenshot shows the Fortinet WebUI System Configuration page. The sidebar on the left has a menu with the following items: General Settings, Basic Networking, Advanced Networking, and Clustering. The Clustering item is highlighted with an orange circle and labeled 'a'. The main content area shows the Virtual Clusters configuration window. The window has four tabs: Virtual Clusters, Fast Failover, Discreet Backup Mode, and Statistics. The Virtual Clusters tab is active and highlighted with an orange circle and labeled 'b'. The Virtual Clusters configuration window contains the following sections:

VIRTUAL CLUSTER CONFIGURATION

Enable All Virtual Clusters:

Disable All Virtual Clusters:

Gratuitous ARP Interval: 60 (30-65535 second, 0 means only send gratuitous ARP when switching to master.)

VIRTUAL CLUSTER LIST Delete Virtual Cluster | Add Virtual Cluster

	Interface Name	Virtual Cluster ID (VCID)	Virtual Cluster Enable	Virtual Cluster
1	port1	5	on	incomplete

Virtual Clusters

Click on the buttons [a] to enable or disable virtual clusters. Set the interval of sending gratuitous ARP packets in the text box [b].

Select “Add Virtual Cluster” [c] and a new page will appear. Give the virtual cluster an ID (1-255), and assign the cluster to an interface via the selector [d]. Then, select “Save” [e]. The information will be displayed in the table [f]. Double click on an entry in the table, the clustering configuration window for the entry will appear. You may also select from the created virtual clusters via the selector [g].

General Settings

Select “General Settings” sub tab [h]. Enable the individual cluster and/or preemption via the check boxes [i]. Set advertisement interval in the text field [j]. Use the radio buttons [k] to configure whether to use an authentication code or not. If “Yes” is selected, you need to further input the password [l]. Click on the button [m] to save changes.

Virtual Clusters (Continue)

Virtual IP (VIP)

Make certain you select the “**Virtual IP (VIP)**” tab [a]. Select the action link “Add VIP Entry” [b]. The configuration window will present a new screen.

Supply the VIP in dotted format in the text field [c]. Next, click on the desired action link [d]. The configured VIP will be displayed in the table [e].

Priority

Select the “**Priority**” sub tab [f]. To set priority, firstly you should add a node from “Config Management” (Please refer to the “Config Management” chapter for further information). Then, navigate back to the “Priority” sub tab and directly double click on the Priority column [g] to modify the value.

Once you’ve added a virtual cluster, it will be displayed in the table [h] under the “Virtual Clusters” tab [i]. You can use either of the two buttons [j] to universally enable or disable the clusters.

Select Virtual Cluster (Interface Name, VCID): port1, 5 [Back to top menu]

General Settings **Virtual IP (VIP)** **Priority**

VIRTUAL CLUSTER VIP CONFIGURATION Delete VIP Entry | Add VIP Entry

	Virtual IP (VIP)	Interface Name	Virtual Cluster ID (VCID)
1	10.10.10.10	port1	5

ADD VIP ENTRY Cancel | Save & Add Another | Save

Virtual IP (VIP):

Select Virtual Cluster (Interface Name, VCID): port1, 5 [Back to top menu]

General Settings **Virtual IP (VIP)** **Priority**

VIRTUAL CLUSTER PRIORITY SETTINGS [Priority Range = 1 - 255, 1=Lowest, 255=Highest]

Please click on the desired Priority column in the table below to change and assign different priority to the node/peer.

	Priority	Node/Peer Name	Node/Peer Type	Node Is Memt
1	100	Primary	*Local/Primary Node	

Virtual Clusters **Fast Failover** **Discreet Backup Mode** **Statistics**

VIRTUAL CLUSTER CONFIGURATION

Enable All Virtual Clusters: Enable NOW

Disable All Virtual Clusters: Disable NOW

Gratuitous ARP Interval: 60 (30-65535 second, 0 means only send gratuitous ARP when switching to master.)

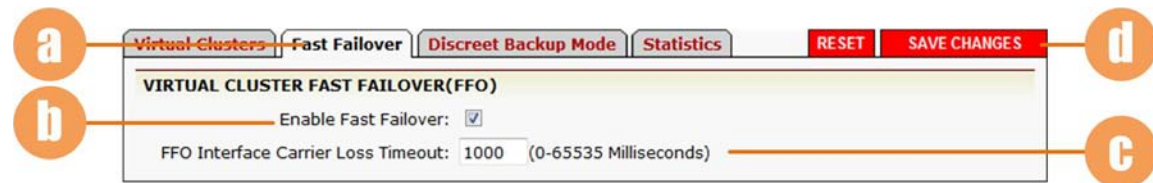
VIRTUAL CLUSTER LIST Delete Virtual Cluster | Add Virtual Cluster

	Interface Name	Virtual Cluster ID (VCID)	Virtual Cluster Enable	Virtual Cluster
1	port1	5	on	incomplete

Fast Failover

Select the “**Fast Failover**” tab [a].

You can enable fast failover by checking the box [b], and set FFO interface carrier loss timeout in the text field [c]. Then, click on the “**SAVE CHANGES**” button [d] to save the settings you made.



Discreet Backup Mode

Select the “**Discreet Backup Mode**” tab [e].

You can enable the cluster discreet backup mode by checking the box [f]. Note that to have the discreet backup mode work, you have to first enable FFO. You can do this by selecting the check box [b] under the “Fast Failover” tab.

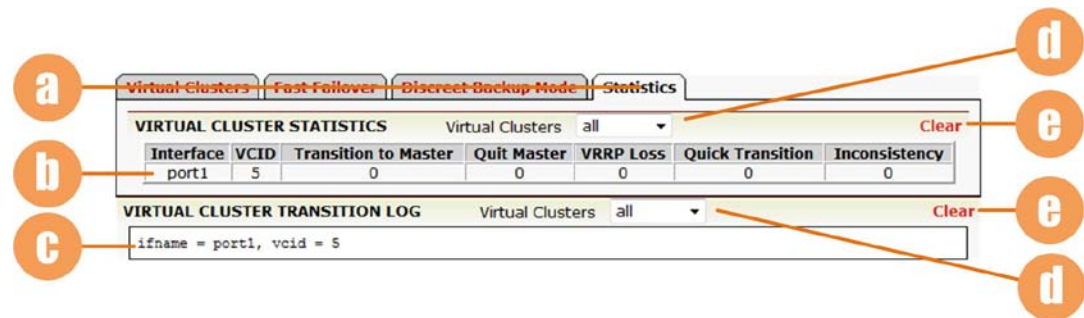
At last, remember to click on the “**SAVE CHANGES**” button [g] to save the changes.



Statistics

Select the “**Statistics**” tab [a]. The statistics information about all configured clusters [b] and transition logs of virtual clusters [c] are displayed here.

To clear cluster statistics or transition logs, users can select a desired cluster or all clusters (all) from the selector [d] and click on the “Clear” action link [e].



VIRTUAL CLUSTER STATISTICS Virtual Clusters: all [Clear](#)

Interface	VCID	Transition to Master	Quit Master	VRRP Loss	Quick Transition	Inconsistency
port1	5	0	0	0	0	0

VIRTUAL CLUSTER TRANSITION LOG Virtual Clusters: all [Clear](#)

ifname = port1, vcid = 5

WebWall

The Webwall function of the FortiBalancer appliance allows you to filter TCP, UDP and ICMP packets from the network by creating permit/deny rules. You can enable the Webwall function on desired interfaces, define various permit/deny access control rules and further bind these rules to desired interfaces within the network.

Make certain you are in Config mode and have selected the feature link “ **Webwall** ” from the sidebar [\[a\]](#).

Access Control

Select the “**Access Control**” tab [\[b\]](#). You can enable the Webwall function on desired interfaces via the check boxes [\[c\]](#). There are two modes: 0 and 1. Refer to section [\[d\]](#) for descriptions of the two modes. Confirm the interfaces and modes to enable and click on “**SAVE CHANGES**” [\[e\]](#) to make your settings take effect.

The screenshot shows the FortiBalancer configuration interface. At the top, a sidebar contains links: General Settings, Basic Networking, Advanced Networking, Clustering, and **Webwall** (highlighted with an orange line and label 'a'). The main panel has tabs for 'Access Control' (labeled 'b') and 'Attacking Packet Filter'. In the 'Access Control' tab, there are 'RESET' and 'SAVE CHANGES' buttons (labeled 'e'). Below the tabs is the 'WEBWALL STATUS' section, which contains a table with columns: Interface Name, Enable: Mode 0, and Enable: Mode 1. The table lists interfaces port1 through port7. Port3 and port4 have checkmarks in the 'Enable: Mode 0' column, indicated by an orange line and label 'c'. Below the table, there is a 'Mode:' section with two options: '0: Normal mode. All the packets will follow ACL rules;' and '1: Ack mode. In this mode, WebWall is backward compatible in that all the ACK TCP packets will be permitted by default.' (labeled 'd').

	Interface Name	Enable: Mode 0	Enable: Mode 1
1	port1	☐	☐
2	port2	☐	☐
3	port3	☒	☐
4	port4	☒	☐
5	port5	☐	☐
6	port6	☐	☐
7	port7	☐	☐

Mode:
0: Normal mode. All the packets will follow ACL rules;
1: Ack mode. In this mode, WebWall is backward compatible in that all the ACK TCP packets will be permitted by default.

Access control (Continue)

To define the access control rules, select the action link “Add” [a]. Some new parameters will appear [b]: supply the Access list ID, permission setting (permit or deny), protocol (ICMP, TCP or UDP), source IP with netmask, destination IP with netmask (if TCP or UDP protocol is selected, you need to further input the source port and destination port), and select an ICMP type via the selector. Then, click on the “Save” action link [c]. The access rule will be displayed in the sort-ready table of access list [d].

After creating an access control list, you can bind the rules in the list with desired interfaces.

First, select an interface via the selector [e], and input the ID (1-999) of the access control rule to bind with the interface in the text box [f]. Then, click on the action link “Add” [g]. The configuration will be displayed in the sort ready table [h].

The screenshot displays three sequential configuration screens in the Fortinet System Configuration interface, with callouts a through h indicating specific elements.

ACCESS LIST CONFIGURATION (Callout a points to the 'Add' link):

ID	Action	Protoc...	Source (IP/NetworkMask:Port)	Destination (IP/NetworkMask:Port)	Interface
1	5	PERMIT	ICMP	10.1.1.1/255.255.255.255	20.2.2.2/255.255.255.255

ADD ACCESS LIST ENTRY (Callout b points to the form fields):

Access List ID: (1 - 999)

Action:

Protocol:

Source IP:

Source Network Mask:

Destination IP:

Destination Network Mask:

ICMP Type:

ACCESS GROUP CONFIGURATION (Callout e points to the 'Interface' selector, callout f points to the 'Access List ID' text box, and callout g points to the 'Add' link):

Interface:

Access List ID: (1 - 999)

	Interface Name	ID
1	port3	5
2	bond1	5

Callout h points to the table in the Access Group Configuration screen.

Attacking Packet Filter

Select the “Attacking Packet Filter” tab [\[a\]](#).

You can set the level to filter invalid packages via the radio buttons [\[b\]](#). Three levels (0, 1 and 2) are available. Refer to section [\[c\]](#) for descriptions of the three levels. After setting the level properly, click on the “SAVE CHANGES” button [\[d\]](#) when it appears to save your configuration.

You can also view the filtering statistics of attacking packets in details in the table [\[e\]](#).

Access Control **Attacking Packet Filter** **RESET** **SAVE CHANGES**

ATTACKING PACKET FILTERING

Filter Level: 0 ☐ 1 ☒ 2 ☐

0: Disable the internal filter for IP packets.
That is to say, it will permit any packets to Ethernet card into our system.

1: System will drop the packets which match the following cases:

- (1) Source IP or destination IP is 0.0.0.0
- (2) Source IP is 255.255.255.255
- (3) Source IP is 224.x.x.x
- (4) TCP port or UDP port is zero. This requires the WebWall on the specific interface.

2: System will drop the packets which match the following cases:

- (1) Source IP or destination IP is 0.0.0.0
- (2) Source IP is 255.255.255.255
- (3) Source IP is 224.x.x.x
- (4) TCP port or UDP port is zero. This requires the WebWall on the specific interface.
- (5) Source IP is the local IP address, but the packets are received by Ethernet interfaces.

ATTACKING PACKET FILTER STATISTICS

Dropped packets				
Invalid IP address	Invalid TCP port	Invalid UDP port	Invalid IP route	RTS route over loopback
0	0	0	0	0

Monitoring

The FortiBalancer appliance allows you to monitor the interface running status and further shows you the realtime interface statistics.

Make certain you are in **Enable mode** and select the feature link “**Monitoring**” from the sidebar [\[a\]](#).



Interface Statistics

Select the “**Interface Statistics**” tab [\[b\]](#) and the window will display detailed information about the realtime interface and VLAN (if configured) statistics in the box [\[c\]](#). The page is automatically refreshed every twenty seconds.

Interface Statistics **NAT Translation Tables**

INTERFACE STATISTICS

Name	Status	Bytes In (MBytes)	Bytes Out (MBytes)	Pkts In	Pkts Out	Errs In	Errs Out	Colls	FW Not Permit	FW Deny
port1	active	4	10	21323	35776	0	0	0	N/A	N/A
port2	no carrier	0	0	0	0	0	0	0	N/A	N/A
port3	no carrier	0	0	0	0	0	0	0	N/A	N/A
port4	no carrier	0	0	0	0	0	0	0	N/A	N/A

Name	Throughput In (MBytes/Sec)	Throughput In (Pkts/Sec)	Throughput Out (MBytes/Sec)	Throughput Out (Pkts/Sec)
port1	0	0	0	0
port2	0	0	0	0
port3	0	0	0	0
port4	0	0	0	0

Note:

- 1) This page will be automatically refreshed every 20 seconds.
- 2) FW Not Permit/Deny value is N/A means currently FireWall is disabled.
- 3) Throughput In/Out shows the average throughput of every 5 minutes

NAT Translation Tables

Select the “**NAT Translation Tables**” tab [\[a\]](#) and the window will display detailed information about the normal NAT translation [\[b\]](#), PPTP GRE NAT table overview [\[c\]](#) and the PPTP GRE NAT table [\[d\]](#). The page is automatically refreshed every five seconds.

Interface Statistics NAT Translation Tables

NORMAL NAT TABLE

	From IP	From Port	Through IP	Through Port	To IP	To Port

PPTP GRE NAT TABLE OVERVIEW

	Current GRE tunnel	Total Out Packets	Total In Packets	Total Out Bytes	Total In Bytes
1	0	0	0	0	0

PPTP GRE NAT TABLE

	From IP	From Call ID	Through IP	Through Call ID	To IP	To Call ID

Note:
This page will be automatically refreshed every 5 seconds.

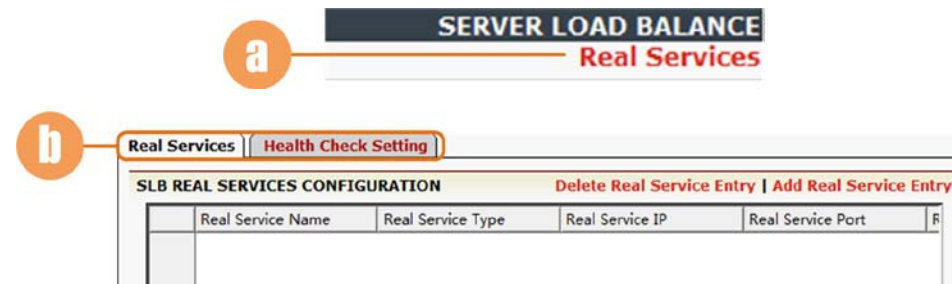
Server Load Balance

Server Load Balancing (SLB) allows you to distribute load and traffic to specific groups of servers or to a specific server. The FortiBalancer appliance supports server load balancing through layer 2 to 7 of the OSI network model. The L4 SLB is mostly concerned with port based load balancing, and the L7 SLB is used when you want to perform load balancing based on URLs, HTTP headers or cookies.

Real Services

The first step in setting up your network architecture with the FortiBalancer appliance to perform SLB tasks is to create and configure your real services.

Make certain you are in Config mode and have selected the feature link “**Real Services**” from the sidebar [\[a\]](#). The configuration window will display two tabs [\[b\]](#). The default page is “**Real Services**”.



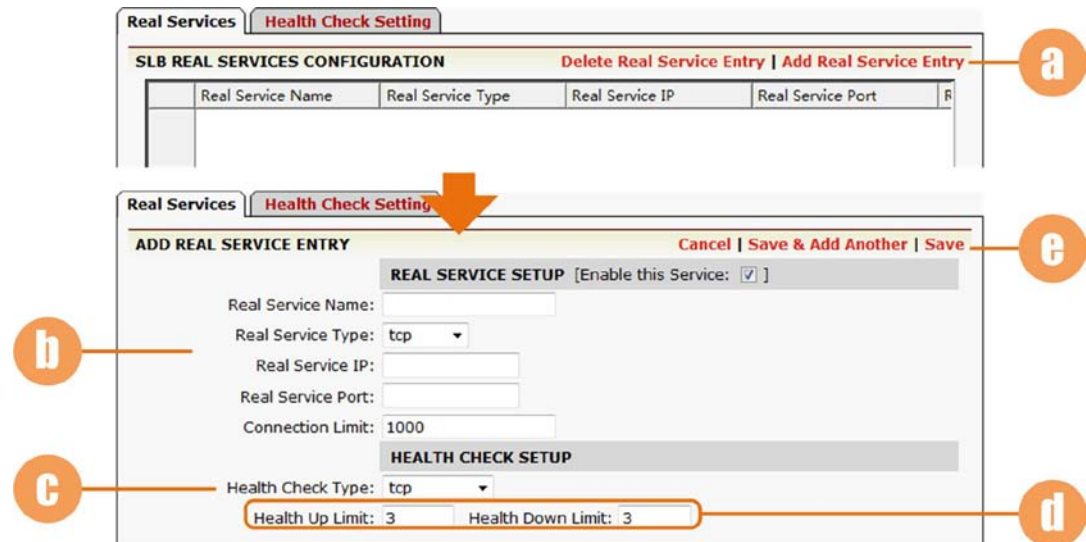
Real Services

Select the action link “Add Real Service Entry” [a]. The configuration window will present a new screen.

The new screen is for you to configure real servers. Depending on which type of real service is specified, certain parameter fields will appear, change or disappear [b].

Then set the health check type for the real service via the selector (FTPS and RDP types are supported in 8.2) [c], and configure the related parameters of health check [d]. The parameter fields may vary with different health check types. Note: For the TCP real services, LDAP health check can be set up. For the UDP and SIP-UDP real services, the Radius health check can be configured.

Finish the configuration of the real service and its health check by clicking on the desired action link [e].



The screenshot displays the Fortinet SLB Real Services Configuration interface. At the top, there are tabs for 'Real Services' and 'Health Check Setting'. Below the tabs is a table titled 'SLB REAL SERVICES CONFIGURATION' with columns: Real Service Name, Real Service Type, Real Service IP, Real Service Port, and an action column. An arrow points from the 'Add Real Service Entry' link in the action column to the 'ADD REAL SERVICE ENTRY' form below. The form is divided into two sections: 'REAL SERVICE SETUP' and 'HEALTH CHECK SETUP'. The 'REAL SERVICE SETUP' section includes fields for Real Service Name, Real Service Type (set to tcp), Real Service IP, Real Service Port, and Connection Limit (set to 1000). The 'HEALTH CHECK SETUP' section includes a Health Check Type selector (set to tcp) and two input fields: Health Up Limit (set to 3) and Health Down Limit (set to 3). Action links 'Cancel', 'Save & Add Another', and 'Save' are at the top right of the form.

Real Services (Continue)

Once you've added a real service, it will be displayed in the sort ready table [a]. The status of the service is also displayed:

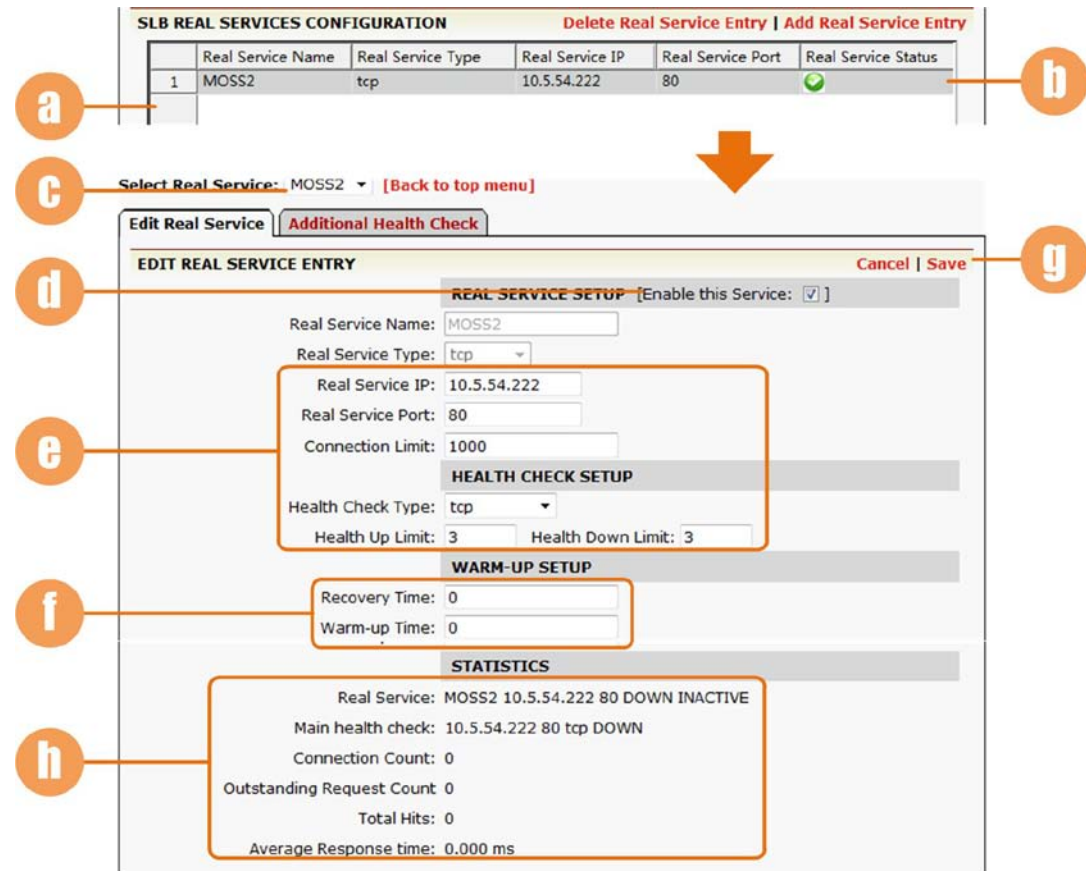
-  Enabled and Up (healthy);
-  Enabled but Down (unhealthy);
-  Disabled.

Select a created real service from the table [b] and double click on it. The configuration window will present a new window to complete more real services configurations.

Edit Real Service

Select a desired real service from the selector [c]. Use the check box to enable the real service [d]. You may change the real service settings and health check settings [e], and finish the system warm-up configuration [f]. Then, remember to click on the "Save" action link [g] to save your settings.

This page also displays the current running statistics concerning the selected real service [h].



The screenshot shows the 'SLB REAL SERVICES CONFIGURATION' page. At the top, there's a table with columns: Real Service Name, Real Service Type, Real Service IP, Real Service Port, and Real Service Status. A single entry 'MOSS2' is shown with a green checkmark status. An arrow points from this entry to the 'EDIT REAL SERVICE ENTRY' window below. The 'EDIT REAL SERVICE ENTRY' window has tabs for 'Edit Real Service' and 'Additional Health Check'. It contains sections for 'REAL SERVICE SETUP' (with fields for Name, Type, IP, Port, and Connection Limit), 'HEALTH CHECK SETUP' (with fields for Type, Up Limit, and Down Limit), 'WARM-UP SETUP' (with fields for Recovery Time and Warm-up Time), and 'STATISTICS' (showing various counts and response times). Annotations a through h point to specific elements: a points to the table, b points to the status icon, c points to the service selector, d points to the 'Enable this Service' checkbox, e points to the service setup fields, f points to the warm-up fields, g points to the 'Save' button, and h points to the statistics section.

Real Services (Continue)

Additional Health Check

Click on the “**Additional Health Check**” tab [\[a\]](#). This page allows you to set additional health check for the specified real service.

Set the relation between additional health checks via the radio buttons [\[b\]](#). Set the health check name and select health check type [\[c\]](#). Enter health check IP address and port [\[d\]](#). Depending on which additional health check type is specified, certain parameter fields will appear, change and disappear [\[e\]](#). The Radius health check and LDAP health check are both supported with different parameter fields.

After completing the operation, click the action link “Add” [\[f\]](#). The added additional health check will be displayed in the table below [\[g\]](#).



Select Real Service: MOSS2 [Back to top menu]

Additional Health Check

ADDITIONAL HEALTH CHECK RELATION

Additional Health Check Relation: or ☐ and ☒

ADD ADDITIONAL HEALTH CHECK Cancel | Add

Real Service Name: MOSS2 Real Service Type: tcp

Health Check IP: Health Check Port:

Type: tcp

Health Up Limit: 3 Health Down Limit: 3

ADDITIONAL HEALTH CHECK LIST Delete

Real Service Name	Health Check IP	Health Check Port	Health Check Type	Real Service Status

Health Check Setting

Make certain you select the “**Health Check Setting**” tab [a]. Use the check box to enable the health check [b]. Set the health check interval and server timeout in seconds [c]. Use the check box to enable failover function [d]. Configure the times of retries before failover [e].

Set the request index and string in the text fields [f]. You may overwrite the existing request string of any index from 0 to 999. The new request string will be listed in the Existing Requests list [g].

Set the response index and string in the text fields [h]. You may also overwrite the response string of any index from 0 to 999. The new response string will also be listed in the Existing Responses list [i].

Set the health early warning threshold in the text field [j], which ranges from 0 to 60000 milliseconds.

Remember to click on the “**SAVE CHANGES**” button after completing the settings [k].

You can click on the “**Delete**” buttons respectively to delete specified existing request or response, or click on the “**Clear**” button to clear all existing requests or responses [l]. You can also click on the “**Clear**” button to clear the health early warning setting [m].

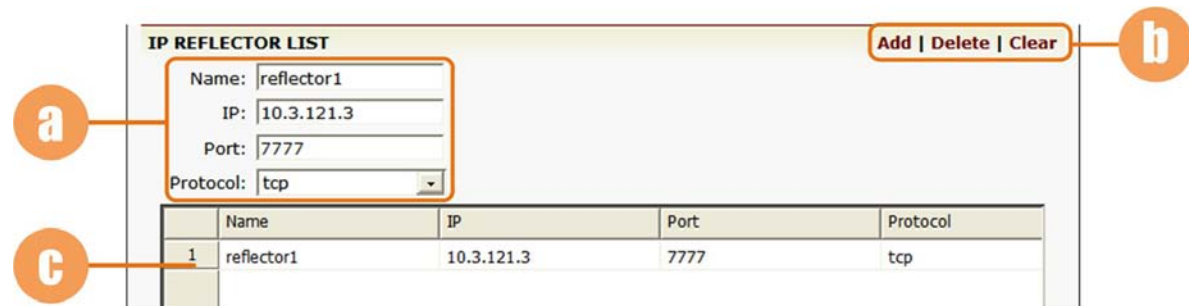
The screenshot shows the 'Health Check Setting' tab in the Fortinet configuration interface. The page has a 'Real Services' tab and a 'Health Check Setting' tab. The 'Health Check Setting' tab is active. The page includes a 'RESET' button and a 'SAVE CHANGES' button. The 'HEALTH CHECK SETTING' section contains the following fields and buttons:

- Enable Health Check:** A checkbox that is checked. (Callout a points to the tab, b points to this checkbox)
- Health Check Interval(seconds):** A text field with the value '5'. (Callout c points to this field)
- Server Timeout(seconds):** A text field with the value '5'. (Callout c points to this field)
- Enable Failover:** A checkbox that is unchecked. (Callout d points to this checkbox)
- Retries Before Failover:** A text field with the value '3'. (Callout e points to this field)
- Request Index:** A text field with the value '0'. (Callout f points to this field)
- Request String:** A text field with the value 'HEAD / HTTP/1.0\r\n\r\n'. (Callout f points to this field)
- Existing Requests:** A dropdown menu showing '0 HEAD / HTTP/1.0\r\n\r\n'. (Callout g points to this dropdown)
- Response Index:** A text field with the value '0'. (Callout h points to this field)
- Response String:** A text field with the value '200 OK'. (Callout h points to this field)
- Existing Responses:** A dropdown menu showing '0 200 OK'. (Callout i points to this dropdown)
- Health Earlywarning:** A text field with the value '0'. (Callout j points to this field)
- Buttons:** There are 'Delete' and 'Clear' buttons next to the 'Existing Requests' and 'Existing Responses' dropdowns. (Callout l points to the 'Delete' button for 'Existing Requests', m points to the 'Clear' button for 'Health Earlywarning') There is also a 'Clear' button next to the 'Health Earlywarning' field.

Health Check Setting (Continue)

To configure a reflector for L2 SLB TCP health check, input the name, IP address, port of the reflector in the text fields and set the protocol via the drop-down list [\[a\]](#). Then click on the action link “Add” [\[b\]](#) and the new reflector will be listed in the sort ready table [\[c\]](#).

You can select a specific reflector and delete it or clear all the reflectors by clicking on the desired action link [\[b\]](#).



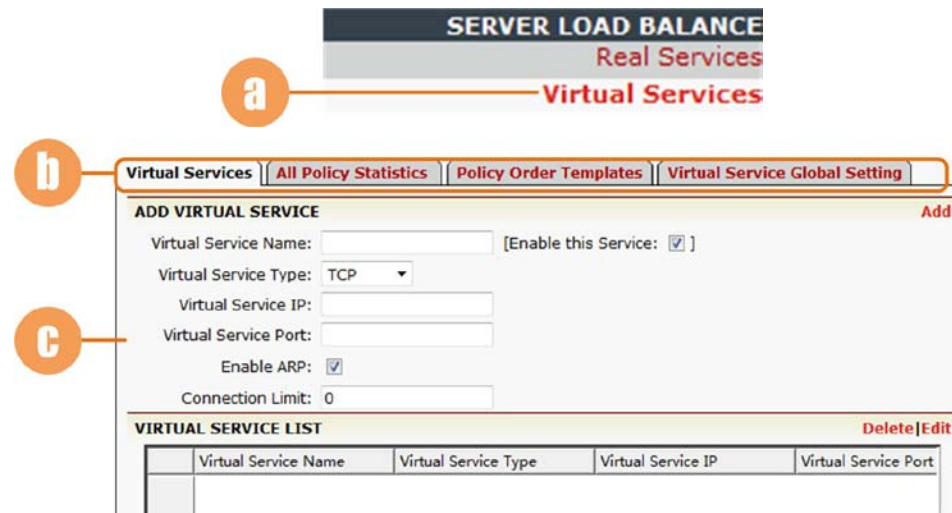
The screenshot shows the 'IP REFLECTOR LIST' configuration page. It includes a form for adding a new reflector and a table of existing reflectors. Callout 'a' points to the form fields, 'b' points to the 'Add | Delete | Clear' buttons, and 'c' points to the table.

IP REFLECTOR LIST				
Add Delete Clear				
Name: reflector1 IP: 10.3.121.3 Port: 7777 Protocol: tcp				
	Name	IP	Port	Protocol
1	reflector1	10.3.121.3	7777	tcp

Virtual Services

A Virtual IP is an IP address that you define and that will service requests for the content which a group is designed for. For example, if group1 is a set of image servers, we could define a VIP of 10.10.0.10 that is tied to group1. Any requests made to this Virtual IP will be passed to either the Cache or SLB subsystem depending on your cache and SLB settings. In essence you are hiding your internal architecture by only exposing one IP and not many.

Make certain you are in the Config mode and have selected the feature link “Virtual Services” from the sidebar [a]. The configuration window will display four tabs [b]. The “**Virtual Services**” page is displayed by default [c].



SERVER LOAD BALANCE

Real Services

Virtual Services

a

b

Virtual Services | All Policy Statistics | Policy Order Templates | Virtual Service Global Setting

c

ADD VIRTUAL SERVICE Add

Virtual Service Name: [Enable this Service: ☒]

Virtual Service Type: TCP

Virtual Service IP:

Virtual Service Port:

Enable ARP: ☒

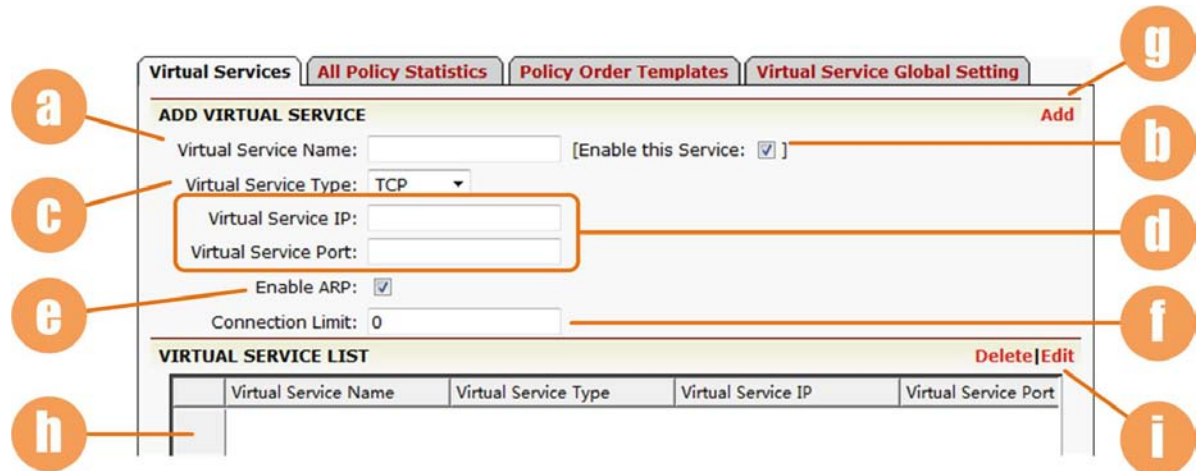
Connection Limit: 0

VIRTUAL SERVICE LIST Delete | Edit

Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port

Virtual Services

Set the virtual service's name [a]. Use the check box to enable the virtual service [b]. Select the virtual service type from the selector (RDP type is supported in 8.2) [c]. Set the virtual service IP and port [d]. Use the check box to enable ARP [e]. Set the maximum number of open connections per virtual service [f]. Depending on which type of virtual service is specified, certain parameter fields will appear, change or disappear. Click on the desired action link [g] to add a virtual service. Once a virtual service is added, it will be displayed within the table [h]. Select a virtual service in the table and double click on it or click on the action link "Edit" [i]. A new configuration window will present a new series of tabs for completing virtual services configuration.



The screenshot shows the 'Virtual Services' configuration page. The top navigation bar includes 'Virtual Services', 'All Policy Statistics', 'Policy Order Templates', and 'Virtual Service Global Setting'. The main section is titled 'ADD VIRTUAL SERVICE' and contains the following fields:

- a**: Virtual Service Name input field.
- b**: [Enable this Service: ☒]
- c**: Virtual Service Type dropdown menu (set to TCP).
- d**: Virtual Service IP and Virtual Service Port input fields.
- e**: Enable ARP checkbox (checked).
- f**: Connection Limit input field (set to 0).
- g**: Add button.

Below the form is a table titled 'VIRTUAL SERVICE LIST' with columns: Virtual Service Name, Virtual Service Type, Virtual Service IP, and Virtual Service Port. The table is currently empty. The bottom right of the table has 'Delete' and 'Edit' links. The table area is labeled **h**. The 'Edit' link is labeled **i**.

Virtual Services (Continue)

Vlink Setting

Select a vlink in “Vlink List” [a], double click it or click the “Edit” actional link [b], and a new window will display.

In the “Vlink Setting” window, you can set the regex case mode for the vlink via the radio button [c]. Then, click on the “Save Changes” button [d].



Virtual Services (Continue)

Virtual Services Settings

You may select from created virtual services via the selector [a], and modify configurations about the virtual service in the area [b]. Then, click on “Save” [c].

More parameter fields [d] are available for completing settings of the selected virtual service. Depending on the different types of the created virtual services [e], certain parameter fields will appear, change or disappear. For the virtual services of TCP, UDP or IP type, the Triangle Proxy mode is available for configuration; for the HTTP type, redirecting all HTTP requests to HTTPS requests is supported; for the UDP type, the packet based forwarding mode can be enabled via the check box [f].

Then, click on the “Save Changes” button [g] to save your settings.

The screenshot shows the 'Virtual Service Settings' page in the Fortinet web interface. The interface is divided into several sections:

- Top Bar:** Includes a 'Select Virtual Service' dropdown menu (labeled 'a') set to 'V1', a '[Back to top menu]' link, and 'RESET' and 'SAVE CHANGES' buttons (labeled 'g').
- Navigation Tabs:** 'Virtual Service Settings' (active), 'Virtual Service Statistics', 'URL Rewrite', 'URL Filter', and 'HTTP Forwarding'.
- VIRTUAL SERVICE INFORMATION:**
 - Virtual Service Name: V1
 - Virtual Service IP: 10.3.70.65
 - Virtual Service Port: 80
 - Enable ARP: ☒
 - Connection Limit: 0
 - Virtual Service Type: HTTP (dropdown menu, labeled 'e')
- Note:** A warning box states: '* Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.'.
- VIRTUAL SERVICE SETTING:**
 - TCP Timeout: [text field]
 - Redirect All HTTP Requests to HTTPS: ☐
 - Enable OWA Support: ☐
 - Additional HTTP Request Headers: [text field]
 - HTTP Client IP Headers: [text field]
 - Remove Port From Location Header: ☐
 - Rewrite Redirections From Backend to Use HTTPS: ☐
 - Enable data compression for this service: ☒
 - Enable X-Forwarded-For for this service: ☒
 - Regex case mode: insensitive ☐ sensitive ☐ use global mode ☒
 - Mode: Use System Mode ☒ Operate as Transparent Proxy ☐ Operate as Reverse Proxy ☐
 - Enable this Service: ☒
 - Enable Cache: ☒
 - Enable Packet Based Forwarding Mode: ☐ (labeled 'f')

Annotations 'a' through 'g' are placed around the interface to highlight specific elements mentioned in the text:

- a:** Select Virtual Service dropdown menu.
- b:** The main configuration area for the virtual service.
- c:** The 'Save' button (part of the 'Cancel | Save' link).
- d:** The 'VIRTUAL SERVICE SETTING' section.
- e:** The Virtual Service Type dropdown menu.
- f:** The 'Enable Packet Based Forwarding Mode' checkbox.
- g:** The 'SAVE CHANGES' button.

Virtual Services (Continue)

Virtual Services Settings (Continue)

And also on this configuration page, if the virtual service's port is set to be 0, the "Port Range List" will be displayed here [a]. Administrators need to configure "Begin port" and "End port" [b] and then click on the action link "Add" [c], and then the port range will be added to the table [d]. For a virtual service, you can configure three port ranges at most.

Also on this configuration page, you may assign the virtual service to the established groups as set up earlier in the configuration process. Use the scroll down menu to select the desired group and the necessary policy [e]. Depending on different virtual service types, certain parameter fields will change, appear or disappear [f]. Click on the desired action link "Add" [g]. The group and the policy will be displayed in the sort ready table [h].

Use the scroll down menu to assign the configured real services [i] to the virtual service. Then choose a policy order template by the selector [j] for the virtual service.

The screenshot shows the 'VIRTUAL SERVICE INFORMATION' configuration page. Callouts a-j point to specific fields and sections:

- a**: Virtual Service Name: asdf
- b**: Virtual Service IP: 172.16.85.41
- c**: Virtual Service Port: 0
- d**: Enable ARP: ☒
- e**: Connection Limit: 0
- f**: * Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.
- g**: PORT RANGE LIST (Add/Delete)
- h**: ASSOCIATE GROUPS (Add/Delete)
- i**: ASSOCIATE REAL SERVICE (STATIC POLICY) (Set)
- j**: ASSOCIATE POLICY ORDER TEMPLATE (Set)

Key fields and sections visible in the form:

- VIRTUAL SERVICE INFORMATION**: Virtual Service Name (asdf), Virtual Service Type (HTTP), Virtual Service IP (172.16.85.41), Virtual Service Port (0), Enable ARP (checked), Connection Limit (0).
- PORT RANGE LIST**: Begin port, End port, Protocol, Destination or port.
- ASSOCIATE GROUPS**: Virtual Service Or Vlink (asdf), Eligible Groups (g1), Eligible Policies (qos clientport), Policy Name, Network IP, Netmask, Low Port, High Port, Policy Precedence.
- ASSOCIATE REAL SERVICE (STATIC POLICY)**: Static Real: [dropdown], Attribute, Value.
- ASSOCIATE POLICY ORDER TEMPLATE**: Policy Order Template: [dropdown].

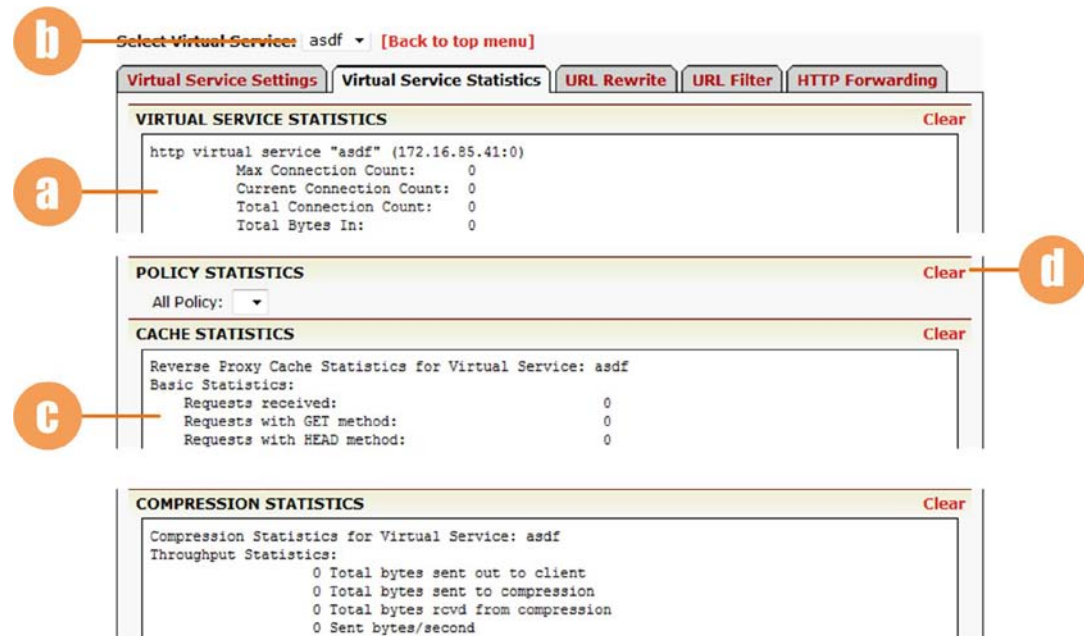
Virtual Services (Continue)

Virtual Services Statistics

Select the “Virtual Service Statistics” sub tab [\[a\]](#).

To view statistics of a desired virtual service, select the service from the drop-down list [\[b\]](#) and the window will display related running statistics for the virtual service, including virtual service statistics, policy statistics, cache statistics and compression statistics [\[c\]](#).

You can clear desired statistics information by clicking on the action link “Clear” [\[d\]](#).



b Select Virtual Service: asdf [Back to top menu]

a Virtual Service Statistics

c Virtual Service Statistics

d Clear

Clear

http virtual service "asdf" (172.16.85.41:0)

Max Connection Count:	0
Current Connection Count:	0
Total Connection Count:	0
Total Bytes In:	0

POLICY STATISTICS **Clear**

All Policy: [v]

CACHE STATISTICS **Clear**

Reverse Proxy Cache Statistics for Virtual Service: asdf

Basic Statistics:

Requests received:	0
Requests with GET method:	0
Requests with HEAD method:	0

COMPRESSION STATISTICS **Clear**

Compression Statistics for Virtual Service: asdf

Throughput Statistics:

0 Total bytes sent out to client
0 Total bytes sent to compression
0 Total bytes rcvd from compression
0 Sent bytes/second

Virtual Services (Continue)

URL Rewrite

Select the “URL Rewrite” sub tab [a], and a configuration screen will appear. The contents in this configuration page are available only if you have selected the HTTP or HTTPS type of virtual service.

HTTP Redirect: Assign a name to the HTTP redirect policy [b]. Set the priority of the rule [c], the larger the higher. Set the HTTP status code to send back response by selecting from the selector [d]. Set an exact string of host header and regular expression to match the path of the request [e]. Select a new protocol of redirected response, either HTTP or HTTPS [f]. Then assign a new name to the redirected response and Set a new string to replace the part matching Path Regex [g]. Click on the desired action link “Add” [h]. The configurations will be displayed in the table below [i].

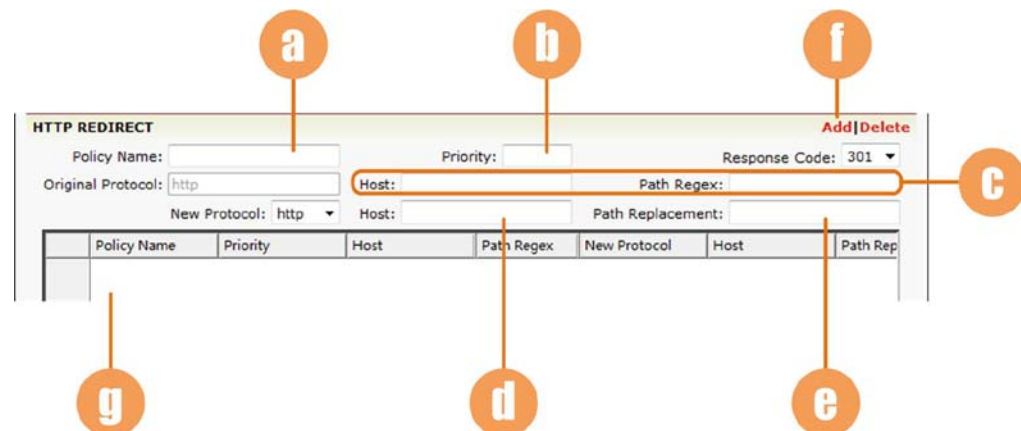
Policy Name	Priority	Host	Path Regex	New Protocol	Host	Path Rep
-------------	----------	------	------------	--------------	------	----------

Virtual Services (Continue)

URL Rewrite (Continue)

HTTP Rewrite Request URL: Assign a name to the HTTP rewrite policy [\[a\]](#). Set the priority of the rule [\[b\]](#), the larger the higher. Set the exact string of host header and regular expression [\[c\]](#) to match the path of the request. Then assign a new name to the rewritten request [\[d\]](#). Set a new string to replace the part matching Path Regex [\[e\]](#).

Click on the desired action link “Add” [\[f\]](#). The configurations will be displayed in the table below [\[g\]](#).



HTTP REDIRECT Add | Delete

Policy Name: Priority: Response Code: 301 ▼

Original Protocol: Host: Path Regex:

New Protocol: Host: Path Replacement:

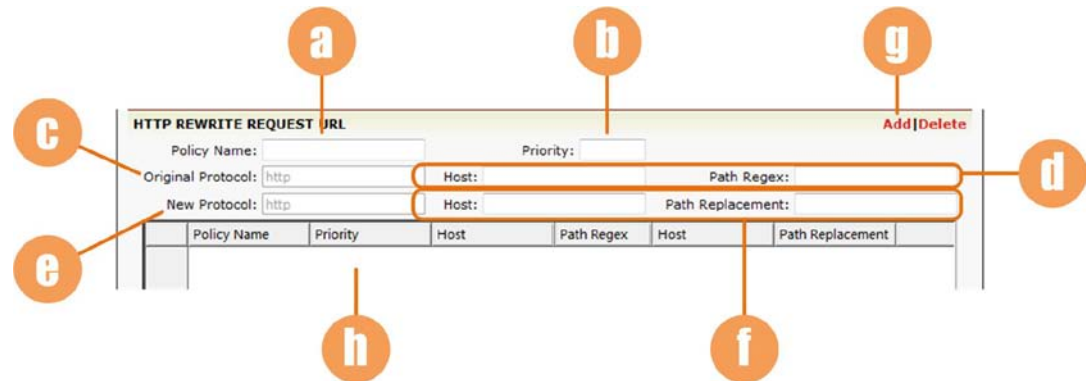
Policy Name	Priority	Host	Path Regex	New Protocol	Host	Path Rep

Virtual Services (Continue)

URL Rewrite (Continue)

HTTP Rewrite Response URL: Assign a name to the HTTP rewrite policy [\[a\]](#). Set the priority of the rule [\[b\]](#), the larger the higher. Use the scroll down menu to select an original protocol, HTTP, HTTPS or both [\[c\]](#). Set the exact host string in the response “Location:” header and regular expression to match the path in the response “Location:” header [\[d\]](#). Use the scroll down menu to select a new protocol [\[e\]](#). Then assign a new host name to the rewritten request and configure a string to replace the part matching Path Regex [\[f\]](#).

Click on the desired action link “Add” [\[g\]](#). The configurations will be displayed in the table below [\[h\]](#).



The screenshot shows the 'HTTP REWRITE REQUEST URL' configuration page. Callouts are as follows:

- a**: Policy Name field
- b**: Priority field
- c**: Original Protocol dropdown menu
- d**: Host and Path Regex fields
- e**: New Protocol dropdown menu
- f**: Host and Path Replacement fields
- g**: Add/Delete action link
- h**: The table below the configuration fields

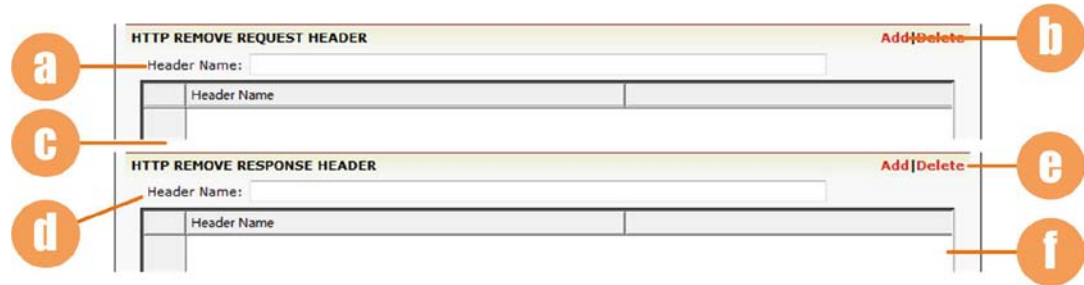
Policy Name	Priority	Host	Path Regex	Host	Path Replacement

Virtual Services (Continue)

URL Rewrite (Continue)

HTTP Remove Request Header: Input the name of the HTTP header to be removed from all client requests for this virtual service in the text box [a] and click on the action link [b]. Then, the header name will be displayed in the table [c]. To delete a header name from the table, select it in the table and click on the action link “Delete” [b].

HTTP Remove Response Header: Input the name of the HTTP header to be removed from all server responses for this virtual service in the text box [d] and click on the action link [e]. Then, the header name will be displayed in the table [f]. To delete a header name from the table, select it in the table and click on the action link “Delete” [e].



The screenshot displays two sections for removing HTTP headers. The top section, 'HTTP REMOVE REQUEST HEADER', features a text box labeled 'Header Name:' (callout a) and 'Add|Delete' links (callout b). Below is a table (callout c) with a single row containing the text 'Header Name'. The bottom section, 'HTTP REMOVE RESPONSE HEADER', similarly has a 'Header Name:' text box (callout d) and 'Add|Delete' links (callout e), followed by a table (callout f) with a row containing 'Header Name'.

Virtual Services (Continue)

URL Filter

Make certain you are in Config mode and Select the “**URL Filter**” sub tab [\[a\]](#), and a configuration screen will appear. URL filtering includes VIP URL filtering and global URL filtering. (Here, only VIP URL filtering configuration is described. Please refer to the “Caching Proxy” chapter for global URL filtering configuration.) The contents in this configuration page are available only if you have selected the HTTP or HTTPS type of virtual service.

URL Filtering: Enable the VIP URL filtering feature [\[b\]](#), and save the change by clicking on “**SAVE CHANGES**” button [\[c\]](#). After saving, more configurations appear.

Alert E-mails: Set the behavior mode for filtering as active or passive [\[d\]](#). Configure the destination email address for filter related alerts and the threshold for the number of dropped requests before issuing the alert [\[e\]](#).



Virtual Services (Continue)

URL Filter (Continue)

Length Based Filtering: Configure the filter length parameters for requests coming into the network [a]. You may reset by clicking on the action link [b].

Keyword Filtering: Assign the default filtering policy as permit or deny [c] and supply the Match Keyword text field [b]. Then, click the action link “Add” [e]. The restrictions will be displayed in the sort ready table [f]. Note that if you want to change the default global filtering policy, you must firstly delete all configured restriction entries displayed in the table [f].

Type Filtering: Set the variable type (integer or string) [g], and supply the variable name [h]. Click the desired action link “Add” [i]. Then, the restrictions will be displayed in the sort ready table [j]. To remove an existing restriction, select the desired entry in table [j] and click on the action link “Delete” [i].

Character Based Filtering: Configure the filter character parameters for requests coming into the network. To deny specific requests based on URL character ranges (ASCII values); enter the starting and ending values of the character range [k]. Click on the action link “Add” [l].

Keyword Filtering Statistics: Display the statistics of default policy, deny policy and permit policy of URL keyword filtering [m].

The screenshot displays the configuration interface for Virtual Services, specifically the URL Filter section. It is divided into several panels:

- LENGTH BASED FILTERING:** Contains input fields for Header (1024), Request (10000), URL (1024), Query (1024), Query Data (512), and Query Variable (128). It has 'RESET' and 'SAVE CHANGES' buttons at the top right.
- KEYWORD FILTERING:** Includes a 'Default Policy' section with radio buttons for 'permit' (selected) and 'deny'. Below it is a 'Match Keyword' text field and a 'Test' button. At the bottom is a table with columns 'Keyword' and 'Policy'. Action links 'Add' and 'Delete' are on the right.
- TYPE FILTERING:** Features a 'Variable Name' text field and a 'Variable Type' dropdown menu set to 'string'. It also has 'Add' and 'Delete' action links.
- CHARACTER BASED FILTERING:** Includes 'Character Range From' and 'Character Range To' text fields. Below is a table with columns 'Character Range ...' and 'Character Range ...'. It has 'Add' and 'Delete' action links.
- KEYWORD FILTERING STATISTICS:** Displays statistics for 'virtual service asdf - default permit - 0 requests matched default'. It has a 'Clear' button.

Annotations (a-m) point to the following elements:

- a: LENGTH BASED FILTERING section header
- b: Match Keyword text field
- c: Default Policy: permit/deny radio buttons
- d: Add/Delete links in Keyword Filtering table
- e: Add link in Keyword Filtering section
- f: Keyword Filtering table
- g: Variable Type dropdown
- h: Variable Name text field
- i: Add/Delete links in Type Filtering section
- j: Table in Type Filtering section
- k: Character Range From/To text fields
- l: Add/Delete links in Character Based Filtering section
- m: Keyword Filtering Statistics section

Virtual Services (Continue)

HTTP Forwarding

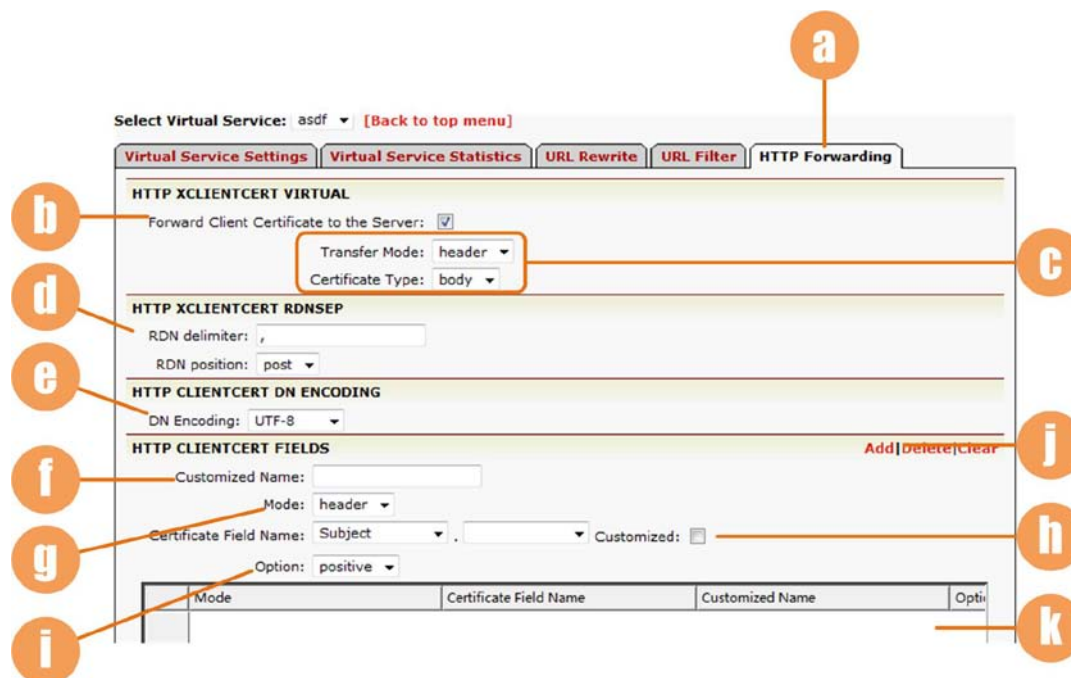
Select the “**HTTP Forwarding**” sub tab [a]. The contents in this configuration page are available only if you have selected the HTTP or HTTPS virtual service. Note: The configuration pages of the HTTP and HTTPS are different. Here, we take the HTTPS page as an example.

HTTP XClientCert Virtual: Turn on forwarding client certificate to the server by selecting the check box [b], and specify the transfer mode and certificate type [c].

HTTP XClientCert RDNSEP: You can customize RDN field separator (defaults to “,”) and specify the position (“pre” or “post”) to put the separator [d].

HTTP ClientCert DN Encoding: You can specify the DN encoding format via the selector [e]. It defaults to UTF-8.

HTTP ClientCert Fields: Input a customized name for the HTTP certificate field [f]. Specify the transfer mode [g], the certificate field name [h] which can be customized, and the DN sequence via the selector [i]. Then, click on the action link “Add” [j], then all the configurations will be presented in the table [k].



Select Virtual Service: asdf [Back to top menu]

Virtual Service Settings Virtual Service Statistics URL Rewrite URL Filter HTTP Forwarding

HTTP XCLIENTCERT VIRTUAL

Forward Client Certificate to the Server: ☒

Transfer Mode: header

Certificate Type: body

HTTP XCLIENTCERT RDNSEP

RDN delimiter: ,

RDN position: post

HTTP CLIENTCERT DN ENCODING

DN Encoding: UTF-8

HTTP CLIENTCERT FIELDS Add Delete Clear

Customized Name:

Mode: header

Certificate Field Name: Subject Customized: ☐

Option: positive

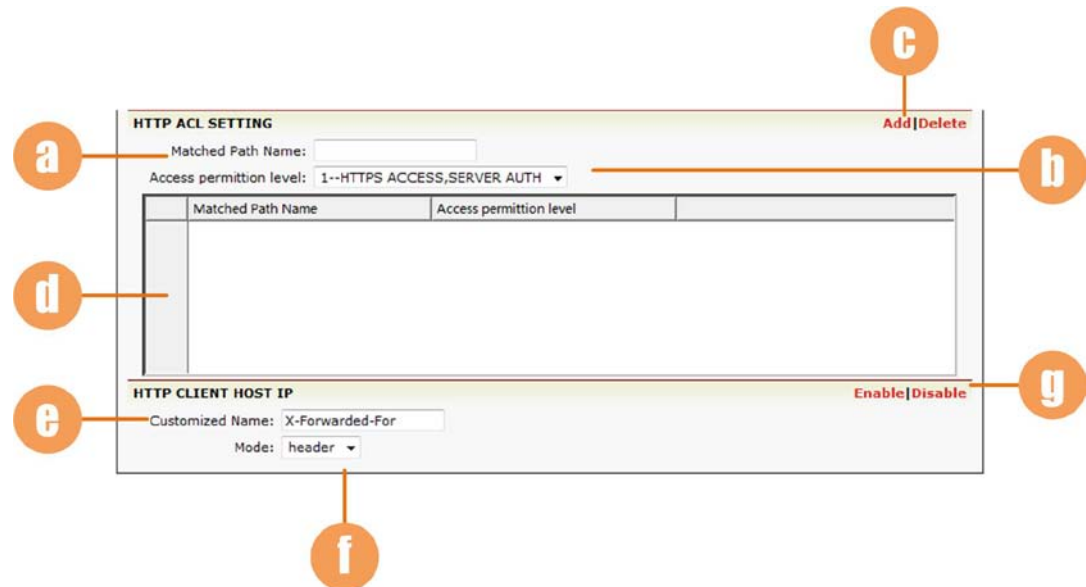
Mode	Certificate Field Name	Customized Name	Option
------	------------------------	-----------------	--------

Virtual Services (Continue)

HTTP Forwarding (Continue)

HTTP ACL Setting: Set the matched URL [a] by which the network resource defined needs to be protected through access level. Select the access permission level through the pull down menu [b]. Click on the “Add” action link [c], and the added ACL rule will be presented in the table [d].

HTTP Client Host IP: Specify a customized name for the IP address [e]. Select the forwarding mode via the pull down menu [f]. Finally, click on the action link “Enable” [g] to forward the IP address to the backend server.



The screenshot displays two configuration sections in the Fortinet web interface:

- HTTP ACL SETTING:**
 - a:** Matched Path Name: (text input field)
 - b:** Access permission level: 1--HTTPS ACCESS, SERVER AUTH (pull-down menu)
 - c:** Add|Delete (action link)
 - d:** A table with two columns: Matched Path Name and Access permission level.
- HTTP CLIENT HOST IP:**
 - e:** Customized Name: X-Forwarded-For (text input field)
 - f:** Mode: header (pull-down menu)
 - g:** Enable|Disable (action link)

All Policy Statistics

Select the tab “All Policy Statistics” [a]. This page shows how many times that all policies have been matched [b], as well as statistics of virtual service policy [c] and vlink policy [d]. You can clear desired statistics information by clicking on the action link “Clear” [e].

Virtual Services All Policy Statistics Policy Order Templates Virtual Service Global Setting

ALL POLICY STATISTICS Clear

VIRTUAL SERVICE POLICY STATISTICS Clear

	Virtual Service Name	qos clientport hits	qos network hits	persistent url hits	rcookie hits
1	asdf	0	0	0	0

VLINK POLICY STATISTICS Clear

	Vlink Name	qos clientport hits	qos network hits	persistent url hits	rcookie hits

Policy Order Templates

Make certain you are in Config mode and have selected the “Policy Order Templates” tab [a].

Assign a name for the new order template [b]. Specify the policy type via the scroll down menu [c]. Supply the desired index [d] for the specified policy. Then, click on the action link “Set” [e], and the created order template will be listed in the table below. If you click on the template name in the table [f], the new policy orders will be displayed in the column “Attribute” on the right [g].

Virtual Services All Policy Statistics Policy Order Templates Virtual Service Global Setting

ADD POLICY ORDER TEMPLATE Set

Order Template Name:

Policy Type: qos-clientport

Policy Index:

POLICY ORDER TEMPLATES LIST Delete

	Order Template Name	Value	Default Policy Type	Attribute
1	aa	1	qos-clientport	
		2	qos-network	
		3	pu	
		4	rc	
		5	ic	
		6	pc	
		7	qos-cookie	
		8	qos-hostname	
		9	qos-url	
		10	regex	
		11	header	
		12	hu	

Virtual Service Global Setting

Click on the “**Virtual Service Global Setting**” tab [a]. A new configuration window will be displayed.

Specify the proxy mode for the system via the radio buttons [b]. In addition to the “reverse” and “transparent” modes, the system also supports the “triangle” mode.

Enable global x-forwarded-for function by selecting the check box [c].

Set the client certificate header name [d]. The default name is X-Client-Cert.

Enable SLB virtual service health check via the check box [e].

Set the port range for data connection in passive FTP/FTPS in the text fields [f]. Users can add 20 to 1000 ports to a port range. The port range is global. It can be used for all FTP/FTPS virtual services.

Enable or disable the global SLB regexcase mode via the radio button [g].

Enable TCP connections soft close feature via the radio button [h].

Once any change is made, the “RESET” and “SAVE CHANGES” buttons [i] will appear. Click on the desired button to reset or save the change.

The screenshot shows the 'Virtual Service Global Setting' configuration window. It features a top navigation bar with tabs: 'Virtual Services', 'All Policy Statistics', 'Policy Order Templates', and 'Virtual Service Global Setting' (selected). At the top right are 'RESET' and 'SAVE CHANGES' buttons. The main configuration area is divided into several sections:

- SYSTEM MODE**: Contains three radio buttons: 'Operate as Reverse Proxy' (selected), 'Operate as Transparent Proxy', and 'Operate as Triangle Proxy'.
- HTTP CLIENT HOST IP**: Contains a checkbox 'Enable Global X-forwarded-for:'.
- XCLIENTCERT HEADER NAME**: Contains a text input field for 'XClientCert Header Name:'.
- SLB VIRTUAL HEALTH**: Contains a checkbox 'Enable SLB Virtual Health:'.
- FTP PASSIVE MODE PORT RANGE**: Contains two text input fields for 'Begin port:' and 'End port:', with a default range '(1024--65535)'.
- REGEX CASE MODE**: Contains two radio buttons: 'Regex case mode: insensitive' and 'Regex case mode: sensitive' (selected).
- TCP CONNECTIONS CLOSING MODE**: Contains two radio buttons: 'Mode: Both Actively and Passively Closing' and 'Mode: Only Passively Closing' (selected).

Callouts a-i point to specific elements: [a] points to the 'Virtual Service Global Setting' tab; [b] points to the 'Operate as Reverse Proxy' radio button; [c] points to the 'Enable Global X-forwarded-for:' checkbox; [d] points to the 'XClientCert Header Name:' text field; [e] points to the 'Enable SLB Virtual Health:' checkbox; [f] points to the 'Begin port:' and 'End port:' text fields; [g] points to the 'Regex case mode: sensitive' radio button; [h] points to the 'Mode: Only Passively Closing' radio button; and [i] points to the 'RESET' and 'SAVE CHANGES' buttons.

Check Lists

A health checker is defined as one transaction of health check. It consists of sending one message and receiving one response. A list of health checkers can compose a health checker list, which is identified by the health checker list name.

Note that the health checker list will work while doing health check only when the hc_type is set as “script_tcp” or “script_udp”.

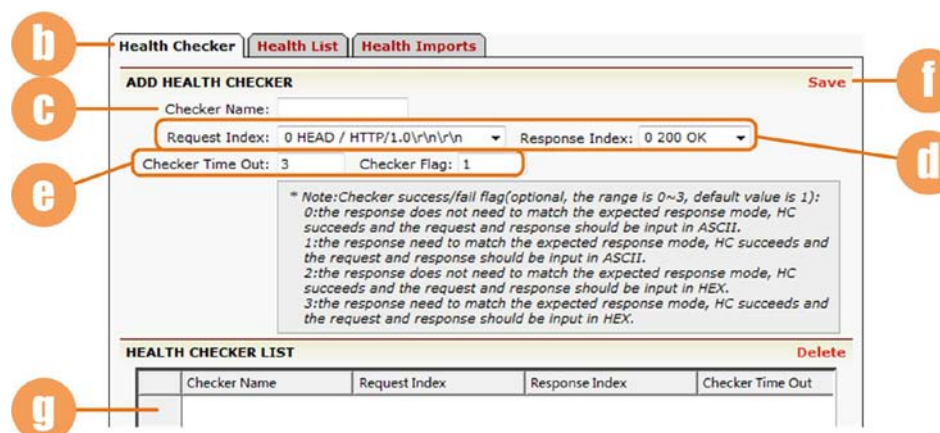
Make certain you are in Config mode and have selected “**Check Lists**” from the sidebar [a]. The configuration window will display three tabs [b]. The “Health Checker” page is displayed by default.



Health Checker

Supply a checker name [c]. Set the request index and response index by selecting from the scroll down menu [d]. Set checker timeout and checker flag [e]. Click on the “Save” action link [f]. The created health checker will be saved and displayed in the table below [g].

To edit a health checker, you can select it in the table [g] and then make desired changes. At last, remember to click on “Save” [f] to make the changes take effect.



Health List

Click on the “**Health List**” tab [a]. Assign a health list name [b]. Click on the action link “Add” [c]. A new health checker list is created and will be displayed in the sort ready table below [d]. Select a desired health list and double click on it or click on the action link “Edit” [e]. A new configuration page will be displayed.

This page is used to add members to the specified health list. Use the scroll down menu [f] to select the created checkers. Set the place index for the selected checker [g]. Click on the desired action link “Add” [h]. The selected checker is added in the specified health list, and will be displayed in the table below [i].

The screenshot shows the Fortinet web interface for configuring health lists. It includes tabs for 'Health Checker', 'Health List', and 'Health Imports'. The 'Health List' tab is active. The page is divided into three main sections: 'ADD HEALTH LIST', 'HEALTH LIST LIST', and 'ADD HEALTH LIST MEMBER'. The 'HEALTH LIST LIST' section contains a table with columns 'List Name' and 'List Member Count'. The 'ADD HEALTH LIST MEMBER' section includes a 'List Name' dropdown, a 'Checker Name' dropdown, and a 'Place' input field. The 'LIST MEMBERS' section at the bottom shows a table for adding members to the selected health list. Numbered callouts (a-i) point to specific UI elements: (a) Health List tab, (b) List Name input, (c) Add button, (d) Health List LIST table, (e) Delete/Edit links, (f) Checker Name dropdown, (g) Place input, (h) Add button, and (i) LIST MEMBERS table.

List Name	List Member Count
1 sample	0

Checker Name

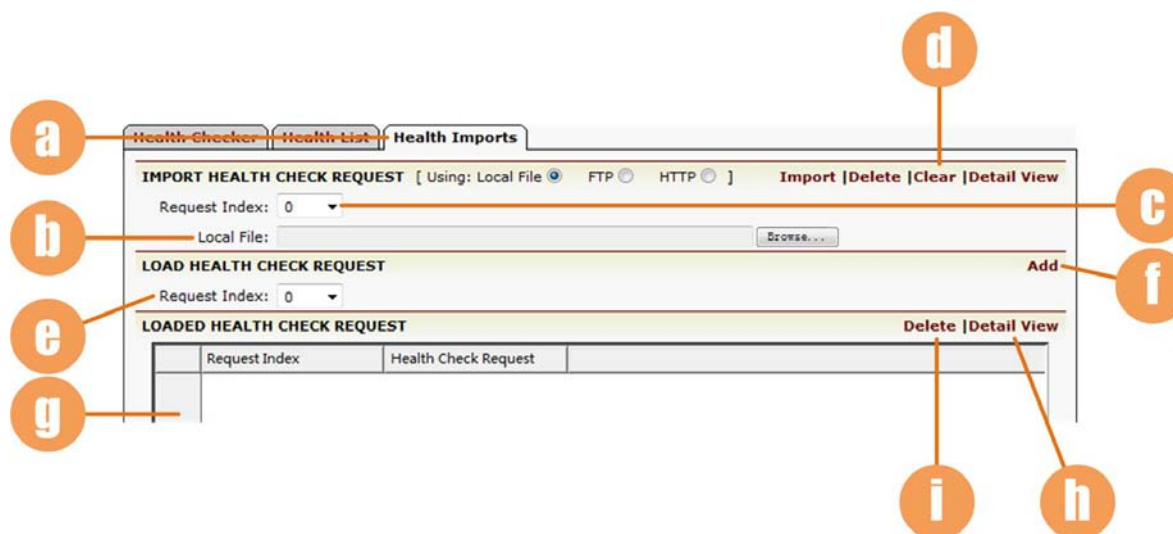
Health Imports

Click on the “**Health Imports**” tab [a]. You can import a health request/response file from a remote URL, and further load imported files into memory.

Input the URL which the request file should be imported from [b], and select the index of the file from the selector [c]. Then, click on the action link “Import” [d]. After the file is imported, you can select the index of the imported file from the selector [e] and click on the action link “Add” [f]. The newly imported request file will be displayed in the table below [g]. Note that only after you have imported a request file can you load it into the memory. You can view detailed information of a request file by double clicking it in the table [g] or clicking on the action link “Detail View” [h].

To delete a loaded request file, you must first select the file from the list [g] and click on the action link “Delete” [i], and then select the index of the file from the selector [c] and click on the action link “Delete” [d].

To delete a file which has been imported but not loaded into memory yet, you only need to select an index from the selector [c] and click on the action link “Delete” [d]. You can also clear all imported request files by clicking on “Clear” action link [d], or view details of desired imported request file by clicking on the action link “Detail View” [d].

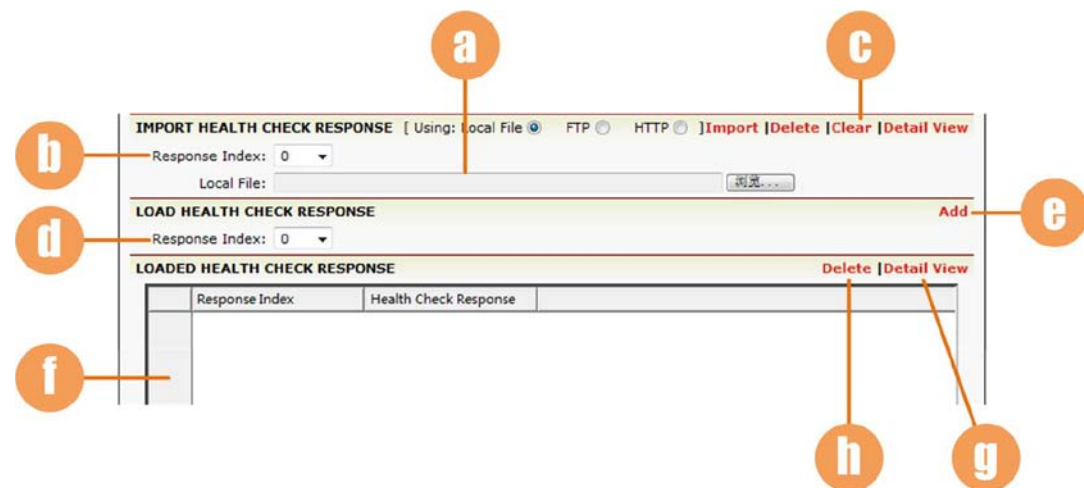


Health Imports (Continue)

To import a health response file from a remote URL, and further load the imported file into memory, you need to first input the URL which the response file should be imported from **[a]**, and select the index of the file from the selector **[b]**. Click on the action link “Import” **[c]**. After the file is imported successfully, you can select the index of the imported file from the selector **[d]** and click on the action link “Add” **[e]**. The newly imported response file will be displayed in the table below **[f]**. Note that only after you have imported a response file can you load it into the memory. You can view detailed information of a response file by double clicking it in the table **[f]** or clicking on the action link “Detail View” **[g]**.

To delete a loaded response file, you must first select the file from the list **[f]** and click on the action link “Delete” **[h]**. And then select the index of the file from the selector **[b]** and click on the action link “Delete” **[c]**.

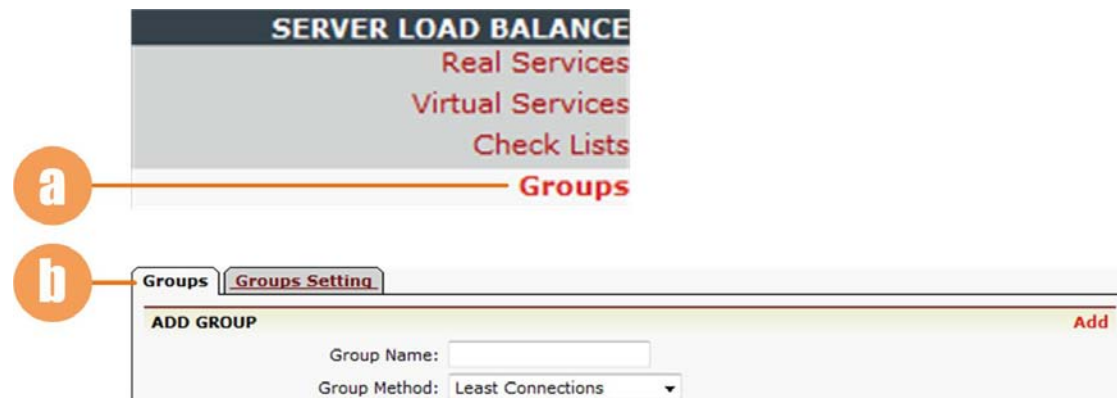
To delete a file which has been imported but not loaded into memory yet, you only need to select the index of the file from the selector **[b]** and click on the action link “Delete” **[c]**. You can also clear all imported response files by clicking on “Clear” action link **[c]**, or view details of desired imported response file by clicking on the action link “Detail View” **[c]**.



Groups

It is time to assign the previously defined real services to groups. A group is first defined by using the slb group command. This command will define a group to which you may add real servers.

Make certain you are in Config mode and have selected the feature link “**Groups**” from the sidebar [\[a\]](#). The configuration window will display two tabs. Click on the “**Groups**” tab [\[b\]](#).

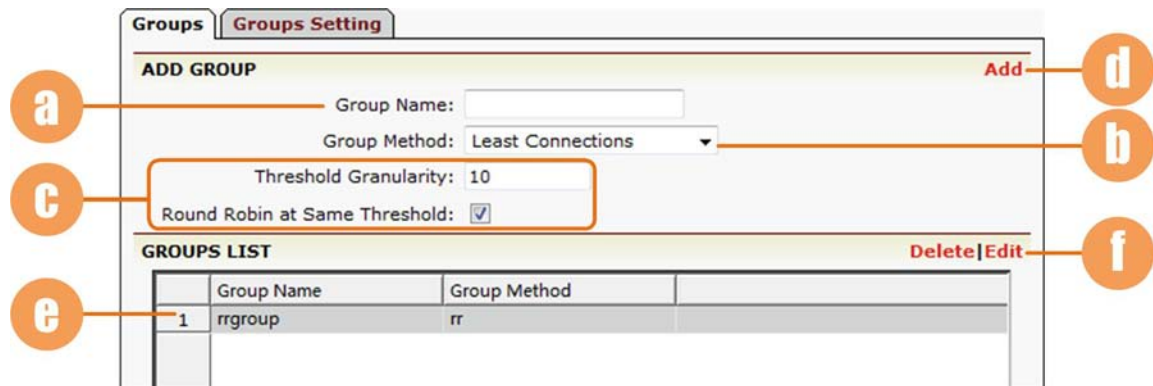


Groups

Supply the group name [\[a\]](#). Select a group method from the pull down menu [\[b\]](#). Depending on the group method selected, different parameter fields will appear for configuration [\[c\]](#).

After making configurations on those parameter fields, click on the action link “Add” [\[d\]](#). Then the newly created group will be displayed in the sort ready table below [\[e\]](#).

Choose a group in the table and double click on it or click on the action link “Edit” [\[f\]](#). A new configuration page will be displayed.



The screenshot shows the 'Groups Setting' page in the Fortinet web interface. It features an 'ADD GROUP' section with a 'Group Name' text box (labeled 'a'), a 'Group Method' dropdown menu set to 'Least Connections' (labeled 'b'), and configuration options for 'Threshold Granularity' (set to 10, labeled 'c') and 'Round Robin at Same Threshold' (checked, labeled 'c'). An 'Add' button is on the right (labeled 'd'). Below is a 'GROUPS LIST' table (labeled 'e') with columns for Group Name, Group Method, and an action column. The table contains one entry: 'rrgroup' with method 'rr'. The action column has 'Delete' and 'Edit' links (labeled 'f').

	Group Name	Group Method	
1	rrgroup	rr	

Groups (Continue)

You can modify the group method and make relevant configurations in the area [a], and click on “Save” [b] to save your changes. Depending on the group method selected, different parameter fields will appear for configuration.

Input the number (1-65535) of real servers to activate in the text field [c]; for pi group, you can also set persistence timeout for it. Then, click on “Set” [d] to save your setting.

To assign an IP Pool to this group, you should select a pool name via the pull down menu [e], and click on the “Add” action link [f], the created IP pool will displayed in the following table [g].

The screenshot shows the 'Groups Setting' interface. It is divided into three main sections: 'GROUP INFORMATION', 'GROUP SETTINGS', and 'IP POOLS LIST'. Annotations a through g point to specific elements:

- a**: Points to the 'GROUP INFORMATION' section header.
- b**: Points to the 'Cancel | Save' buttons at the top right of the 'GROUP INFORMATION' section.
- c**: Points to the 'Number of Active Real Servers' input field in the 'GROUP SETTINGS' section.
- d**: Points to the 'Set | Clear' buttons at the top right of the 'GROUP SETTINGS' section.
- e**: Points to the 'All IP Pools' dropdown menu in the 'IP POOLS LIST' section.
- f**: Points to the 'Add | Delete | Clear' buttons at the top right of the 'IP POOLS LIST' section.
- g**: Points to the 'Pool Name' column header in the table below the dropdown.

GROUP INFORMATION

Group Name: Group

Method: ▼

Threshold Granularity:

Round Robin at Same Threshold: ☒

Keep group member configuration only: ☐

** Note: Change group parameter may not success because of the compatibility among real service type, group method, policy and virtual service.
For example:
Group member and group method is not compatible: A group with TCP member can not change method from Round Robin to Insert Cookie.
Group method and virtual service type is not compatible: A Hash Header method group can not associate with a FTP virtual service by any policy.
Group method and policy is not compatible: A group with insert cookie method can not associate with virtual service by policies except default and insert cookie.*

GROUP SETTINGS

Number of Active Real Servers: (1-65535)

Persistence Timeout: Minutes (0-50000)

IP POOLS LIST

All IP Pools: ▼

Pool Name

Groups (Continue)

To assign a configured real service to a newly created group, you can select an eligible real service via the pull down menu [a], configure required parameter [b], and set the priority of the group member [c].

For the parameter [b], set the Weight value for the method lc, rr, ph, pi, ic, rc, hc, hh or sslsid; set the Cookie value for pc; set the URL value for pu; for other methods, no parameter will be required for configuration.

Then, click on the “Add” action link [d] and the assigned real service will appear in the table [e]. You can change the configured parameters in the table directly, and click on “Save” [d] to save your changes.

At this page, you can view real-time group statistics [f]. To view the latest statistics, you can click on “Refresh” [g].

GROUP MEMBERS Add | Delete | Save

Eligible Reals: MOSS1

Weight: 1

Priority: 0

	Real Service Name	Weight	Priority	Active	Reason
1	MOSS1	1	0	NO	HEALT
2	Real1	1	0	NO	HEALT

GROUP STATISTICS Refresh

Group Name	Method	Hits
g1	lc	0

Groups Setting

Click on the “**Groups Setting**” tab [a], and a new configuration window will be displayed. Set “pi” group method timeout value for SLB [b]. Use the pull down menu to set the SLB insert/rewrite cookie mode [c]. Use the pull down menu to finish the insert cookie setting [d]. Remember to click on the “**SAVE CHANGES**” button to save the settings [e].

To assign an IP pool as a global IP pool, select an IP pool via the pull down menu [f], and click on the “**Add**” action link [g], the created IP pool will be displayed in the following table [h].

The screenshot shows the 'Groups Setting' configuration window. It has a 'Groups' tab and a 'Groups Setting' sub-tab. At the top right are 'RESET' and 'SAVE CHANGES' buttons. The 'GROUPS SETTING' section contains: 'Persistence Timeout: 0', 'Icookie Setting: plainname' (a dropdown menu), and 'Icookie Setting: always' (another dropdown menu). Below this is the 'GLOBAL IP POOLS LIST' section, which includes a dropdown menu 'All IP Pools: Pool1' and an 'Add | Delete' link. At the bottom is a table with one row containing '1' and 'Pool1'. Callouts a through h point to various elements: [a] points to the 'Groups Setting' tab, [b] points to the 'Persistence Timeout' field, [c] points to the first 'Icookie Setting' dropdown, [d] points to the second 'Icookie Setting' dropdown, [e] points to the 'SAVE CHANGES' button, [f] points to the 'All IP Pools' dropdown, [g] points to the 'Add | Delete' link, and [h] points to the table.

	Pool Name
1	Pool1

Application Setting

Make certain you are in **Config mode** and have selected the feature link “**Application Setting**” from the sidebar [a]. The configuration presents two tabs. The SIP NAT configuration page is displayed by default.

SIP NAT

Users may set the SIP NAT rules for the defined SIP real services on this configuration page.

Turn on the multi-register function via the check box [b], if the backend servers don’t share the same database.

Set the source IP address and port of a SIP real service [c]. And set the source IP address and port of the virtual service [d] which the packets from the SIP real service will be translated into. Configure the timeout value (in seconds) [e]. Specify the protocol of the packets to be translated through the pull down menu [f]. Click on the action link “Add” [g] to add the SIP NAT rule. Then, the rule will be displayed in the sort ready table [h].

Users can view the statistics of all the SIP NAT rules [i].

Direct Forward

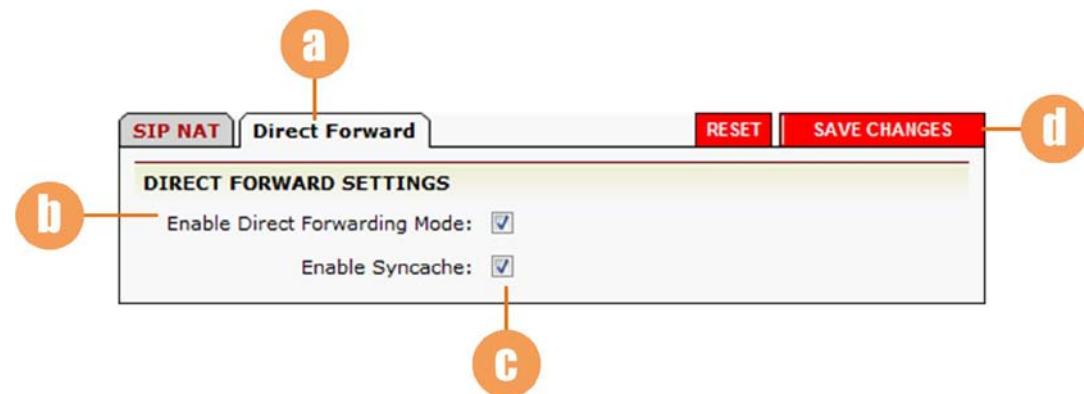
Direct Forward is a new L4 SLB module by utilizing a multi-thread and non-lock architecture based on a multi-core system. This new architecture has maximized the advantage of the multi-core system. Compared with the traditional L4 SLB, the Direct Forward module provides remarkably better L4 SLB performance.

Click on the “**Groups Setting**” tab [\[a\]](#).

To enable the Direct Forward function, you can select the check box [\[b\]](#).

You can also enable the Direct Forward module’s syncache function via the check box [\[c\]](#). This function can avoid synflood attacking effectively.

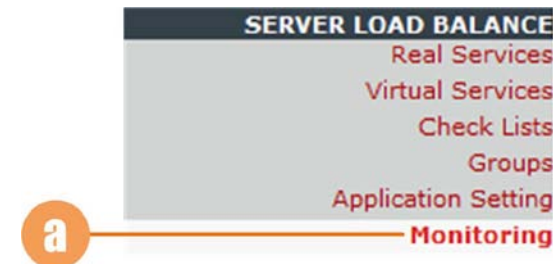
Remember to click on the “**SAVE CHANGES**” button to save the settings [\[d\]](#).



Monitoring

This feature allows you to monitor the general status of the related groups and real services of a specified virtual service, and further view their statistic information.

Make certain you are in Enable mode and select “**Monitoring**” from the sidebar [a]. The configuration presents four tabs. The “**Status** page” [b] is displayed by default.



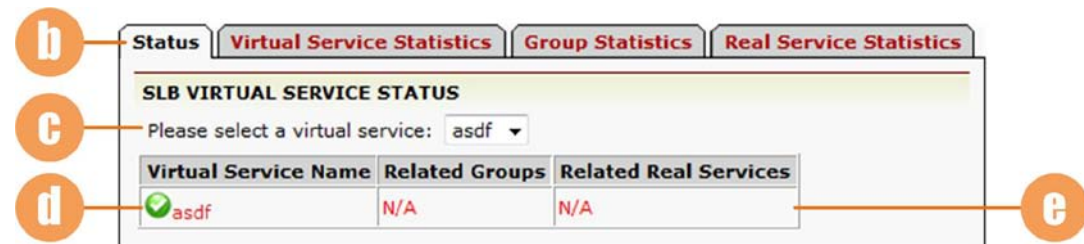
Status

Select a desired virtual service via the selector [c], and the general status information of its related groups and real services will be displayed in the table [d]:

- : Enabled and Up (healthy);
- : Enabled but Down (unhealthy);
- : Disabled.

Note: The icon descriptions also apply to the “Virtual Service Statistics” and “Real Service Statistics” pages.

You can view the statistics of a virtual service, a group or a real service by clicking on it in the table [e].



Proxy

Compression

Setting

Make certain that you are in the **Config mode** and have selected “**Compression**” [a]. The configuration window will present three tabs. The “**Setting**” page is displayed by default [b].

Enable or disable the HTTP data compression via the check box [c]. The selector [d] lists all configured HTTP/HTTPS virtual services. You can choose one and click on the “Enable VS Compression” action link [e]. The HTTP/HTTPS virtual service for which compression feature is enabled will be displayed in the sort ready table [f]. To disable the compression of a virtual service, you can select the service in the table [f] and click on the “Disable VS Compression” action link [e].

You can add a url-exclude policy for a virtual service to disable the compression function. Input the wildcard expression [g], and select a desired HTTP/HTTPS virtual service from the selector [h]. Click on the action link “Add” [i], and the new configuration will be displayed in the sort ready table below [j].

PROXY
Compression

Setting | **Type** | **Statistics**

HTTP COMPRESSION SETTING Enable VS Compression | Disable VS Compression

Enable Compression: ☐

HTTP/HTTPS Virtual Service(s): asdf

COMPRESSION IS ENABLED FOR THE FOLLOWING HTTP/HTTPS VIRTUAL SERVICES:

	Virtual service
1	asdf

COMPRESSION URL EXCLUDE Add

Wildcard Expression:

HTTP/HTTPS Virtual Service(s): asdf

URL EXCLUDE LIST Delete

	Virtual service	Wildcard Expression
--	-----------------	---------------------

Callouts: a points to the 'Compression' title; b points to the 'Setting' tab; c points to the 'Enable Compression' checkbox; d points to the 'HTTP/HTTPS Virtual Service(s)' dropdown; e points to the 'Enable VS Compression' and 'Disable VS Compression' links; f points to the table of virtual services; g points to the 'Wildcard Expression' input field; h points to the 'HTTP/HTTPS Virtual Service(s)' dropdown; i points to the 'Add' button; j points to the 'URL EXCLUDE LIST' table.

Type

Click on the “**Type**” tab [\[a\]](#). Enter a particular browser name in the field [\[b\]](#). Select one compression MIME type from the “Mime Type” select box [\[c\]](#). Click on the “Add Mime Type” action link [\[d\]](#). The added user agent and mime type will be displayed in the table below [\[e\]](#).

To remove the added user agent and mime type, select a desired entry or multi entries from the displayed list [\[f\]](#) and click on the “Delete Mime Type” action link [\[d\]](#).

Click on “Apply Tested User Agents” [\[d\]](#), and the default user agents and mime types will be displayed in the table [\[e\]](#).

COMPRESSION MIME TYPES [Add Mime Type](#) [Delete Mime Type](#) [Apply Tested User Agents](#)

User Agent:

Mime Types: JS (JavaScript)

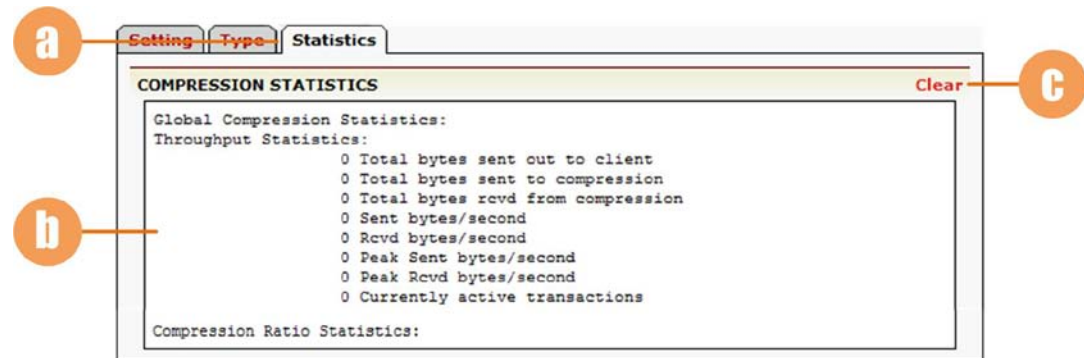
SUPPORTED COMPRESSION MIME TYPES

	User Agent	Mime Type
1	MSIE 6	css
2	MSIE 6	js
3	MSIE 7.0	css
4	MSIE 7.0	js
5	MSIE 8.0	css
6	MSIE 8.0	js
7	Mozilla/5.0	css
8	Mozilla/5.0	js

Statistics

Click on the “Statistics” tab [\[a\]](#).

The main window displays global compression statistics and content statistics information [\[b\]](#). Click on “Clear” action link [\[c\]](#), and the statistics will default to 0.



Caching Proxy

The reverse proxy cache better enhances the overall speed and performance of your Web servers. Using the cache will improve website performance and throughput, and will reduce server load by moving heavily requested data closer to the end user and away from the backend servers. You may set up limitations on queries made to your network based on header length, request length, URL and query length as well as ASCII character ranges and keyword matches.



Global URL Filter

Make certain you are in **Config mode** and have selected the feature link “**Caching Proxy**” [a]. The configuration window will display four tabs, and the default page is “**Global URL Filter**” [b].

On the Global URL Filter page, you can enable the global URL filtering feature by selecting the “**Enable**” check box [c]. Save the change by clicking on the “**SAVE CHANGES**” button [d]. After saving, more configurations appear.

You can set the behavior mode for filtering as active or passive [e], and enable or disable the control characters filtering feature of URL filter via the check box [f]. Configure the destination email address for filter related alerts and the threshold for the number of dropped requests before issuing the alert [g].

Click on the “**SAVE CHANGES**” button to save the changes [d].



Global URL Filter (Continue)

Configure length-based filtering rules for requests coming into the network [a]. Then click on the action link “SAVE CHANGES” to save your settings [b].

Assign the default filtering policy as permit or deny [c]. Supply the match keyword and click on the “Test” button to check whether the inputted keyword matches one of configured regular expressions for URL filter rules [d]. Confirm your settings, and click the action link “Add” [e]. The restrictions will be displayed in the table [f]. Note: If you want to change the default global filtering policy, you must first delete all configured restriction entries displayed in the table here.

Name the variable in the text field [g], and set the variable type (integer or string) [h]. Click the desired action link “Add” [i]. The new restriction will be displayed in the table [j].

Configure character-based filter rules for requests coming into the network. To deny specific requests based on URL character ranges (ASCII values), enter the starting [k] and ending [l] values of the character range respectively and click on the action link “Add” [m]. The new restriction will be displayed in the table [n].

This page also displays statistics about the filter URL keyword default policy, deny policy and permit policy [o]. You can click on “Clear” [p] to clear all statistics.

The screenshot shows the 'LENGTH BASED FILTERING' configuration page. It includes sections for 'LENGTH BASED FILTERING', 'KEYWORD FILTERING', 'TYPE FILTERING', 'CHARACTER BASED FILTERING', and 'KEYWORD FILTERING STATISTICS'. Callouts a-p point to various fields and buttons: a (Header), b (SAVE CHANGES), c (Default Policy), d (Test button), e (Add/Delete), f (Keyword table), g (Variable Name), h (Variable Type), i (Add/Delete), j (Variable table), k (Character Range From), l (Character Range To), m (Add/Delete), n (Character Range table), o (Statistics), and p (Clear button).

LENGTH BASED FILTERING

Header: 1024 Request: 10000 URL: 1024
Query: 1024 Data: 512 Variable: 128

KEYWORD FILTERING

Default Policy: permit ☒ deny ☐
Match Keyword: Test

TYPE FILTERING

Variable Name: Variable Type: string
Variable Name Variable Type

CHARACTER BASED FILTERING

Character Range From: Character Range To:
Character Range ... Character Range ...

KEYWORD FILTERING STATISTICS

virtual service global - default permit - 0 requests matched default
virtual service global - default permit - 0 requests matched default
There are no permit rules configured for this vip. Please use the command show statistics url keyword deny

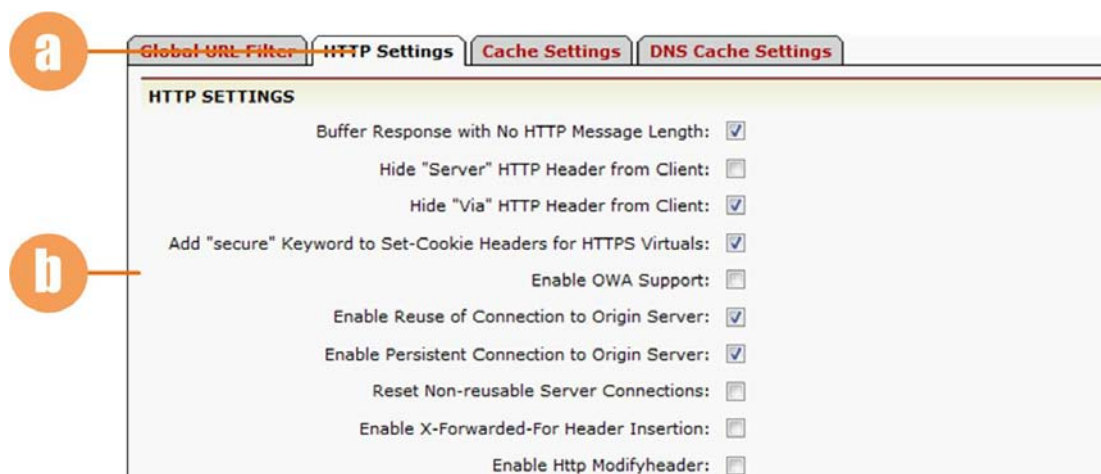
HTTP Settings

This page allows you to set/enable various parameters for your network caching strategy. For specific HTTP settings based on individual virtual sites, please refer to the “Virtual Services” section in the “Server Load Balancing” chapter.

Select the “HTTP Settings” tab [\[a\]](#).

HTTP Setting: You may enable the following functions [\[b\]](#):

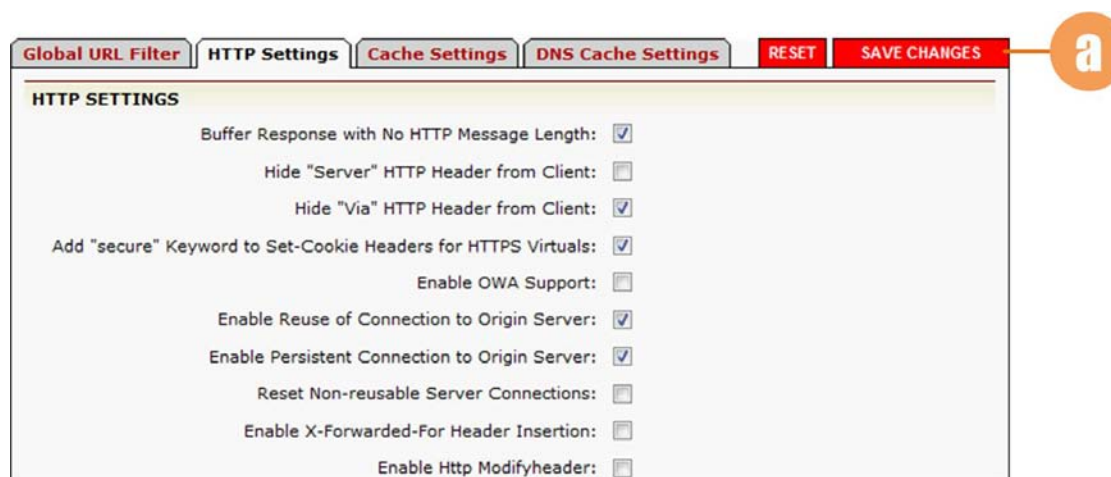
- Buffer response with no HTTP message length: When enabled, responses that don’t process an “end of response” HTTP message length indicator within the headers will still be buffered before returning the information to the client.
- Hide “Server” HTTP header from client: Removes Server header from the response that is forwarded to the client.
- Hide “Via” HTTP header from client: Does not insert Via header into the response that is forwarded to the client.
- Add “secure” keyword to Set-Cookie headers for HTTPS Virtuals: Inserts secure keyword into the Set-Cookie header in the responses that are sent to HTTP clients.
- OWA support: Enables or disables the subsystem, which inserts OWA (Outlook Web Access) specific header FRONT-END-HTTPS: on in the requests forwarded to backend servers.



HTTP Settings (Continue)

- Reuse of connection to origin server: If disabled, each connection will be used only for a single transaction after which the connection is terminated. If enabled, each server connection will be used by multiple transactions.
- Persistent connection to origin server: When connection reuse is enabled, enabling connection persistence ensures that all transactions from the same client connection are forwarded to the same backend server. If connection reuse is enabled but connection persistence is disabled, then transactions from the same client connection may be forwarded to different backend servers. Note that the connection persistence option is only applicable when real server persistence methods such as hash IP or persistent cookie are disabled.
- Reset non-reusable server connections.
- X-Forwarded-For header insertion: Turns on/off inserting the X-Forwarded-For header in the request forwarded to the backend server. The client IP address is set as the value of this header. This header is currently inserted even if the client request already has an X-Forwarded-For header.
- HTTP Modifyheader: Enables or disables HTTP modify header.

Confirm your settings and click on “SAVE CHANGES” [a] to make them take effect.



Global URL Filter HTTP Settings Cache Settings DNS Cache Settings RESET SAVE CHANGES

HTTP SETTINGS

- Buffer Response with No HTTP Message Length: ☒
- Hide "Server" HTTP Header from Client: ☐
- Hide "Via" HTTP Header from Client: ☒
- Add "secure" Keyword to Set-Cookie Headers for HTTPS Virtuals: ☒
- Enable OWA Support: ☐
- Enable Reuse of Connection to Origin Server: ☒
- Enable Persistent Connection to Origin Server: ☒
- Reset Non-reusable Server Connections: ☐
- Enable X-Forwarded-For Header Insertion: ☐
- Enable Http Modifyheader: ☐

HTTP Settings (Continue)

HTTP OWA Virtual: Set an OWA virtual service in the text field [a]. Click on the desired action link “Add” [b], and the OWA virtual service name will be displayed in the table [c]. To delete an entry, select the desired entry and click on the desired action link “Delete” [b].

HTTP XClientCert Virtual: Set an Xclientcert virtual service in the text field, and select the transfer mode and certificate type via the selectors [d]. Click on the desired link “Add” [e], and then the Xclientcert virtual service name will be displayed in the table [f]. To delete an entry, select the desired entry and click on the desired link “Delete” [e].

HTTP Host Permissions: Set the host name for HTTP Host Permissions [g]. Click on the desired action link “Add” [h], and then the host will be displayed in the sort ready table [i]. To delete an entry, select the desired entry and click on the desired link “Delete” [h].

HTTP Method Permissions: Use the selector [j] to set the virtual IP. Select the desired HTTP method in the field [k] and click on the button [l] to add it into the text field [m]. You can also select one method in the field [m] and click on the button [n] to move the method to the “Allowed HTTP method” list.

The screenshot shows the Fortinet Proxy configuration interface with the following sections and elements:

- HTTP OWA Virtual:**
 - Text field [a] for OWA Virtual.
 - Action links [b] Add/Delete.
 - Table [c] with one entry: OWA Virtual, OWA Virtual.
- HTTP XClientCert Virtual:**
 - Text field [d] for XClientCert Virtual.
 - Transfer Mode selector [d] (header).
 - Certificate Type selector [d] (body).
 - Action links [e] Add/Delete.
 - Table [f] with one entry: 1, asdf, header, body.
- HTTP Host Permissions:**
 - Text field [g] for Hostname.
 - Action links [h] Add/Delete.
 - Table [i] with one entry: Allowed HTTP H...
- HTTP Method Permissions:**
 - Virtual IP selector [j] (0.0.0.0).
 - Allowed HTTP methods list [k] (get, post, put, delete, trace).
 - Denied HTTP methods list [m] (empty).
 - Buttons [l] >> and [n] << to move methods between lists.
 - Action link [j] Clear.

HTTP Settings (Continue)

HTTP Error Pages: Supply the HTTP error code [a]. Configure the desired destination that generated the error in the “Hostname” text field [b]. Set the location of the customized error page in the text field “URL” [c]. The supported HTTP error codes for importing customized error pages include:

400: Bad request

403: Forbidden

412: Precondition failed

416: Requested range not certifiable

502: Bad gateway

503: Service unavailable

The screenshot shows the 'HTTP ERROR PAGES' configuration window. It includes a title bar with 'Add|Delete' buttons. The form contains the following fields and controls:

- Error Code:** A dropdown menu currently showing '400'. Callout 'a' points to this field.
- Hostname:** A text input field. Callout 'b' points to this field.
- URL:** A text input field. Callout 'c' points to this field.
- Enabled:** A checkbox area with a '>>' button.
- Disabled:** A checkbox area with a '<<' button.

Cache Settings

Select the “Cache Settings” tab [\[a\]](#). You will be presented with three sub-tabs. The default page is “Cache Settings” [\[b\]](#).

Cache Settings

You can enable the cache function via the check box [\[c\]](#). If enabled, you need to further set the maximum size of cacheable objects (defaults to 5120KB) and the expiration time of the cached objects (defaults to 82800 seconds) in the text fields [\[d\]](#). Then, click on “SAVE CHANGES” button to save your settings [\[e\]](#).

This page also displays the cache settings of existing virtual services [\[f\]](#). Here, you can enable or disable the cache setting for a virtual service. To do this, simply select a desired virtual service in the table and click on the “Enable” or “Disable” action link [\[g\]](#).

To view specific cache contents, just supply the host name and URL regular expression [\[h\]](#) and click on the action link “View” [\[i\]](#).

The screenshot shows the Fortinet Proxy configuration interface. At the top, there are tabs: Global URL Filter, HTTP Settings, Cache Settings (selected), and DNS Cache Settings. To the right of these tabs are buttons for RESET and SAVE CHANGES. Below the tabs, there are three sub-tabs: Cache Settings (selected), Cache Filter, and Caching Proxy Statistics. The main content area is divided into three sections:

- CACHE SETTINGS:** This section contains a checkbox for 'Enable Cache' (checked), a text field for 'Maximum Cacheable Object Size(KB)' (5120), and a text field for 'Expiration Time(Seconds)' (82800). To the right of these fields is a button labeled 'Enable | Disable'.
- VIRTUAL SERVICE CACHE SETTINGS:** This section contains a table with the following data:

	Virtual Service Name	Enabled	
1	asdf	YES	
- VIEW CACHE CONTENT:** This section contains two text fields: 'Host:' and 'URL Regex:'. To the right of these fields are buttons for 'View' and 'Clear'.

Callouts a-i point to specific elements: a points to the 'Cache Settings' tab; b points to the 'Cache Settings' sub-tab; c points to the 'Enable Cache' checkbox; d points to the 'Maximum Cacheable Object Size(KB)' text field; e points to the 'SAVE CHANGES' button; f points to the 'VIRTUAL SERVICE CACHE SETTINGS' table; g points to the 'Enable | Disable' button; h points to the 'Host:' text field; and i points to the 'View' button.

Cache Settings (Continue)

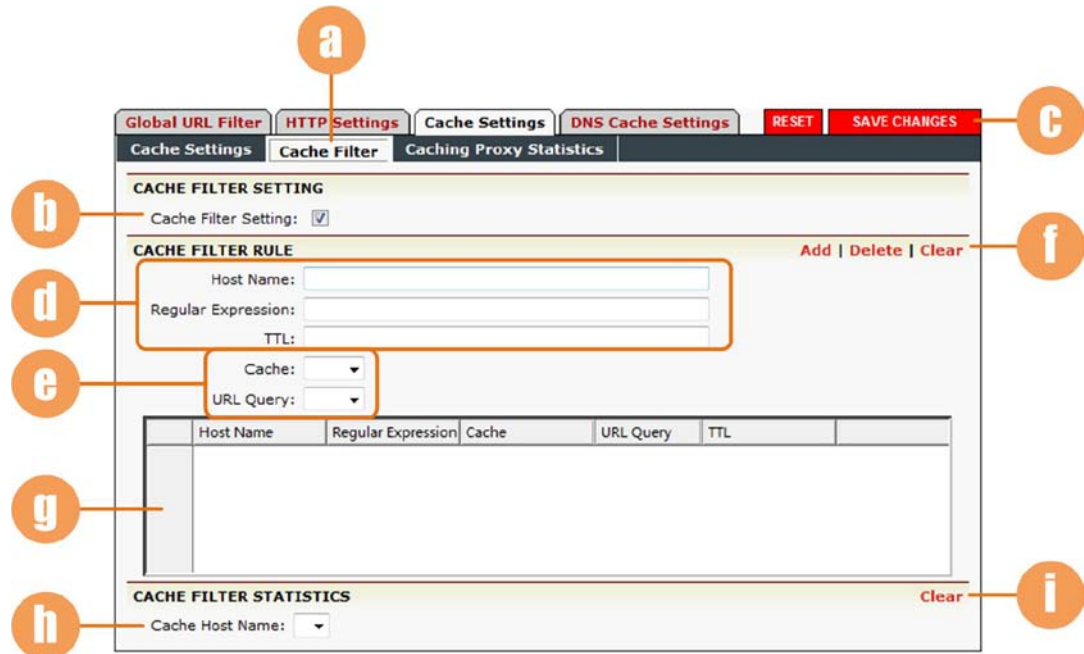
Cache Filter

Select the sub-tab “Cache Filter” [a].

You can enable the cache filter function via the check box [b]. Remember to click on the “SAVE CHANGES” button [c] to save your change.

To add a cache filter rule, supply the host name, regular expression and TTL in the text fields [d] and choose to enable (yes) or disable (no) the Cache or URL query function for the host via the selectors [e]. Then, click on the action link “Add” [f], and the rule will be displayed in the table [g].

The “Cache Host Name” selector lists all hosts configured with cache filter rules. You can choose one from the selector [h] to view related cache filter statistics. To clear the statistics, simply click on the action link “Clear” [i].



The screenshot shows the Fortinet Proxy configuration interface for the 'Cache Filter' sub-tab. The page is divided into several sections: 'CACHE FILTER SETTING', 'CACHE FILTER RULE', and 'CACHE FILTER STATISTICS'. Annotations a-i point to specific elements:

- a**: Points to the 'Cache Filter' sub-tab in the top navigation bar.
- b**: Points to the 'Cache Filter Setting' checkbox, which is checked.
- c**: Points to the 'SAVE CHANGES' button in the top right corner.
- d**: Points to the 'Host Name', 'Regular Expression', and 'TTL' input fields in the 'CACHE FILTER RULE' section.
- e**: Points to the 'Cache' and 'URL Query' dropdown selectors in the 'CACHE FILTER RULE' section.
- f**: Points to the 'Add | Delete | Clear' action links in the 'CACHE FILTER RULE' section.
- g**: Points to the table displaying the list of cache filter rules.
- h**: Points to the 'Cache Host Name' dropdown selector in the 'CACHE FILTER STATISTICS' section.
- i**: Points to the 'Clear' button in the 'CACHE FILTER STATISTICS' section.

Host Name	Regular Expression	Cache	URL Query	TTL

Cache Settings (Continue)

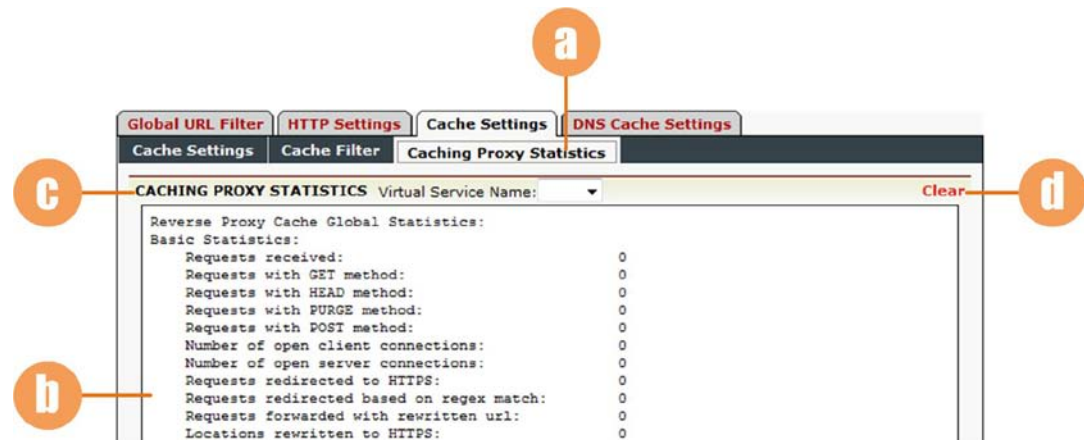
Caching Proxy Statistics

Click on the “**Caching Proxy Statistics**” sub-tab [\[a\]](#).

The window displays the statistics information about reverse proxy cache [\[b\]](#), including basic statistics and advanced statistics.

You can select a desired virtual service from the selector [\[c\]](#) to view its cache proxy statistics.

To clear the statistics, simply click on the action link “**Clear**” [\[d\]](#).



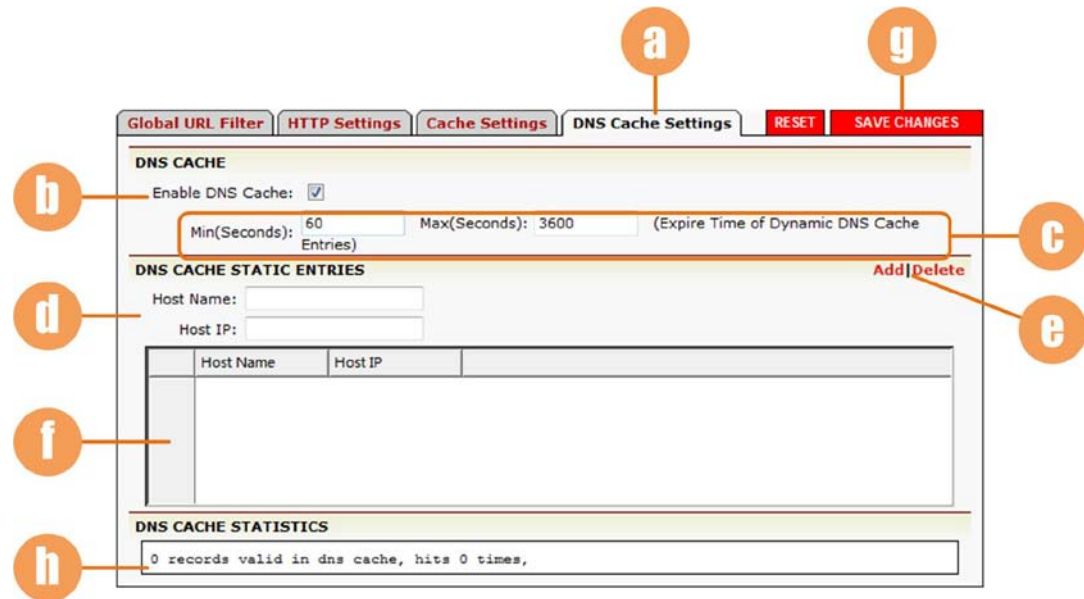
DNS Cache Settings

DNS Cache Settings

Click on the “**DNS Cache Settings**” tab [a]. Enable the DNS cache via the check box [b]. Set the time to live for the cache entry in the text field [c].

In “DNS CACHE STATIC ENTRIES”, enter the desired host name and IP in the text fields [d] and click on the action link “Add” [e]. Then the added host will be displayed in the table [f]. Remember to click on the “SAVE CHANGES” button [g] after changing the DNS Cache settings. You can reset the configuration by clicking on the “RESET” button [g].

In “DNS CACHE STATISTICS”, all DNS cache statistics information is displayed [h].



The screenshot shows the Fortinet web interface for DNS Cache Settings. The page has a top navigation bar with tabs: Global URL Filter, HTTP Settings, Cache Settings, and DNS Cache Settings (selected). There are also buttons for RESET and SAVE CHANGES. The main content area is divided into three sections: DNS CACHE, DNS CACHE STATIC ENTRIES, and DNS CACHE STATISTICS.

- Callout a:** Points to the "DNS Cache Settings" tab.
- Callout b:** Points to the "Enable DNS Cache" checkbox, which is checked.
- Callout c:** Points to the "Min(Seconds): 60" and "Max(Seconds): 3600" input fields, with a note "(Expire Time of Dynamic DNS Cache Entries)".
- Callout d:** Points to the "Host Name:" and "Host IP:" input fields.
- Callout e:** Points to the "Add/Delete" action link.
- Callout f:** Points to the table for "DNS CACHE STATIC ENTRIES". The table has columns for Host Name and Host IP.
- Callout g:** Points to the "RESET" and "SAVE CHANGES" buttons.
- Callout h:** Points to the "DNS CACHE STATISTICS" section, which displays "0 records valid in dns cache, hits 0 times,".

SSL

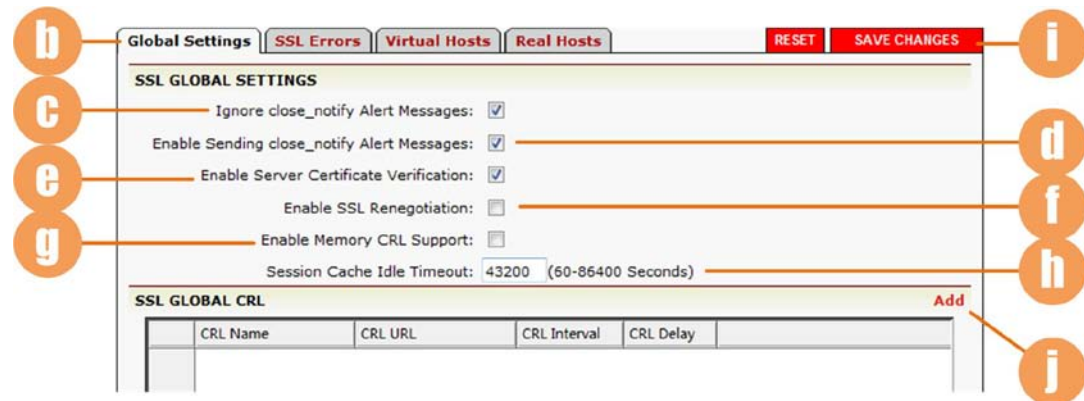
To do SSL configurations, **make certain you are in Config mode** and select the “SSL” feature link [a]. The configuration window will display four tabs: Global Settings, SSL Errors, Virtual Hosts and Real Hosts. The Global Settings page is displayed by default [b].

Global Settings

On this page, you can complete the following SSL global settings: specify whether to ignore the close_notify alert messages [c], specify whether to enable sending the close_notify alert messages [d], enable the certificate verification function [e], enable the SSL renegotiation function [f], enable the CRL (Certification Revocation List) memory support function [g], and set the session cache idle timeout (in seconds) [h].

Then, confirm your settings and click on “SAVE CHANGES” [i] to make them take effect.

To add a global CRL, click on the action link “Add” [j], and a new configuration window will appear.



Global Settings (Continue)

In the new window, assign a name to the CRL in the text field [a]. Specify the URL where the CRL is downloaded [b], the time interval between two downloads [c] and the delay time [d]. At last, click the desired button to save the configurations [e]. The new added global CRL is displayed in the sort ready table [f].

A new session appears after adding the global CRL [g]. Select the desired global CRL via the pull down menu [h], and then associate the global CRL with the specified virtual host or disassociate the global CRL from the specified virtual host via the buttons [i].

The image displays three screenshots of the Fortinet Proxy configuration interface, with callouts a through i indicating specific fields and actions.

Top Screenshot: CRL Configuration

- a**: CRL Name text field.
- b**: CRL URL text field.
- c**: CRL Interval (1440) (Minutes) field.
- d**: CRL Delay (0) (Minutes) field.
- e**: Cancel | Save & Add Another | Save buttons.

Middle Screenshot: SSL GLOBAL CRL Table

- f**: Table showing the added CRL.

	CRL Name	CRL URL	CRL Interval	CRL Delay	
1	sample	http://www.abc.com	1440	0	

Bottom Screenshot: GLOBAL CRL ASSOCIATION WITH HOSTS

- g**: Global CRL dropdown menu (sample).
- h**: Dissociated Hosts list.
- i**: Association buttons (>> and <<).
- g**: Associated Hosts list.

Global Settings (Continue)

You can import a trusted CA certificate via selecting a local file, using TFTP or manually inputting the certificate.

To import from a local file, specify the file path in the text field [\[a\]](#); to import via TFTP, select the radio button “TFTP” and supply the server address [\[b\]](#); to import via manual input, select the radio button “Manual Input” and supply the global certificate in the text field [\[c\]](#). After confirming the supplied information, click on the action link “Import” to import the CA certificate [\[d\]](#).

To view the global CA certificate information, click on the “View” action link [\[e\]](#). Then a new window displays all global CA certificates in numeric order [\[f\]](#). You can view the simple or complete mode of certificates via the radio buttons [\[g\]](#).

You can also delete an undesired certificate. Select the sequence number of the certificate from the list [\[h\]](#) and click on the “Delete” button [\[i\]](#) to start deleting.

You can further import or view CRL CA certificate by following the steps of importing or viewing global CA certificate.

The screenshot displays the Fortinet Global Settings interface for CA certificates. It is divided into two main sections: 'GLOBAL ROOT CA CERTIFICATE' and 'VIEW GLOBAL ROOT CA CERTIFICATE'.

- GLOBAL ROOT CA CERTIFICATE:** This section contains two sub-panels. The top panel is for 'GLOBAL ROOT CA CERTIFICATE' with radio buttons for 'Using: Local File' (selected), 'TFTP', and 'Manual Input'. It includes a 'Local File Path' text field with a 'Browse...' button. The bottom panel is for 'GLOBAL CRL CA CERTIFICATE' with similar radio buttons and a 'Local File Path' text field with a 'Browse...' button. Callout **a** points to the 'Local File Path' field in the top panel. Callout **b** points to the 'TFTP' radio button in the bottom panel. Callout **c** points to the 'Global Root CA Certificate' text area in the bottom panel. Callout **d** points to the 'Import' link in the top panel. Callout **e** points to the 'View' link in the top panel.
- VIEW GLOBAL ROOT CA CERTIFICATE:** This section shows a list of certificates. Callout **f** points to the 'Certificate 1:' header. Callout **g** points to the 'Mode: Simple' radio button. Callout **h** points to the list of certificates (1-6). Callout **i** points to the 'Delete' button.

The 'VIEW GLOBAL ROOT CA CERTIFICATE' section displays the following information for Certificate 1:

```

Certificate 1:
Issuer: C=US,O=American Express Company\, Inc.,OU=American Express Technologies
Validity
Not Before: Aug 14 22:01:00 1998 GMT
Not After : Aug 14 23:59:00 2006 GMT
Subject: C=US,O=American Express Company\, Inc.,OU=American Express Technologies
    
```

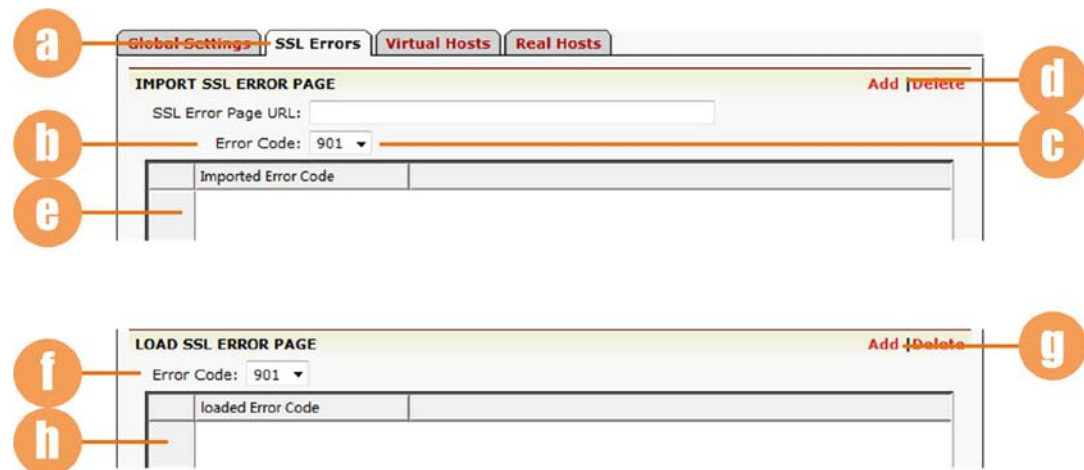
Below the certificate information is a list of certificates (1-6) and a 'Delete' button.

SSL Errors

Click on the “SSL Errors” tab [a].

First, import a customized static error page from the administrator’s remote host. You need to input the URL address of the remote host in the text box [b], from which you can obtain the static error page. Select the code for the customized error page from the selector [c], where error codes 901 to 906 are available. Click “Add” on the upper right side [d], and then the imported error code will be displayed in the display window [e].

Next, load the imported SSL customized error page into the FortiBalancer appliance system memory. Thus, when client authentication fails, this error page will be displayed at the SSL client. Select the error code for the customized error page from the selector [f], and click “Add” on the upper right side [g]. Then, the loaded error code for the error page will be displayed in the display window [h].

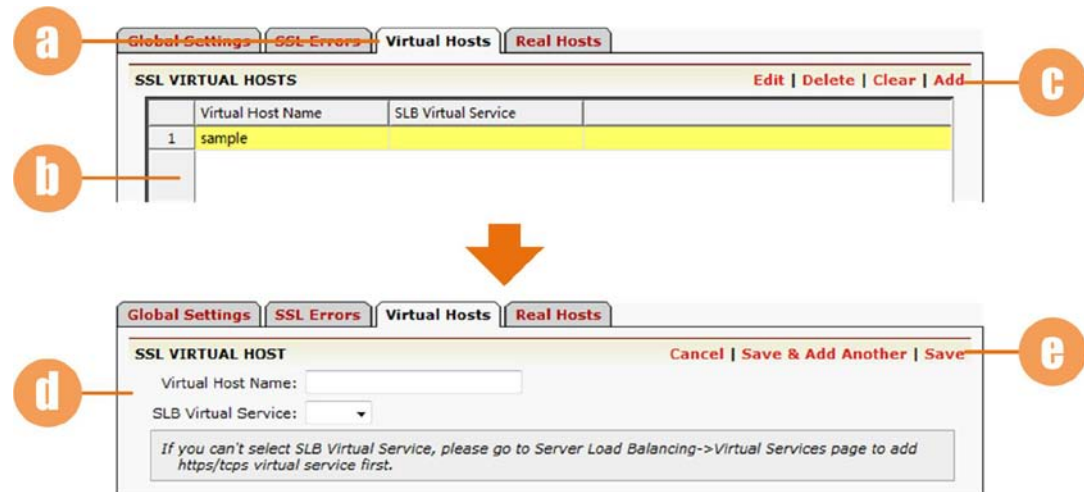


Virtual Hosts

Make certain that you have already created virtual hosts via the Virtual Services configuration.

Select the “**Virtual Hosts**” tab [a]. A list of SSL virtual hosts will be displayed in the sort ready table [b].

To add a virtual host, click on the action link “Add” [c], and supply the virtual host name and select an SLB virtual service [d], and then click on the desired action link [e]. Then, the newly added host names will be displayed in the table [b].



Virtual Hosts (Continue)

Double click on a host in the table, and the configuration window displays two tabs: “**Virtual Host CSR/Cert/Key**” and “**Virtual Host Settings**”. The “**CSR/Key**” sub tab under the “**Virtual Host CSR/Cert/Key**” tab is displayed by default [a].

You can select a virtual host from the selector [b] to complete configurations about it.

Virtual Host CSR/Cert/Key

CSR/Key

To create a new CSR/Key, supply the country code for the CSR [c], and supply the parameter fields properly [d]. Then, you can set the private key to be exportable or not (Yes/No) [e]. If you select “Yes”, you need to further set the private key password in the text boxes [f].

Then, click on the action link “Apply” [g] to create a new CSR/Key [h]. To delete the generated CSR, you can click on the action link “Remove” [i].

You can also view the SSL exportable key in the area [j].

The screenshot shows the "Virtual Host CSR/Cert/Key" configuration window. At the top, there is a "Select SSL Virtual Host:" dropdown menu with "dd" selected and a "[Back to top menu]" link. Below this is a tabbed interface with "Virtual Host CSR/Cert/Key" and "Virtual Host Settings". The "CSR/Key" sub-tab is active. The main section is titled "GENERATE A NEW CSR/KEY" and includes an "Apply" button. It contains fields for "Key Length" (1024 bit), "Generate New Key" (checked), "Country (2 letter code)", "State/Province", "City/Locality", "Organization", "Organizational Unit", "Don't use vhost name as Common Name" (unchecked), "Common Name", and "Administrator Email". There is a "Private Key Exportable" section with "No" selected and "Yes" as an option. Below this are "Private Key Password" and "Confirm Private Key Password" fields. A section titled "SSL EXPORTABLE KEY" shows a message "key is not marked exportable". Below that is an "EXISTING CSR" section with a "Remove" button and a large text area containing a base64-encoded CSR. At the bottom, another "SSL EXPORTABLE KEY" section shows the same "key is not marked exportable" message. Annotations a-j point to various elements: a points to the "CSR/Key" sub-tab, b points to the "Select SSL Virtual Host:" dropdown, c points to the "Country" field, d points to the "Organization" field, e points to the "Private Key Exportable" radio buttons, f points to the "Private Key Password" field, g points to the "Apply" button, h points to the "Remove" button, i points to the "EXISTING CSR" section, and j points to the "SSL EXPORTABLE KEY" section at the bottom.

Virtual Hosts (Continue)

Import Cert/Key

Select the “**Import Cert/Key**” tab [\[a\]](#). You can import an existing Cert/Key pair via local file, TFTP or manual input method.

To import an existing Cert/Key pair via a local file, you can select the radio button “Local File” [\[b\]](#), and specify the local file path and input the password [\[c\]](#).

To import a Cert/Key pair via TFTP, select the radio button “TFTP” [\[d\]](#), and supply the server address, file name and key password [\[e\]](#).

To manually input a Cert/Key pair, select the radio button “Manual Input” [\[f\]](#), paste your existing certificate and key into the text fields, and supply the key password [\[g\]](#).

After confirming the supplied information, click on the action link “Import” to import the Cert/Key pair [\[h\]](#).

Select SSL Virtual Host: sample [Back to top menu]

Virtual Host CSR/Cert/Key **Virtual Host Settings**

CSR/Key **Import Cert/Key** **Backup/Restore Cert/Key** **Import Client Cert/Key**

SSL KEY [Using: Local File ☒ TFTP ☐ Manual Input ☐] **Import**

Local File Path:

Key Passphrase:

SSL CERTIFICATE [Using: Local File ☒ TFTP ☐ Manual Input ☐] **Import**

Local File Path:

Key Passphrase:

Note: You should input key passphrase when the format of a certificate is pfx, otherwise, keep it empty.

INTERMEDIATE CA CERTIFICATE [Using: Local File ☒ TFTP ☐ Manual Input ☐] **Import**

Local File Path:

TRUSTED CA CERTIFICATE [Using: Local File ☒ TFTP ☐ Manual Input ☐] **Import**

Note: This is used for Verifying Client Certificates

Local File Path:

CRL CA CERTIFICATE [Using: Local File ☒ TFTP ☐ Manual Input ☐] **Import**

Local File Path:

INTERMEDIATE CA CERTIFICATE [Using: Local File ☐ TFTP ☒ Manual Input ☐] **Import**

TFTP:

File Name: sample.crt

INTERMEDIATE CA CERTIFICATE [Using: Local File ☐ TFTP ☐ Manual Input ☒] **Import**

Intermediate CA Certificate:

Virtual Hosts (Continue)

Backup/Restore Cert/Key

To backup or restore an existing Cert/Key, select the **“Backup/Restore Cert/Key”** sub tab [\[a\]](#).

To backup an existing Cert/Key, supply the file name and password in the text fields [\[b\]](#), and click on the action link “Backup” to save a backup file [\[c\]](#). Then the saved file will be displayed in the “Backup Files” list [\[d\]](#).

To restore a Cert/Key from the server, select a backup file from the list [\[d\]](#) and click on the desired action link [\[e\]](#).

To restore a Cert/Key from a local station, supply the TFTP server address, file name and password in the text fields [\[f\]](#), and click on the action link “Restore” [\[g\]](#).

The screenshot shows the 'Virtual Hosts' configuration page with the 'Backup/Restore Cert/Key' sub-tab selected. The interface includes a 'Select SSL Virtual Host' dropdown set to 'sample' and a '[Back to top menu]' link. The main content area is divided into three sections: 'BACKUP CERTIFICATE/PRIVATE KEY', 'RESTORE CERTIFICATE/PRIVATE KEY', and 'REMOTE RESTORE CERTIFICATE/PRIVATE KEY'. Callouts a through g point to specific elements: 'a' points to the 'Backup/Restore Cert/Key' sub-tab; 'b' points to the 'FileName:' and 'Password:' input fields in the backup section; 'c' points to the 'Backup' action link; 'd' points to the 'Backup Files' table; 'e' points to the 'Save | Delete | Restore' action links; 'f' points to the 'TFTP:', 'Backup FileName:', and 'Backup File Password:' input fields in the remote restore section; and 'g' points to the 'Restore' action link.

Select SSL Virtual Host: sample [Back to top menu]

Virtual Host CSR/Cert/Key Virtual Host Settings

CSR/Key Import Cert/Key Backup/Restore Cert/Key Import Client Cert/Key

BACKUP CERTIFICATE/PRIVATE KEY Backup

FileName: Password:

RESTORE CERTIFICATE/PRIVATE KEY Save | Delete | Restore

Backup Files	
1	

REMOTE RESTORE CERTIFICATE/PRIVATE KEY Restore

TFTP: Backup FileName: Backup File Password:

Virtual Hosts (Continue)

Import Client Cert/Key

Select the “**Import Client Cert/Key**” sub tab [\[a\]](#). You can import a client Cert/Key pair via local file, TFTP, HTTP or manual input method.

To import via a local file, you can select the radio button “Local File” [\[b\]](#), specify the file path and input the password [\[c\]](#).

To import a client Cert/Key pair via TFTP, select the radio button “TFTP” [\[d\]](#), and supply the TFTP address and password [\[e\]](#).

To import a client Cert/Key pair via FTP, select the radio button “FTP” [\[f\]](#), and supply the FTP address and password [\[g\]](#).

To import a client Cert/Key pair via HTTP, select the radio button “HTTP” [\[h\]](#), and supply the HTTP address and password [\[i\]](#).

To manually input a client Cert/Key pair, select the radio button “Manual Input” [\[j\]](#), paste your existing certificate and key into the text fields, and supply the key password [\[k\]](#).

After confirming the supplied information, click on the action link “Import” to import the client Cert/Key pair [\[l\]](#).

Select SSL Virtual Host: sample [Back to top menu]

Virtual Host CSR/Cert/Key **Virtual Host Settings**

CSR/Key **Import Cert/Key** **Backup/Restore Cert/Key** **Import Client Cert/Key**

SSL CLIENT KEY [Using: Local File ☒ TFTP ☐ FTP ☐ HTTP ☐ Manual Input ☐] **Import**

Local File Path:

Key Passphrase:

SSL CLIENT CERTIFICATE [Using: Local File ☒ TFTP ☐ FTP ☐ HTTP ☐ Manual Input ☐] **Import**

Local File Path:

Key Passphrase: (Only use when certificate format is pfx)

SSL CLIENT KEY [Using: Local File ☐ TFTP ☒ FTP ☐ HTTP ☐ Manual Input ☐] **Import**

TFTP URL: tftp://

Key Passphrase:

SSL CLIENT KEY [Using: Local File ☐ TFTP ☐ FTP ☒ HTTP ☐ Manual Input ☐] **Import**

FTP URL: ftp://

Key Passphrase:

SSL CLIENT KEY [Using: Local File ☐ TFTP ☐ FTP ☐ HTTP ☒ Manual Input ☐] **Import**

HTTP URL: http://

Key Passphrase:

SSL CLIENT KEY [Using: Local File ☐ TFTP ☐ FTP ☐ HTTP ☐ Manual Input ☒] **Import**

SSL Client Key:

Key Passphrase:

Virtual Hosts (Continue)

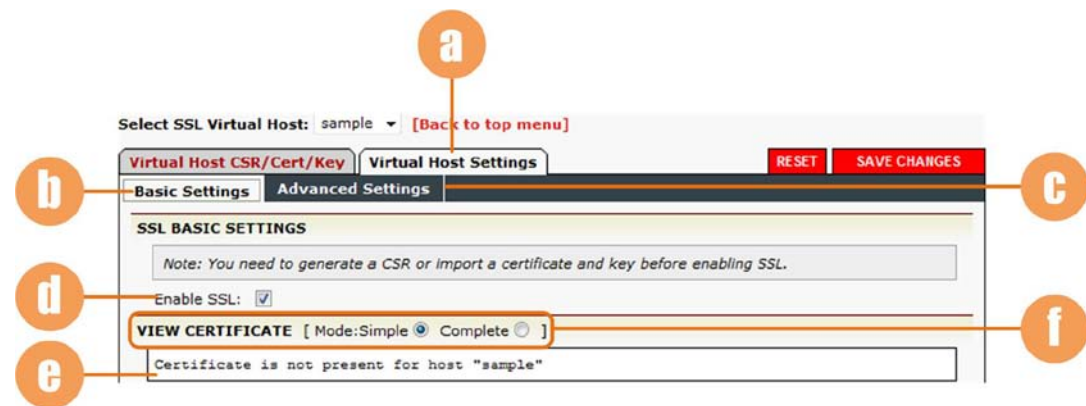
Virtual Host Settings

To execute virtual host settings, make sure that you have already generated a CSR or imported a certificate and key. Select the “**Virtual Host Settings**” tab [a], and the configuration window will display two sub tabs “**Basic Settings**” [b] and “**Advanced Settings**” [c].

Basic Settings

On this configuration page, you can enable SSL on this virtual host by selecting the check box “**Enable SSL**” [d].

You can view certificate information in the configuration window [e]. Select the display mode via the radio buttons [f]. If you choose the “**Complete**” mode, complete certificate information will be displayed.



Virtual Hosts (Continue)

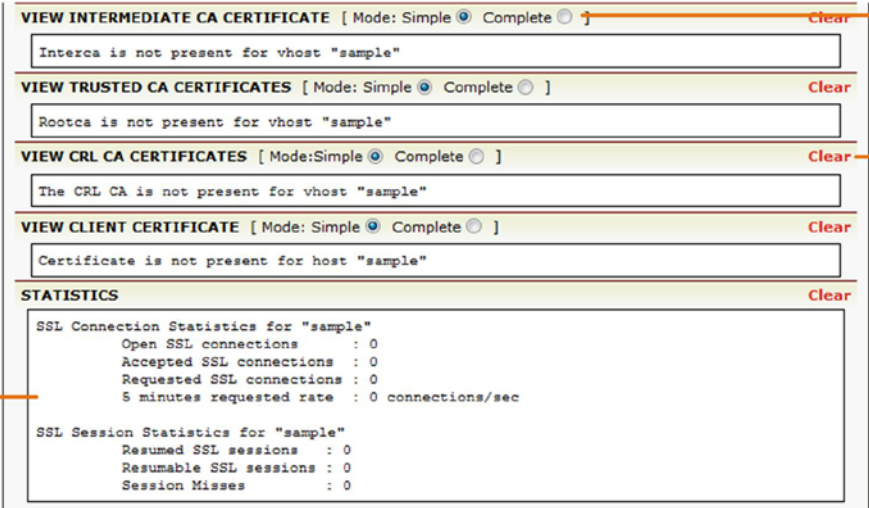
Basic Settings (Continue)

On this configuration page, you can also view intermediate CA certificate, trusted CA certificate, CRL CA certificate and client certificate information.

Select the display mode of certificate information (simple or complete) via the radio buttons [\[a\]](#).

You can click on the “Clear” action link [\[b\]](#) to remove the certificate.

You can also view SSL statistics information on this page [\[c\]](#).



The screenshot displays the 'Virtual Hosts' configuration page with the following sections and callouts:

- VIEW INTERMEDIATE CA CERTIFICATE** [Mode: Simple ☒ Complete ☐] [Clear](#) [a](#)
- Interca is not present for vhost "sample"
- VIEW TRUSTED CA CERTIFICATES** [Mode: Simple ☒ Complete ☐] [Clear](#)
- Rootca is not present for vhost "sample"
- VIEW CRL CA CERTIFICATES** [Mode: Simple ☒ Complete ☐] [Clear](#) [b](#)
- The CRL CA is not present for vhost "sample"
- VIEW CLIENT CERTIFICATE** [Mode: Simple ☒ Complete ☐] [Clear](#)
- Certificate is not present for host "sample"
- STATISTICS** [Clear](#) [c](#)
- SSL Connection Statistics for "sample"
 - Open SSL connections : 0
 - Accepted SSL connections : 0
 - Requested SSL connections : 0
 - 5 minutes requested rate : 0 connections/sec
- SSL Session Statistics for "sample"
 - Resumed SSL sessions : 0
 - Resumable SSL sessions : 0
 - Session Misses : 0

Virtual Hosts (Continue)

Advanced Settings

Click on the sub tab “**Advanced Settings**” [a].

SSL Advanced Settings: You can select proper SSL version (SSLv3 or TLSv1) [b], enable session reuse [c] or enable SSL renegotiation [d]. Then, click on the “**SAVE CHANGES**” button [e] to make your settings take effect.

Client Authentication: To enable client authentication, you can select the check box [f], and click on the “**SAVE CHANGES**” button [e]. Then, some new configuration items will appear [g] where you can: input authentication certificate subject (optional), select client authentication mode (mandatory or non-mandatory), set whether to accept certificate chain from peer, enable OCSP and input OCSP URL address, and enable CRL online check. After completing the configurations, click on “**Apply**” [h] to make them take effect. (**Note:** If OCSP is enabled, CRL online check will be disabled, and you cannot make CRL settings.)

Client Authentication-CRL Settings: After enabling client authentication, CRL settings can be configured. Click on “**Add**” [i] and a new window will appear. Supply the CRL name, the URL where to download the CRL, the interval between two downloads (in minutes) and the delay time (in minutes) [j]. Then click on “**Save**” [k], and the added settings will be displayed in the table [l].

The screenshot shows the Fortinet Virtual Host Settings page. The page has a top navigation bar with tabs: "Virtual Host CSR/Cert/Key", "Virtual Host Settings", "Basic Settings", and "Advanced Settings". The "Advanced Settings" tab is selected. The page is divided into sections: "SSL ADVANCED SETTINGS", "CLIENT AUTHENTICATION", and "CLIENT AUTHENTICATION -- CRL SETTINGS".

Annotations and their corresponding elements:

- a**: Select SSL Virtual Host: sample [Back to top menu]
- b**: SSL Versions: SSLv3: [x] TLSv1: [x]
- c**: Enable Session Reuse: [x]
- d**: Enable SSL Renegotiation: []
- e**: RESET SAVE CHANGES
- f**: Enable Client Authentication: [x]
- g**: Auth Cert Subject: (Optional)
- h**: Apply
- i**: Add
- j**: CRL Name, CRL URL, CRL Interval, CRL Delay, Download Time
- k**: Cancel | Save & Add Another | Save

The "CLIENT AUTHENTICATION -- CRL SETTINGS" section contains a table with the following columns: CRL Name, CRL URL, CRL Interval, CRL Delay, and Download Time. Below the table, there are input fields for: Virtual Host Name: sample, CRL Name: , CRL URL: , CRL Interval: 1440 (Minutes), and CRL Delay: 0 (Minutes).

Virtual Hosts (Continue)

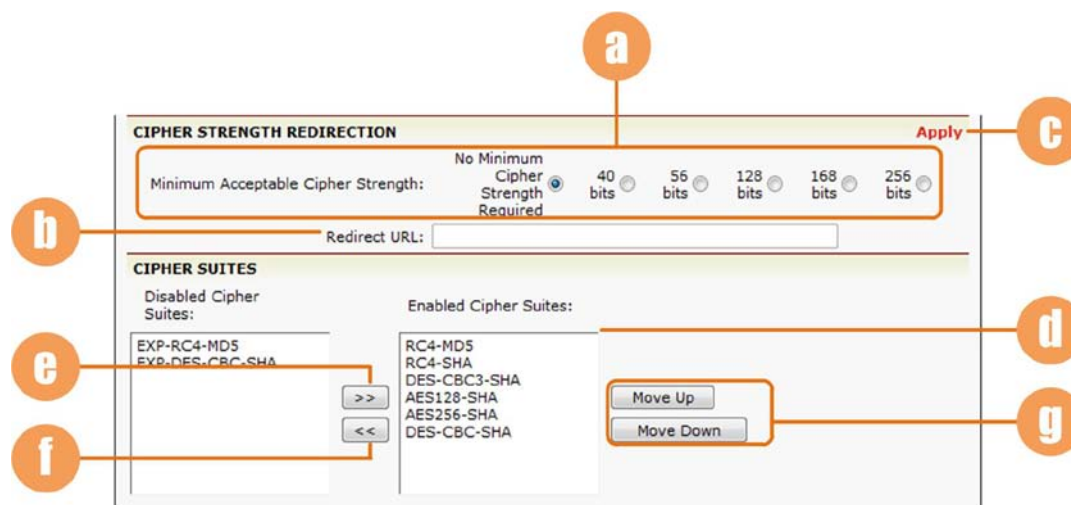
Advanced Settings (Continue)

Cipher Strength Redirection: Specify the minimum cipher strength via the radio buttons [a], and fill in the text field with redirect URL [b]. Then click on “Apply” [c] to save the changes.

Cipher Suites: In order to determine whether to enable a cipher suite or not, select the desired cipher suite from the list [d], and then click on the button to either enable it [e] or disable it [f].

You can also change the position of the cipher suites in the list by clicking on the “Move Up” or “Move Down” button [g].

Note: To modify the configurations of a virtual host, you have to make sure that the virtual host is in inactive status (unselect the “Enable SSL” check box on the Basic Settings page). That is because the WebUI will execute “stop host” first before the modification operation and “start host” after the modification operation without asking for your confirmation. This may cause unexpected risks.



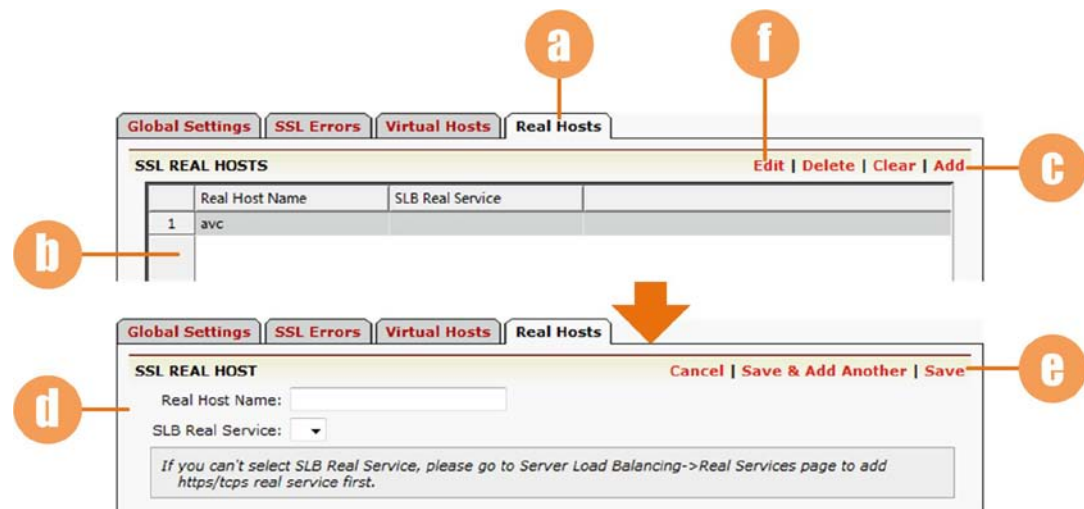
Real Hosts

To perform real host configuration, first make certain that you have already created real services via the Server Load Balance.

Select the tab “**Real Hosts**” [a] to enter the “SSL Real Hosts” configuration window, where the previously created SSL real hosts are displayed in the sort ready table [b].

To add an SSL real host, click on the action link “Add” [c], and a new configuration window will appear. Supply the real host name and specify the SLB real service [d], and then click on the “Save” action link [e].

After a real host is added successfully, it will be displayed in the table [b]. You can edit a real host by double clicking on it or click a real host in the table and select the action link “Edit” [f]. Then, a new configuration window will appear.



Real Hosts (Continue)

Double click on the real host name in the list box, and the configuration window will display two tabs “Real Host Cert/Key” and “Real Host Settings”. By default, the sub tab “Import Cert/Key” under the “Real Host Cert/Key” tab is displayed [a].

You can switch among the created real hosts by selecting from the selector [b].

Import Cert/Key

You can import a Cert/Key pair via local file, TFTP or manual input method.

To import a Cert/Key pair via a local file, select the radio button “Local File” [c], and supply the file path and password [d].

To import via TFTP, select the radio button “TFTP” [e], and supply the server address and password in the text fields [f].

To manually input a Cert/Key pair, select the radio button “Manual Input” [g], and paste your SSL key and CA certificate into the blanks and supply the key password [h].

After confirming the information input, click on the action link “Import” [i].

Select SSL Real Host: avc [Back to top menu]

Real Host Cert/Key **Real Host Settings**

Import Cert/Key **Backup/Restore Cert/Key**

SSL KEY [Using: Local File ☒ TFTP ☐ Manual Input ☐] **Import**

Local File Path: Browse...

Key Passphrase:

SSL CERTIFICATE [Using: Local File ☒ TFTP ☐ Manual Input ☐] **Import**

Local File Path: Browse...

Key Passphrase:

Note: You should input key passphrase when the format of a certificate is pfx, otherwise, keep it empty.

SSL KEY [Using: Local File ☐ TFTP ☒ Manual Input ☐] **Import**

TFTP:

File Name: avc.key

Key Passphrase:

SSL KEY [Using: Local File ☐ TFTP ☐ Manual Input ☒] **Import**

SSL Key:

Key Passphrase:

Real Hosts (Continue)

Backup/Restore Cert/Key

To backup or restore an existing Cert/Key pair, select the sub tab “Backup/Restore Cert/Key” [\[a\]](#).

To backup an existing certificate or private key, supply the file name and password [\[b\]](#), and then click on the action link “Backup” [\[c\]](#). The saved files will be displayed in the “Backup Files” list [\[d\]](#).

To restore from local backup files, select an entry from the backup files list [\[d\]](#), and click on the desired action link [\[e\]](#).

To restore via remote server, supply the TFTP server address, backup filename and password [\[f\]](#), and click on the action link “Restore” [\[g\]](#).

Select SSL Real Host: avc [\[Back to top menu\]](#)

Real Host Cert/Key **Real Host Settings**

Import Cert/Key **Backup/Restore Cert/Key**

BACKUP CERTIFICATE/PRIVATE KEY [Backup](#)

FileName:

Password:

RESTORE CERTIFICATE/PRIVATE KEY [Save](#) | [Delete](#) | [Restore](#)

Backup Files	
1	

REMOTE RESTORE CERTIFICATE/PRIVATE KEY [Restore](#)

TFTP:

Backup FileName:

Backup File Password:

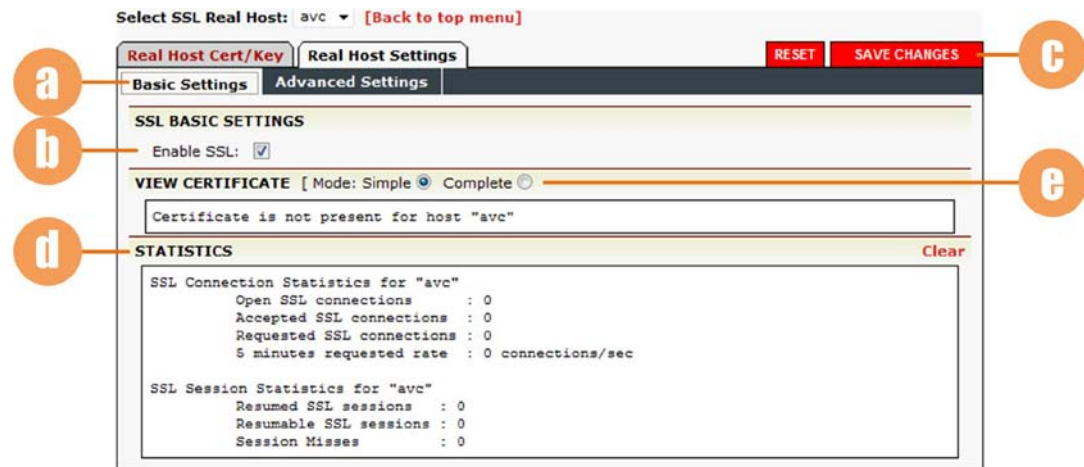
Real Hosts (Continue)

Basic Settings:

Make certain you have selected the “**Real Host Settings**” tab, and the “**Basic Settings**” page is displayed by default [a].

Select the check box to enable SSL on this real host [b]. Then, click on the “**SAVE CHANGES**” button when it appears to save the configuration [c].

You can also view the certificate and statistics [d]. Select the display mode via the radio buttons [e]. If the display mode is set to “**Complete**”, all the certificate information will be displayed on the page.



Real Hosts (Continue)

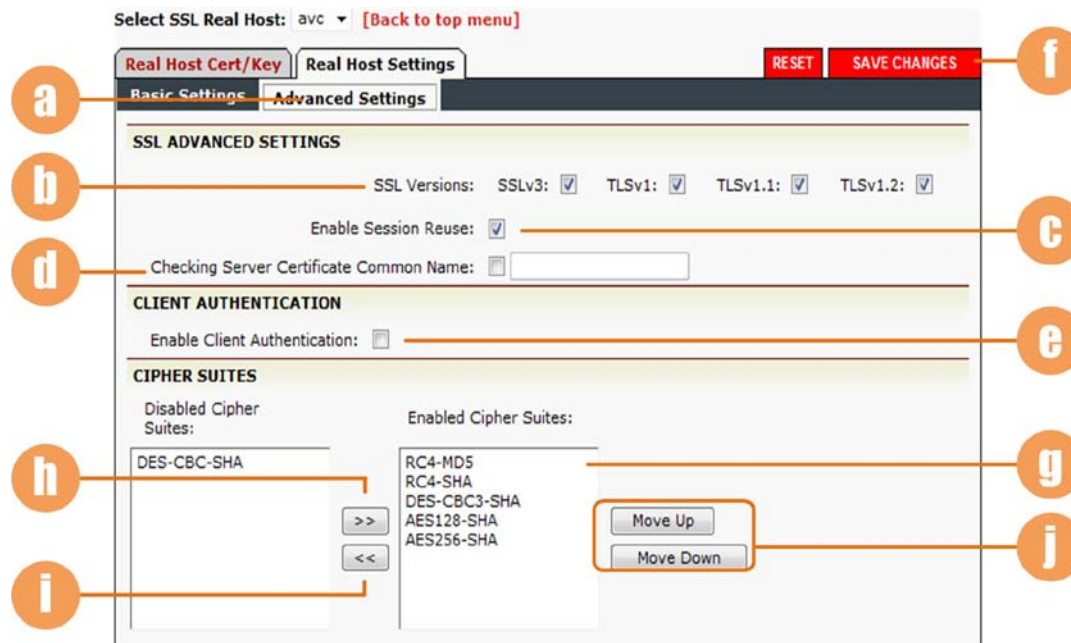
Advanced Settings

Select the sub tab “**Advanced Settings**” [a]. Specify the SSL version (SSLv3 or TLSv1) via the check boxes [b]. Enable SSL session reuse via the check box [c]. To enable the function of checking server certificate common name, you can first check the box [d] and then input the common name in the text box thereafter. You can also enable the client authentication feature by selecting the check box [e].

After finishing these settings, you can click on the “SAVE CHANGES” button to save your configuration [f].

In order to determine whether to enable a cipher suite or not, select the desired cipher suite from the list [g], and click on the button to either enable it [h] or disable it [i].

You can also change the position of the cipher suites by clicking on the “Move Up” or “Move Down” button [j].

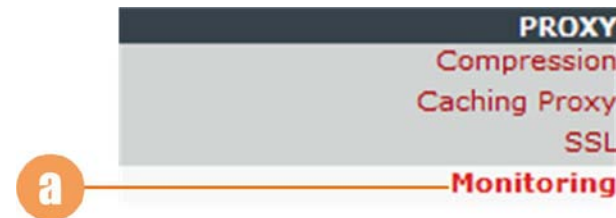


Note: To modify the configurations of a real host, you have to make sure that the real host is in inactive status (unselect the “Enable SSL” check box on the Basic Settings page). That is because the WebUI will execute “stop host” first before the modification operation and “start host” after the modification operation without asking for your confirmation. This may cause unexpected risks.

Monitoring

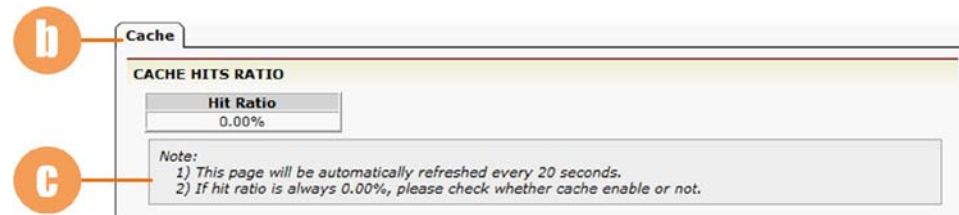
The FortiBalancer appliance allows you to monitor the cache hits ratio in real time.

Make certain you are in the **Config Mode** and select the feature link “**Monitoring**” from the sidebar [\[a\]](#).



Cache

Select the “**Cache**” tab [\[b\]](#) and the window will display the realtime hit ratio in the box [\[c\]](#). The page is automatically refreshed every twenty seconds.



Advanced Load Balance

Link Load Balancing (LLB) allows TCP/IP network traffic to be balanced through up to 128 upstream Internet Service Providers (ISPs). Load balancing can be performed on egress to the Internet (outbound LLB) or on ingress from the Internet (inbound LLB).

Make certain you are in Config mode, and select the **Link Load Balance** feature link from the sidebar [a]. The window will present you four tabs [b].

NAT **IPv6** **IP Region** **IP Pool** **Port Forwarding**

Addresses **Routing** **NATPT**

IPv6 NATPT SETTINGS Set

Enable NATPT: ☐

Prefix:

NATPT IPv6 TO IPv4 SETTINGS Set | Delete

IPv4 Address:

Start Port: (1025 - 65535)

End Port: (1025 - 65535)

NATPT IPv4 TO IPv6 SETTINGS Add

IPv4 Address:

IPv6 Address:

IPv4 Address	IPv6 Address

NATPT TRANSLATIONS

Protocol	Local Address(src)	Local Address(dst)	Remote Ac

InBound Settings

Select the “InBound Settings” tab [a]. First, set the DNS load balance method via the selector [b]. Click on the “SAVE CHANGES” button [c] when it appears to save your setting.

To create a DNS entry, click on the “Add” action link [d] and then supply the host name, host IP, port number, weight value and link route in the text fields [e] and click on the “Save” action link [f]. The newly created DNS entry will be displayed in the sort ready table [g].

To change the DNS TTL value, select a desired host in the table [h] and click on “Modify” [i]. Input the new TTL value in the new configuration page [j], and click on “Save” [k] to make your change take effect.

The screenshot shows the 'InBound Settings' tab in the Fortinet Advanced Load Balance configuration interface. The interface includes tabs for 'InBound Settings', 'OutBound Settings', 'Statistics', and 'Report'. There are 'RESET' and 'SAVE CHANGES' buttons at the top right. The 'DNS LOAD BALANCE' section shows the 'Method' set to 'Weighted Round Robin'. Below this is a 'DNS ENTRIES' table with columns for Host Name, IP, Port, Weight, and an action column with 'Delete' and 'Add' links. An 'ADD DNS ENTRY' form is shown below the table, with fields for Host Name, IP, Port, Weight, and Link Route. A 'TIME TO LIVE' table is also present, with columns for Host Name, TTL, and an action column with a 'Modify' link. A 'MODIFY DNS TTL' form is shown below the table, with fields for Host Name and TTL. Arrows and callouts (a-k) indicate the sequence of steps: (a) InBound Settings tab, (b) Method selector, (c) SAVE CHANGES button, (d) Add link, (e) ADD DNS ENTRY form fields, (f) Save link, (g) DNS ENTRIES table, (h) TIME TO LIVE table, (i) Modify link, (j) MODIFY DNS TTL form fields, and (k) Save link.

DNS ENTRIES Table:

	Host Name	IP	Port	Weight	
1	www.a.com	10.10.2.2	0	1	
2	www.b.com	10.10.2.3	0	1	
3	www.c.com	10.10.2.4	0	1	

TIME TO LIVE Table:

	Host Name	TTL	
1	www.a.com	60	
2	www.b.com	60	
3	www.c.com	60	

OutBound Settings

Click on the tab “**OutBound Settings**” [a]. The configuration window presents a new configuration page.

Set the Link Load Balance method via the selector [b]. If “Dynamic Detecting” method is selected, you need to set time interval and connection count for triggering DD refresh [c]. Use the check box [d] to enable the LLB health check. Once any change is made, the “RESET” and “SAVE CHANGES” buttons will appear. Remember to save any change made by clicking on the “SAVE CHANGES” button [e].

Select the action link “Add” [f]. A new configuration page is displayed.

Specify the link name, gateway IP, weight value for the link, set the health check source IP and bandwidth threshold [g]. At last, remember to click on the action link “Save” [h] to complete the configuration. The newly added LLB link route will be displayed in the table [i].

The screenshot shows the 'OutBound Settings' configuration page. It includes tabs for 'InBound Settings', 'OutBound Settings', 'Statistics', and 'Report'. At the top right are 'RESET' and 'SAVE CHANGES' buttons. The main section is titled 'LLB LINK GLOBAL SETTINGS' and contains a 'Method' dropdown (set to 'Round Robin'), an 'Enable Link Health Check' checkbox (checked), and a table titled 'LLB LINK ROUTE'. The table has columns for Link Name, GateWay IP, Health Check IP, Interval, Weight, Enable, and Health Check Source IP. A modal window titled 'ADD LINK ROUTE' is open, showing fields for Link Name, GateWay IP, Health Check IP, Interval (10 seconds), Weight (1), and Health Check Source IP. The modal also has a 'DD REFRESH TRIGGER' section with 'Time Interval' (300 seconds) and 'Connection Count' (1000). Callouts a-i point to various elements: a (OutBound Settings tab), b (Method dropdown), c (DD REFRESH TRIGGER section), d (Enable Link Health Check checkbox), e (SAVE CHANGES button), f (Add button), g (Link Name field), h (Save button), and i (LLB LINK ROUTE table).

OutBound Settings (Continue)

In the LLB link list, you can enable a link via the check box [a]. Then, remember to click on “SAVE CHANGES” [b] to save your configuration.

To modify the settings of a link, double click on it in the table [c], or select it and click on the action link “Edit” [d]. A new configuration page will be displayed.

Enable or disable the link via the check box [e]. Then, click on “Save” [f] to make your setting take effect.

To add an LLB link health checker, click on the action link “Add” [g]. A new configuration page will appear.

Select the health check type, and supply the required information [h]. The parameter fields may vary with different health check types. After finishing the configuration, click on the action link “Save” [i], and information about the health checker will be displayed in the sort ready table [j].

The screenshot shows the Fortinet Advanced Load Balance configuration interface. It includes a table for LLB LINK ROUTE, a form for editing a link, and a table for LINK HEALTH CHECKER. Annotations a-j point to specific UI elements:

- a**: RESET button
- b**: SAVE CHANGES button
- c**: LLB LINK ROUTE table
- d**: Edit | Delete | Add action links
- e**: Enable checkbox
- f**: Cancel | Save buttons
- g**: Delete | Add action links
- h**: ADD LINK HEALTH CHECKER form
- i**: Cancel | Save & Add Another | Save buttons
- j**: LINK HEALTH CHECKER table

LLB LINK ROUTE Table:

	Link Name	GateWay IP	Weight	Source IP	Bandwidth Threshold	Enable
1	link1	10.3.10.1	1	0.0.0.0	10Mbps	☒
2						☐

LLB LINK ROUTE Form:

Link Name: link1
 GateWay IP: 10.3.10.1
 Weight: 1
 Source IP: 0.0.0.0
 Bandwidth Threshold: 10Mbps
 Enable: ☒

LINK HEALTH CHECKER Table:

	Type	Host	Port	Domain Name	Interval	Timeout	Continuous Up	Continuous Down
1	icmp	10.3.121.52			10	5	3	3
2	tcp	10.3.121.51	333		104	5	3	3
3	dns	10.3.121.54		www.xyz.com	10	5	3	3

ADD LINK HEALTH CHECKER Form:

Link Name: link1
 Type: icmp
 Host:
 Interval: 10 Seconds
 Timeout: 5 Seconds
 Continuous Up: 3
 Continuous Down: 3

Statistics

Make certain you are in **Config mode** and have selected the “Statistics” tab [\[a\]](#).

Use the check box [\[b\]](#) to enable the function of displaying the LLB statistics. Once any change is made, the “RESET” and “SAVE CHANGES” buttons appear. Remember to save any change made by clicking on the button [\[c\]](#).

Once the “Enable LLB Statistics” function is enabled, you can view the statistics about all the links in the table [\[d\]](#).

LLB STATISTICS SETTINGS

Enable LLB Statistics: ☒

LLB LINK STATISTICS Clear

Link Name: all

Link "link1":

status statistics:		Interval	Weight	Resp_time	Status	Down	Up_time
Gateway	Destination	10	1	0.000ms	Down	1	00:00:30
10.3.121.1	---	---	---	---	Down	1	00:00:30
Basic HC:	10.3.121.99	---	---	---	Down	1	00:00:30
Extra HC:	10.3.70.59	---	---	---	Down	1	00:00:30

Bandwidth statistics:

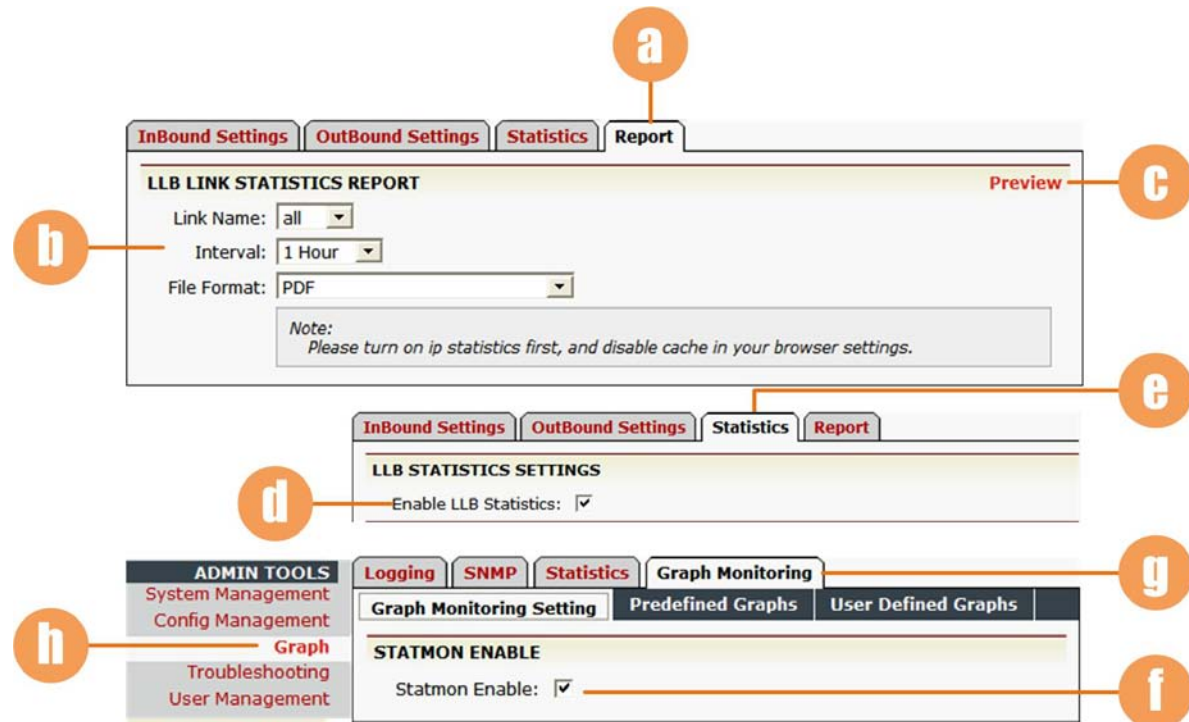
Bandwidth (bit/sec):	Min.	5min.	Hour	Day
10.3.121.1 Avg.:	128.000 (bps)	128.000 (bps)	128.000 (bps)	128.000 (bps)
10.3.121.1 Peak:	128.000 (bps)	128.000 (bps)	128.000 (bps)	128.000 (bps)

Report

Select the “**Report**” tab [a]. You can view the report under the Enable mode.

Specify the link name, interval and format of the report via the selectors [b] and click on the action link “Preview” [c]. Then, you will be presented with an LLB Link Statistics Report in the format you have specified.

Note that the **Report** page is available only after you have selected the “Enable LLB Statistics” check box [d] on the **Statistics** page [e], and also have enabled the statmon function via the check box [f] on the **Graph Monitoring Setting** page under the “**Graph Monitoring**” tab [g] (select the Graph feature link under the **Admin Tools** feature group [h]).



Global Load Balance

Fortinet GSLB (SDNS) solution transforms the FortiBalancer appliance into a complementary DNS server which is able to resolve a set of defined domain names based on the configured load balancing methods. SDNS runs on each FortiBalancer appliance and is able to resolve a given domain name (A Record) as an authoritative DNS server. When DNS queries (typically forwarded by Corporate DNS Server or ISP DNS Server) for the domain name received, the SDNS function will resolve the domain name with IP addresses selected from its Domain Name and IP Service Database with load balancing method configured.

Make certain you are in Config mode, and have selected the feature link **Global Load Balance** from the sidebar [a]. Then, nine tabs [b] will be displayed on the configuration page. The default page is **General Settings**.

The screenshot displays the FortiBalancer configuration interface. On the left sidebar, the 'Config' mode is selected. The 'ADVANCED LOAD BALANCE' section is expanded, and 'Global Load Balance' is selected, indicated by an orange circle 'a'. The main configuration area shows the 'General Settings' tab selected, indicated by an orange circle 'b'. The 'General Settings' tab contains the following options:

- SDNS Status:
- SDNS Statistics: ☒
- SDNS Local Statistics: ☒
- SDNS Report Interval:
- SDNS Heart Beat Interval:
- SDNS persistent timeout:
- Recursion: ☐

Below the 'General Settings' tab is the 'SDNS MEMBER SETTINGS' section, which includes a table with the following data:

	Name	Type	IP Address	Port	Max Connections	Status
1	sdns1	all	172.16.63.2	5888	1000	DOWN
2	sdns2	proxy	172.16.63.3	5888	1000	DOWN

At the top right of the 'SDNS MEMBER SETTINGS' section, there are links for 'Delete Member Entry' and 'Add Member Entry'.

General Settings

Select the **General Settings** tab [a]. First, turn on or turn off the SDNS function via the selector [b]; to turn on the function, you need to further specify checking (on check) or not checking (on no check) virtual hosts' health status.

Next, you can make some basic SDNS settings [c]: enable or disable the SDNS statistics and local DNS statistics functions, specify how often HTTP proxy cache servers should report their local status information, specify how long the FortiBalancer appliance will wait to send heartbeat messages to all other members in an SDNS network, specify the SDNS persistent timeout value, and enable or disable the SDNS recursive query. Then, click on the "SAVE CHANGES" button [d] to save your settings.

To add an SDNS member, click on the action link "Add Member Entry" [e]. In the new configuration page, specify the name, type, IP address and port number (defaults to 5888) of the SDNS host [f], and click on "Save" [g]. The newly created SDNS host will be displayed in the sort ready table [h].

You can also change the SDNS members' type or set them as local DNS member in the sort ready table. Remember to click on "SAVE CHANGES" [d] to save your change.

The screenshot shows the FortiBalancer SDNS configuration interface. The top navigation bar includes tabs: General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA, Statistics, Report, RESET, and SAVE CHANGES. The 'General Settings' tab is selected (callout a). Below the tabs, the 'GENERAL SETTINGS' section contains:

- SDNS Status: on check (callout b)
- SDNS Statistics: ☒
- SDNS Local Statistics: ☒
- SDNS Report Interval: 30 (callout c)
- SDNS Heart Beat Interval: 2
- SDNS persistent timeout: 3600
- Recursion: ☐

 The 'SDNS MEMBER SETTINGS' section features a table with columns: Name, Type, IP Address, Port, Max Connections, Status, and Local Member. It includes 'Delete Member Entry' and 'Add Member Entry' links (callout e). The table contains two entries:

	Name	Type	IP Address	Port	Max Connections	Status	Local Member
1	sdns1	all	172.16.63.2	5888	1000	DOWN	☐
2	sdns2	proxy	172.16.63.3	5888	1000	DOWN	☐

 (callout h)

 Below the table is the 'ADD MEMBER ENTRY' form (callout f) with fields for Name, Type (set to proxy), IP Address, and Port (5888). At the bottom right of this form are buttons: Cancel, Save & Add Another, and Save (callout g).

Records

Select the “**Records**” tab [a]. The configuration page will display five sub-tabs. The default page is A [b].

A

On this page, all the existing DNS A records in the system are displayed in the sort ready table [c]. Select a host via the selector [d], and the table will only display the A records about the selected host. To delete a record, simply select it in the table and click on the “Delete” action link [e].

To add a new A record, supply the domain name, IP address, port number, weight value and link route in the text fields [f], and click on the “Save” action link [g]. The newly created A record will be displayed in the table [c].

In the sort ready table [h], all the existing real servers and virtual servers in the system are displayed. You can use their IP addresses as the IP address of newly added A records. To do this, simply input the domain name, select one or more real/virtual server in the table [h], input the port and weight, and click on “Save”. The newly created A record(s) will be displayed in the table [c].

Records (Continue)

Cname

Select the sub-tab “Cname” [a]. You can add new CNAME records for a domain name. Supply the domain name and alias name in the text fields [b] and click on the action link “Add” [c]. The newly added CNAME records will be displayed in the sort ready table [d].

To delete an entry in the table, simply select the entry and click on the “Delete” action link [e].

The screenshot shows the 'SDNS CNAME SETTINGS' interface. At the top, there are tabs: 'A', 'Cname' (selected), 'Others', 'IPv6', and 'SNMP IP'. Below the tabs, there are two text input fields: 'Domain Name:' and 'Alias:'. To the right of these fields are two action links: 'Delete' and 'Add'. Below the input fields is a table with two columns: 'Domain Name' and 'Alias'. The table contains two entries: 'domain1' with alias 'alias1' and 'domain2' with alias 'alias2'. Annotations a-e point to specific elements: 'a' points to the 'Cname' tab, 'b' points to the 'Domain Name' and 'Alias' input fields, 'c' points to the 'Add' link, 'd' points to the table, and 'e' points to the 'Delete' link.

	Domain Name	Alias
1	domain1	alias1
2	domain2	alias2

Records (Continue)

Others

Select the sub-tab “Others” [a].

You can reboot the local DNS function by clicking on the “Restart” button [b].

Supply the path and name of the zone file in the text fields [c] and click on the action link “Import” [d]. Then, the name of the imported zone file will be displayed in the list box [e]. Multiple zone files can be imported.

To view the contents of a file, double click on the file in the list, or select it and click on the action link “View” [f]. The file contents will be displayed in a new page. To save a zone file, simply click on the action link “Save” [g].

Specify the path of the config file in the text field [h] and click on the action link “Import” [i]. The contents of the config file will be displayed in the box [j]. You can save the file by clicking on the action link “Save” [k].

IPv6

Select the sub-tab “IPv6” [l]. You can add a new IPv6 record for a domain name. Supply the domain name and IPv6 address in the text fields [m] and click on the action link “Add” [n]. The newly added record will be displayed in the sort ready table [o].

The screenshot shows the Fortinet Advanced Load Balance configuration interface. The top navigation bar includes tabs for General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA, Statistics, and Report. The 'Records' tab is active, and the 'Others' sub-tab is selected. The interface is divided into several sections:

- LOCALDNS RESTART**: Contains a 'LocalDNS Restart' button (b).
- ZONE FILE**: Contains text fields for 'Zone File Path' (c) and 'Zone Name' (c), and an 'Import' button (d).
- ZONE FILE LIST**: A table listing imported zone files. The first entry is '1 sample.rev' (e). Action links 'Save' (g), 'Delete', and 'View' (f) are present for each entry.
- CONF FILE**: Contains a 'Conf File Path' text field (h) and an 'Import' button (i).
- VIEW CONF FILE INFORMATION**: Displays the contents of the selected config file (j). A 'Save' button (k) is located at the bottom right.
- SDNS AAAA SETTINGS**: Contains text fields for 'Domain Name' (m) and 'IPv6 Address' (m), and an 'Add' button (n).
- IPv6 RECORDS**: A table listing IPv6 records. The first entry is '1 www.fortipv6.com 2001:db8:85a3:8d3:1319:8a2e:370:7344' (o).

Callouts a through o are placed around the interface to indicate the location of specific elements mentioned in the text.

Records (Continue)

SNMP IP

Select the sub-tab “SNMP IP” [a].

To create an SNMP service group, you can supply the group name in the text field [b] and click on the action link “Add” [c]. The newly added group information will be displayed in the sort ready table [d].

You can further add members for the SNMP group. Select a group via the selector, and then specify the service type and OID [e], and click on the action link “Add” [f]. The group member information will be displayed in the sort ready table [g].

You can set the SNMP check interval (in seconds) in the text field [h] and click on “Set” to save your setting [i].

Then, you can configure the IP address of the created SNMP group. Supply the IP address, select the group name and set the SNMP community and port number [j]. Then, click on the action link “Add” [k]. The newly created SNMP IP information will be displayed in the sort ready table [l].

General Settings **Records** **Topology** **Methods** **Bandwidth** **DPS** **IANA** **Statistics** **Report**

A **Cname** **Others** **IPv6** **SNMP IP**

SERVICE GROUP Add | Delete

Group Name:

	Group Name
1	group1
2	group2

GROUP MEMBER Add | Delete

Group Name:

Service Type:

OID:

	Service Type	OID

SNMP CHECK INTERVAL Set

SNMP Check Interval: Seconds

SNMP IP Add | Delete | Clear

IP Address:

Group Name:

SNMP Community:

SNMP Port:

	IP Address	Group Name	SNMP Community	SNMP Port
1	172.16.63.4	group1	aaa	161
2	172.16.63.5	group1	bbb	161

Topology

Select the “**Topology**” tab [a]. The configuration page will display five sub-tabs. The default page is Site [b].

Site

On the “**Site**” page, all sites previously configured are displayed in the sort ready table [c]. To add a new site, click on the action link “Add Site Entry” [d], supply the site name and weight [e] in the new configuration page and click on “Save” [f]. Then the newly created site will be displayed in the sort ready table [c].

You can select a desired site via the radio button to view the members of the selected site [g]. To edit the site members, click on the action link “Edit Members of the Site” [h]. Select the members for the site via the check boxes [i], and click on the “SAVE CHANGES” button [j] when it appears to make your change take effect.

General Settings | **Records** | **Topology** | **Methods** | **Bandwidth** | **DPS** | **IANA** | **Statistics** | **Report**

Site | **Region** | **Proximity** | **Over Flow Chain** | **DR Group**

SDNS SITE SETTINGS Delete Site Entry | Add Site Entry

	Site	Weight	Members	View
1	beijing	1	2	☐
2	tianjin	2	0	☐

ADD SITE ENTRY Cancel | Save & Add Another | Save

Site:
Weight:

MEMBERS OF THE SELECTED VIEW Delete Member | Edit Members of the Site

	Name	IP Address	Status
1	sdns1	172.16.63.2	all
2	sdns2	172.16.63.3	proxy

SDNS SITE'S LIST Cancel

Name	IP Address	Status	Is Site Member
sdns1	172.16.63.2	all	☒
sdns2	172.16.63.3	proxy	☒

Topology (Continue)

Region

Select the sub-tab “**Region**” [a].

On the “Region” page, all regions previously configured are displayed in the sort ready table [b]. To add a new region, click on the action link “Add Region” [c], supply the region name and weight [d] in the new configuration page and click on “Save” [e]. Then the newly created region will be displayed in the sort ready table [b].

You can select a desired region via the radio button to view its child regions [f]. To add a new child region for the selected region, click on the action link “Add Region Division” [g], and select a division region via the selector [h]. Then click on the “Save” action link [i] to make your setting take effect.

The screenshot shows the Fortinet SDNS configuration interface. The top navigation bar includes tabs for General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA, Statistics, and Report. The 'Region' sub-tab is selected. The main content area is titled 'SDNS REGION SETTINGS' and includes a table of existing regions, an 'Add Region' form, and a 'Divisions of the Selected View' section.

Annotations:

- a:** Points to the 'Region' sub-tab in the navigation bar.
- b:** Points to the 'SDNS REGION SETTINGS' table.
- c:** Points to the 'Add Region' link.
- d:** Points to the 'Name' and 'Weight' input fields in the 'ADD REGION' form.
- e:** Points to the 'Save' link in the 'ADD REGION' form.
- f:** Points to the radio button in the 'View' column of the region table.
- g:** Points to the 'Add Region Division' link.
- h:** Points to the 'Select a Division Region' dropdown in the 'ADD REGION DIVISION' form.
- i:** Points to the 'Save' link in the 'ADD REGION DIVISION' form.

SDNS REGION SETTINGS Table:

	Name	ID	Band Limit(Mbytes/S)	Weight	Divisions	View
1	Asia	3		1	1	☒
2	Euro	4		2	0	☐

ADD REGION Form:

Name:
 Weight:

Cancel | Save & Add Another | Save

DIVISIONS OF THE SELECTED VIEW Table:

Parent:	Children
1	beijing

ADD REGION DIVISION Form:

Select a Division Region:

Cancel | Save & Add Another | Save

Topology (Continue)

Proximity

Select the sub-tab “**Proximity**” [a].

You can set the distance between two sites. First, specify two sites via the selectors respectively [b] and input the distance between the two sites [c]. Click on the action link “Add Site Distance” [d]. The new configuration will be displayed in the sort ready table [e].

Still on this configuration page, click on the action link “Add Proximity Rule” [f]. The window will display a new configuration page.

Input the IP address, mask and weight in the text fields [g], select the location type via radio buttons [h] and set the site via the pull down menu [i]. Then, click on “Save” [j]. The newly created proximity rule will be displayed in the sort ready table [k].

The IP region information will be shown in the “IP Region Proximity” table [l]. Clicking on the action link “IP Region Table” and “IP Region Route” [m] will direct you to the related configuration pages..

The screenshot shows the Fortinet Proximity configuration page. The top navigation bar includes tabs for General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA, Statistics, and Report. The 'Proximity' sub-tab is selected. The page is divided into two main sections: SITE DISTANCE and PROXIMITY RULES.

SITE DISTANCE section:

- a**: General Settings tab
- b**: Site 1 selector (dropdown menu)
- c**: Distance input field
- d**: Add Site Distance action link
- e**: Table showing site distances

	Site 1	Site 2	Distance
...	beijing	beijing	
1	beijing	tianjin	1
2	tianjin	shanghai	2

PROXIMITY RULES section:

- f**: Add Proximity Rule action link
- g**: IP Address input field
- h**: IP Mask input field
- i**: Weight input field
- j**: Save button
- k**: Table showing proximity rules

	IP Address	IP Mask	Site	Weight
1	10.3.121.55	255.255.255.255	beijing	10
2	10.3.121.56	255.255.255.255	tianjin	20

ADD PROXIMITY RULE dialog box:

- g**: IP Address input field
- h**: IP Mask input field
- i**: Weight input field
- j**: Save button
- k**: Select Location Type (Site/Region radio buttons)
- l**: Site selector (dropdown menu)

IP REGION PROXIMITY table:

- m**: IP Region Table and IP Region Route action links

	Name	Site/Region	Priority

Topology (Continue)

Over Flow Chain

Select the sub-tab “Over Flow Chain” [a].

On this page, all overflow chains previously configured are displayed in the sort ready table [b]. To add a new chain, click on the action link “Add Overflow Chain” [c], supply the chain name [d] in the new configuration page and click on “Save” [e]. Then the newly created chain will be displayed in the sort ready table [b].

You can select a desired chain via the radio button to view the members of the chain [f]. To edit the chain members, click on the action link “Edit Members of the Chain” [g]. Select the members for the chain via the check boxes [h], and click on the “SAVE CHANGES” button [i] when it appears to make your change take effect.

OVERFLOW CHAINS Delete Overflow Chain | Add Overflow Chain

	Chain Name	View Members
1	chain1	☒
2	chain2	☐
3	chain3	☐

ADD OVERFLOW CHAIN Cancel | Save & Add Another | Save

Chain Name:

MEMBERS OF THE CHAIN Delete Member | Edit Members of the Chain

	Name	IP Address	Status
1	sdns2	172.16.63.3	DOWN
2	sdns1	172.16.63.2	DOWN

SDNS CHAIN'S LIST Cancel

Name	IP Address	Status	Is Chain Member
sdns1	172.16.63.2	all	☒
sdns2	172.16.63.3	proxy	☒

Topology (Continue)

DR Group

Select the sub-tab “DR Group” [a].

Enter the DR (disaster recovery) group name and the domain name that requires disaster recovery in the text fields [b], and click on the action link “Add DrGroup” [c]. The newly added group information will be displayed in the sort ready table [d].

In the table, you can switch on/off a DR group via the check box [e]. Remember to click on the “SAVE CHANGES” button [f] when it appears to save your change.

Select a desired DR group via the radio button [g], and you can see the list of the sites in the group [h]. You can further add these sites into a primary DR group or a standby DR group. To do this, select “Primary” or “Standby” via the selector [i], and specify the sites to be added into the group via the check boxes [j]. Then, click on the “Save Group Site Settings” action link [k] to save your changes.

You can disable the primary group or standby group via the check boxes [l].

The screenshot shows the Fortinet SDNS configuration interface for DR Groups. The top navigation bar includes tabs for General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA, Statistics, and Report. The 'DR Group' sub-tab is selected. The interface is divided into two main sections: 'SDNS DRGROUP SETTINGS' and 'SDNS DRGROUP SITE SETTINGS'.

SDNS DRGROUP SETTINGS:

- Group Name:** [b] (Text input field)
- Domain Name:** [b] (Text input field)
- Buttons:** [c] Delete DrGroup, [c] Add DrGroup
- Table:** [d] (Table with columns: Group Name, Domain Name, Primary Status, Standby Status, Switch On, View Sites)
- Table Data:**

	Group Name	Domain Name	Primary Status	Standby Status	Switch On	View Sites
1	drgroup1	www.drg1.com	Inactive	Inactive	☐	☒
2	drgroup2	www.drg2.com	Inactive	Inactive	☐	☐
- Buttons:** [f] RESET, [f] SAVE CHANGES

SDNS DRGROUP SITE SETTINGS:

- Buttons:** [k] Reset Group Site Settings, [k] Save Group Site Settings
- Form:**
 - Disable Primary Group:** [l] (Check box)
 - Disable Standby Group:** [l] (Check box)
 - Select Group/Site View:** [i] (Dropdown menu, currently set to Primary)
- Table:** [h] (Table with columns: Site, To Current Group)
- Table Data:**

	Site	To Current Group
1	beijing	☐
2	tianjin	☐

Methods

Select the “**Methods**” tab [a]. The configuration page will display two sub-tabs. The default page is Host [b].

Host

Click on the action link “Add SDNS Host” [c]. Enter the SDNS host name in the text field and specify the host method via the selector [d]. Then, click on the action link “Save” [e] to save your settings. The created SDNS host will be displayed in the sort ready table [f].

You can modify the SDNS hosts’ methods via the selectors [g]. Select a desired SDNS host via the radio buttons [h] and the window will display details about the SDNS host in the table [i].

You can add backup IP addresses for SDNS hosts. Click on the “Add Backup IP Entry” action link [j], and then select desired host name from the drop-down list of existing hosts and further specify the backup IP address for the host [k]. Click on “Save” [l], and the configured backup IP address will be displayed in the sort-ready table [m]. Note that backup IP address is used for DNS resolving when and only when all the other IP addresses are not available.

The screenshot shows the Fortinet SDNS configuration interface. The top navigation bar includes tabs: General Settings, Records, Topology, **Methods**, Bandwidth, DPS, IANA, Statistics, and Report. The 'Methods' tab is active, showing sub-tabs: Host (selected) and Region/Pool. The 'Host' sub-tab displays the 'SDNS HOST SETTINGS' table with columns: Domain Name, Method, TTL, Up Vips, Down Vips, Total Traffic, and View Detail. Three hosts are listed: www.gr.com (method: grr), www.vwgr.com (method: vwgr), and www.glc.com (method: glc). Action links 'Delete Host Entry' and 'Add SDNS Host' are at the top right. Below the table is the 'ADD SDNS HOST' form with fields for Domain Name and Method (dropdown), and buttons 'Cancel', 'Save & Add Another', and 'Save'. Below this is the 'DETAILS OF SDNS HOST' section showing details for www.a.com. At the bottom is the 'BACKUP IP' table with columns: Domain Name and Backup IP, listing backup IPs for www.gr.com and www.vwgr.com. Action links 'Clear Backup IP Entry', 'Delete Backup IP Entry', and 'Add Backup IP Entry' are at the top right of this section. Below is another 'ADD SDNS HOST' form, but this one includes a 'Backup IP' field in addition to the 'Domain Name' field. Callouts a-l point to these specific elements.

Methods (Continue)

Region/Pool

Select the sub-tab “Region/Pool” [a].

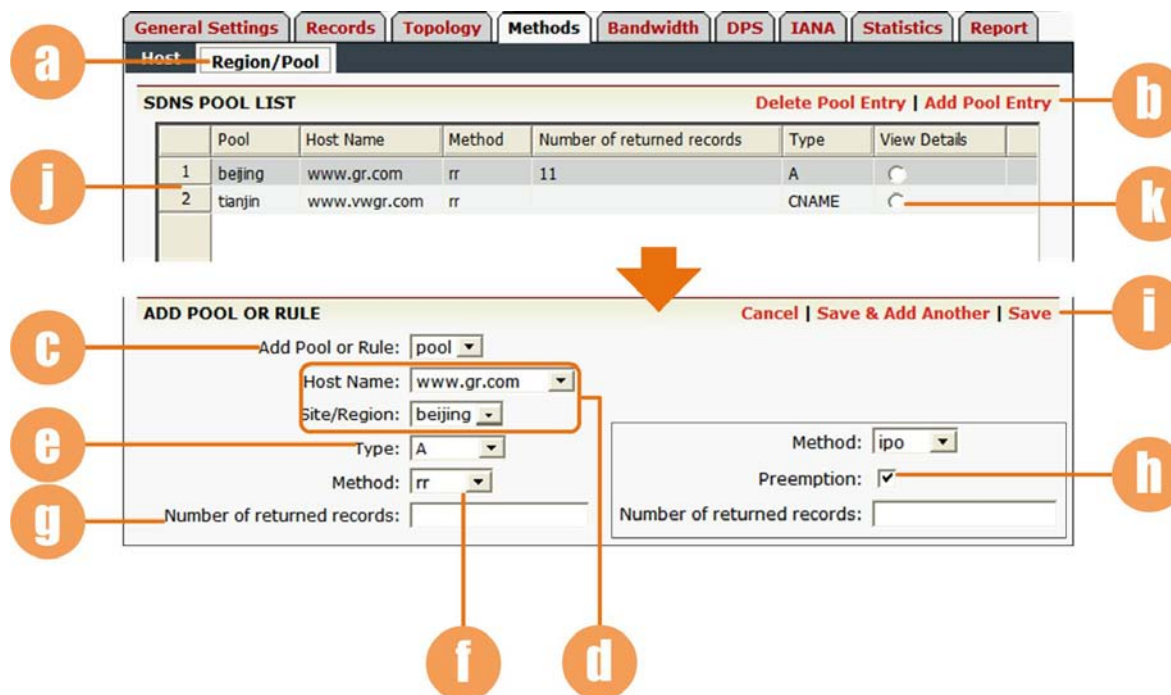
Click on the action link “Add Pool Entry” [b]. A new configuration page will appear. Select to add an SDNS pool or an SDNS rule via the selector [c], and the parameter fields will vary with your selection. The following will introduce how to add an SDNS pool and how to add an SDNS rule.

To add an SDNS pool, specify a host and select a configured region or site to be the pool via the selectors respectively [d], and set the pool type (A or CNAME) via the selector [e].

For type “A”, you need to set the pool’s method [f]. For method rr, wrd or snmp, you need to enter the number of returned IPs [g]. For method ipo, you need to enable or disable the SDNS pool ipo preemption [h] and further enter the number of returned IPs.

Then, click on “Save” [i]. The newly added pool will be displayed in the sort ready table [j].

To modify the SDNS pool settings, you can select an entry and select the radio button [k], or double click on the entry. The window will display a new configuration page.



Methods (Continue)

Region/Pool (Continue)

In this new page, you can modify the pool type via the selector [a]. If A is selected, you need to set the method [b]. If you select the “snmp” method, you need to further set the order type (ascending or descending), service type and weight value [c]. Click on the action link “Save” [d] to save your configuration.

If the “ipo” method is selected and if the SDNS pool ipo preemption is disabled, you can manually preempt [e].

You can further add pool resources.

For pool type “A”, you need to specify the record type (A or AAAA) via the selector [f]: if “A” is selected, you need to input the IP address and priority in the text fields [g]; if “AAAA” is selected, you need to input the IPv6 address and priority in the text fields [h].

For pool type “CNAME”, you need to input the IP address [i].

Click on the action link “Add” [j]. The newly added pool resource will be displayed in the sort ready table [k].

The screenshot displays the Fortinet SDNS configuration interface, divided into two main sections: "SDNS POOL SETTINGS" and "SDNS POOL RESOURCES".

SDNS POOL SETTINGS (Top Section):

- Pool:** beijing
- Host Name:** www.gr.com
- Type:** A (Callout a)
- Method:** rr (Callout b)
- Number of returned records:** 11
- Method:** ipo (Callout e)
- Preemption:** ☐ (Callout e)
- Number of returned records:** 20
- Method:** snmp (Callout c)
- Number of returned records:** 20
- Order Type:** ASC (selected) / DES
- Service Type:** (Callout c)
- Weight:** (Callout c)

SDNS POOL RESOURCES (Middle Section):

- Record type:** A (Callout f)
- IP Address:** (Callout g)
- Weight:** (Callout g)
- Record type:** AAAA (Callout f)
- IPv6 Address:** (Callout h)
- Priority:** (Callout h)

SDNS POOL RESOURCES (Bottom Section):

- Pool:** tianjin
- Host Name:** www.vwgr.com
- Type:** CNAME (Callout i)
- IP Address:** (Callout i)
- Weight:** N/A

Action Links:

- Cancel | Save:** (Callout d)
- Delete | Add:** (Callout j)
- Delete | Add:** (Callout k)

Methods (Continue)

Region/Pool (Continue)

To add an SDNS rule, click on the “Add Rule Entry” action link [\[a\]](#). In the new configuration page, select “rule” via the selector [\[b\]](#), input the rule name in the text field and select a configured region or site via the selector [\[c\]](#). Set the method via the selector [\[d\]](#) and enter the number of returned records in the text field [\[e\]](#).

Click on the “Save” action link [\[f\]](#). The newly added rule will be displayed in the sort ready table [\[g\]](#).

In the table, you can select the radio button [\[h\]](#) or double click on an entry. The window will display a new configuration page.

The screenshot displays the Fortinet SDNS configuration interface. At the top, the 'SDNS RULE LIST' table is shown with columns: Site/Region, Rule, Method, Number of returned records, and View Details. The table contains three entries: 1. beijing, rule1, rr, 20; 2. tianjin, rule2, wrr, 22; 3. Asia, rule3, snmp, 33. Each entry has a radio button in the 'View Details' column. Callout 'g' points to the table, and callout 'h' points to the radio button for the 'beijing' entry. Above the table are links for 'Delete Rule Entry' and 'Add Rule Entry', with callout 'a' pointing to 'Add Rule Entry'. Below the table is the 'ADD POOL OR RULE' configuration form. Callout 'b' points to the 'Add Pool or Rule' dropdown menu, which is currently set to 'rule'. Callout 'c' points to the 'Rule' text input field. Callout 'd' points to the 'Site/Region' dropdown menu, which is currently set to 'beijing'. Callout 'e' points to the 'Method' dropdown menu, which is currently set to 'rr'. Callout 'f' points to the 'Number of returned records' text input field. Callout 'f' also points to the 'Save' link at the bottom right of the form. A large orange arrow points from the 'ADD POOL OR RULE' form up to the 'SDNS RULE LIST' table.

	Site/Region	Rule	Method	Number of returned records	View Details
1	beijing	rule1	rr	20	☐
2	tianjin	rule2	wrr	22	☐
3	Asia	rule3	snmp	33	☐

ADD POOL OR RULE

Add Pool or Rule: rule

Rule:

Site/Region: beijing

Method: rr

Number of returned records:

[Cancel](#) | [Save & Add Another](#) | [Save](#)

Methods (Continue)

Region/Pool (Continue)

In this new page, you can modify the method via the selector [a], and set the number of returned records in the text field [b]. Then, click on the action link “Save” [c] to save your configuration.

You can further add rule resources. Input the IP address and weight properly in the text fields [d] and click on the action link “Add” [e]. Then the newly added information will be displayed in the sort ready table [f].

You can further specify the hosts that use the created rule. Specify the desired hosts via the check boxes [g] and click on the “SAVE CHANGES” button [h] when it appears to make your settings take effect.

The screenshot shows the 'SDNS RULE SETTINGS' page. At the top right are 'RESET' and 'SAVE CHANGES' buttons. Below them are 'Cancel' and 'Save' links. The main form contains the following sections:

- SDNS RULE SETTINGS:**
 - Rule: rule1
 - Site/Region: beijing
 - Method: rr (dropdown menu)
 - Number of returned records: 20 (text field)
- SDNS RULE RESOURCES:**
 - IP Address: (text field)
 - Weight: (text field)
 - Table with 3 columns: ID, IP Address, Weight. It contains one row with ID 1, IP 10.3.121.1, and Weight 1.
- HOSTS USING THIS RULE:**
 - Table with 3 columns: ID, Host Name, Use Current Rule. It contains four rows:

ID	Host Name	Use Current Rule
1	www.a.com	☒
2	www.b.com	☐
3	www.c.com	☐
4	www.d.com	☐

Callouts a through h point to specific elements: a points to the Method dropdown, b points to the Number of returned records field, c points to the Save link, d points to the IP Address field, e points to the Add link, f points to the SDNS RULE RESOURCES table, g points to the Use Current Rule checkbox for www.c.com, and h points to the SAVE CHANGES button.

Bandwidth

Select the “Bandwidth” tab [a]. The configuration page will display five sub-tabs. The default page is Region [b].

Region

On the new page, all regions configured previously are displayed in the sort ready table [c]. To specify the maximum bandwidth of a region, double click on the entry under the “Limit” column and input the value in the text field [d]. You can also set the mode of each region via the selector [e]. Remember to click on the “SAVE CHANGES” button [f] when it appears to save your configuration.

Site

Select the sub-tab “Site” [g]. Follow the same steps with the region band settings to set the bandwidth for sites.

Member

Select the sub-tab “Member” [h]. Follow the same steps with the region band settings to set the bandwidth for members.

The screenshot shows the Fortinet SDNS configuration interface. At the top, there are tabs for General Settings, Records, Topology, Methods, Bandwidth (selected), DPS, IANA, Statistics, and Report. On the right, there are buttons for RESET and SAVE CHANGES. Below the tabs, there are sub-tabs for Region, Site, Member, Host, and IP. The Region sub-tab is active, showing the SDNS REGION BAND SETTINGS table. The table has columns for Name, ID, Limit(Mbytes/S), Usage(Bytes/S), and Mode. There are two entries: 1. Asia (ID 3) and 2. Euro (ID 4). The Limit column for the first entry is highlighted in yellow. Callouts point to various elements: 'a' points to the Bandwidth tab; 'b' points to the Region sub-tab; 'c' points to the table; 'd' points to the Limit column; 'e' points to the Mode dropdown; 'f' points to the SAVE CHANGES button; 'g' points to the Site sub-tab; and 'h' points to the Member sub-tab.

Name	ID	Limit(Mbytes/S)	Usage(Bytes/S)	Mode
1 Asia	3		0	null
2 Euro	4		0	null

Site	ID	Limit(Mbytes/S)	Usage(Bytes/S)	Mode
1 beijing	1		0	null
2 tianjin	2		0	null

Name	Limit(Mbytes/S)	Usage(Bytes/S)	Mode
1 sdns1	0		null
2 sdns2	0		null

Bandwidth (Continue)

Host

Select the sub-tab “**Host**” [a]. Enter the domain name and the maximum bandwidth in the text fields [b]. Specify the bandwidth mode via the selector [c]. Then, click on the action link “Add Band Entry” [d], and the information will be displayed in the sort ready table [e].

You can modify the maximum bandwidth by double clicking on it under the “Limit” column [f]. You can also change the mode via the selector [g].

IP

Select the “IP” sub-tab [h]. Enter the IP address and the maximum bandwidth of the IP address in the text fields [i]. Set the bandwidth mode via the selector [j]. Then, click on the action link “Add Band Entry” [k], and the configured information will be displayed in the sort ready table [l].

To modify the IP bandwidth and mode, follow the same way with the host bandwidth modification.

The screenshot displays the Fortinet SDNS configuration interface, specifically the Bandwidth section. It is divided into two main tabs: Host and IP. The Host tab is currently active, showing the 'SDNS HOST BAND SETTINGS' section. The IP tab is also visible, showing the 'SDNS IP BAND SETTINGS' section. The interface includes various input fields, dropdown menus, and action links for adding and deleting band entries. Numbered callouts (a through k) highlight specific elements: a points to the Host tab, b points to the Domain Name field, c points to the Mode dropdown, d points to the 'Add Band Entry' link, e points to the table of host band settings, f points to the Limit column, g points to the Mode dropdown in the table, h points to the IP tab, i points to the IP Address field, j points to the Mode dropdown, k points to the 'Add Band Entry' link, and l points to the table of IP band settings.

SDNS HOST BAND SETTINGS

Band Mode For Host:
A: Client Request + Client Response + Server Request + Server Response
B: Client Request + Server Request
C: Client Response + Server Response
D: Client Request + Client Response

Domain Name:
Limit(Mbytes/S):
Mode: A

	Domain Name	Limit(Mbytes/S)	Usage(Bytes/S)	Mode
1	www.a.com	99	0	A
2	www.b.com	88	0	B

SDNS IP BAND SETTINGS

IP Address:
Limit(Mbytes/S):
Mode: in&out

	IP Address	Limit(Mbytes/S)	Usage(Bytes/S)	Mode
1	172.16.63.5	66	0	in&out

DPS

SDNS Dynamic Proximity System (DPS) aims at providing a dynamically generated proximity rule table, instead of statically configured proximity rules for Fortinet SDNS. For DPS feature, DPS detectors are needed for proximity detection and DPS servers are used for DNS resolution.

Select the “DPS” tab [\[a\]](#). The configuration page will display three sub-tabs. The default page is SDNS DPS Settings [\[b\]](#).

SDNS DPS Settings

You can turn on SDNS DPS by selecting the check box [\[c\]](#), and start the DPS master by selecting the check box [\[d\]](#). Specify the interval of SDNS dynamic proximity query, the interval of sending local DNS IP addresses, the time span of history data that the detector detects, and the expiry count in the text fields respectively [\[e\]](#). Select the method of SDNS DPS server via the selector [\[f\]](#) (defaults to “rtt”). If you set the method to “mix”, the DPS detector will detect a mixed value of the rtt, plr and hops methods. In this case, you need to further specify the weights of the three methods in the text fields [\[g\]](#).

After confirming the inputted information, click on the “SAVE CHANGES” button to save the settings [\[h\]](#).

The screenshot shows the Fortinet SDNS configuration interface. At the top, there are tabs: General Settings, Records, Topology, Methods, Bandwidth, **DPS** (selected), IANA, Statistics, and Report. Below these are sub-tabs: **SDNS DPS Settings** (selected), Dynamic Proximity Rules, and Local Detectors. The main content area is titled "SDNS DPS SETTINGS" and contains the following fields:

- SDNS DPS:** A checkbox (callout [\[c\]](#)) currently unchecked.
- SDNS DPS Master:** A checkbox (callout [\[d\]](#)) currently unchecked.
- Query Interval:** A text field with the value 1200.
- Send Interval:** A text field with the value 120.
- History Scale:** A text field with the value 9000.
- Expire Count:** A text field with the value 1.
- Method:** A dropdown menu (callout [\[f\]](#)) currently set to "rtt".
- Weights:** A row of text fields (callout [\[g\]](#)) for "rtt" (1), "plr" (1), and "hops" (1).
- Buttons:** "RESET" and "SAVE CHANGES" (callout [\[h\]](#)) buttons are at the top right. A "Clear" button is at the top right of the settings area (callout [\[d\]](#)).

DPS (Continue)

SDNS DPS Settings (Continue)

To add a DPS server into the DPS member list, enter the IP address of the DPS server in the text field [\[a\]](#) and click on the “Add” action link [\[b\]](#). The new member will be displayed in the sort ready table [\[c\]](#). You can delete a member from the list or clear all members by clicking on the desired action link [\[d\]](#).

To add an SDNS DPS detector, you can click on the action link “Add” [\[e\]](#), and the configuration window will display a new page. Specify the site (must have been defined in SDNS configuration), the IP address of the detector, port number (defaults to 44544) and detect interval in the text fields [\[f\]](#). Click on the “Save” action link [\[g\]](#), and the settings will be displayed in the sort ready table [\[h\]](#). You can select to delete a detector, edit detector configuration or clear all detectors’ configuration by clicking on the desired action link [\[i\]](#).

The screenshot displays the SDNS DPS configuration interface. It is divided into two main sections: **SDNS DPS MEMBERS** and **SDNS DPS DETECTORS**. Below these is a modal window titled **ADD OR EDIT SDNS DPS DETECTOR**.

SDNS DPS MEMBERS section includes:

- a**: Member IP Address input field.
- b**: Clear | Delete | Add action links.
- c**: Table with 2 columns: Member ID, Member IP Address.

Member ID	Member IP Address
1	172.16.63.6
2	172.16.63.7

SDNS DPS DETECTORS section includes:

- e**: Clear | Delete | Edit | Add action links.
- h**: Table with 5 columns: Detector ID, Site, IP Address, Port, Detect Interval.

Detector ID	Site	IP Address	Port	Detect Interval
1	beijing	172.16.63.5	44544	900
2	tianjin	172.16.63.6	44544	900

ADD OR EDIT SDNS DPS DETECTOR modal window includes:

- f**: Site, IP Address, Port, Detect Interval input fields.
- g**: Cancel | Save & Add Another | Save action links.

DPS (Continue)

Dynamic Proximity Rules

Select the “Dynamic Proximity Rules” sub tab [a]. On this page, all the dynamic proximity statistics generated based on the detection results will be displayed in the table [b].

To export the dynamic proximity statistics, you can first select the sort standard and specify to export the statistics in ascending or descending order [c], and then click on the “Export” action link [d].

You can export the dynamic proximity rules via three methods: File, SCP and TFTP. For File method, select the “File” radio button and input the file name in the text field [e]; for SCP method, select the “SCP” radio button and input required information in the text fields [f]; for TFTP method, select the “TFTP” radio button and input required information in the text fields [g].

After confirming the inputted information, click on the “Export” action link [h] to start exporting.

General Settings | **Records** | **Topology** | **Methods** | **Bandwidth** | **DPS** | **IANA** | **Statistics** | **Report**

SD-WAN DPS Settings | **Dynamic Proximity Rules** | **Local Detectors**

DYNAMIC PROXIMITY STATISTICS First Page | Previous Page | Next Page | Last Page

IP Address	Default region	Best site

EXPORT DYNAMIC PROXIMITY STATISTICS Export

Sort Standard: IP Address ☐ ASC: ☒ DESC: ☐

EXPORT DYNAMIC PROXIMITY RULES Export

Export Method: File ☒ SCP ☐ TFTP ☐

File Name:

Export Method: File ☐ SCP ☒ TFTP ☐

Server IP Address:

Username:

Password:

File Path:

File Name:

Export Method: File ☐ SCP ☐ TFTP ☒

Server IP Address:

File Name:

DPS (Continue)

Local Detectors

Select the “**Local Detectors**” sub tab [\[a\]](#).

To add an SDNS DPS local detectors, first specify a name for the local detector [\[b\]](#). Then, enter the IP address, interface name, detect port number, report port number and detect timeout value in the text fields [\[c\]](#). After confirming the inputted information, click on the action link [\[d\]](#). The configured information of the local detectors will be displayed in the table below [\[e\]](#).

To delete a local detector or clear all local detectors, you can click on the desired action link [\[f\]](#).

You can view the version information of the SDNS DPS local detector in the table [\[g\]](#).

The screenshot shows the Fortinet web interface for configuring SDNS DPS Local Detectors. The top navigation bar includes tabs for General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA, Statistics, and Report. The sub-navigation bar has SDNS DPS Settings, Dynamic Proximity Rules, and Local Detectors. The main content area is titled 'ADD AN SDNS DPS LOCAL DETECTOR' and contains a form with fields for Name, IP Address, Interface, Detect Port (53455), Report Port (44544), and Detect Timeout (30). An 'Add' button is in the top right. Below the form is a table titled 'SDNS DPS LOCAL DETECTORS' with columns for Name, IP Address, Interface, Detect Port, Report Port, and Detect Timeout. It lists two detectors: detector1 and detector2. A 'Clear | Delete' link is in the top right of the table. At the bottom is a section titled 'SDNS DPS LOCAL DETECTOR VERSION' showing version 1 and copyright information. Callouts a through g point to specific elements: a (Local Detectors tab), b (Name field), c (IP Address, Interface, Detect Port, Report Port, Detect Timeout fields), d (Add button), e (Table), f (Clear | Delete link), and g (Version section).

Name	IP Address	Interface	Detect Port	Report Port	Detect Timeout
detector1	172.16.63.2	bond1	53455	44544	30
detector2	172.16.63.3	bond1	53456	44544	30

IANA

Select the “IANA” tab [a]. The window presents two sub tabs. The Import page is displayed by default [b].

Import

You can import an IANA address table via HTTP or FTP method. To import via HTTP method, supply the URL address in the text field [c]. To import via FTP method, supply the parameter fields properly [d].

Confirm the inputted information, and click on the action link “Import” [e].

Query

Select the “Query” sub tab [f]. You can query the corresponding region of an IANA address. Supply the address in the text field [g] and click on the action link [h] to begin query.

The screenshot displays the Fortinet web interface for the IANA configuration page. The top navigation bar includes tabs for General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA (selected), Statistics, and Report. The IANA tab is highlighted with callout 'a'. Below the navigation bar, there are two sub-tabs: Import (selected, callout 'b') and Query (callout 'f').

The Import sub-tab contains the following elements:

- Callout 'c' points to the 'URL' text field.
- Callout 'd' points to the 'Server IP', 'User Name', 'Password', and 'File Name' input fields.
- Callout 'e' points to the 'Import' button.
- Below the input fields, there is a note: "Note: If FTP server supports access with anonymous mode, User Name and Password should be reserved empty!"

The Query sub-tab contains the following elements:

- Callout 'g' points to the 'Address' text field.
- Callout 'h' points to the 'Query' button.

Statistics

Select the “**Statistics**” tab [\[a\]](#), and the configuration page will display four sub-tabs. The default page is **Local DNS** [\[b\]](#). To view the statistics, you just need to enter the Enable mode.

Local DNS

This page displays all local DNS statistics information [\[c\]](#).

SDNS Host

Select the sub-tab “SDNS Host” [\[d\]](#). This page displays all SDNS host statistics, including host name, method, time to live (TTL), the number of up VIPs, the number of down VIPs and total traffic [\[e\]](#).

VIP Address

Select the sub-tab “VIP Address” [\[f\]](#). The configuration page will display all VIPs statistics of SDNS, including virtual IP, traffic information, the number of TCP connections and the VIP status [\[g\]](#).

Query

Select the “Query” sub tab [\[h\]](#) to view all query statistics of SDNS [\[i\]](#).

The screenshot shows the Fortinet SDNS Statistics page. The top navigation bar includes tabs: General Settings, Records, Topology, Methods, Bandwidth, DPS, IANA, Statistics (selected), and Report. Below this, there are sub-tabs: Local DNS (selected), SDNS Host, VIP Address, and Query. The page is divided into four main sections, each with a table of statistics:

- LOCAL DNS STATISTICS** (Callout [\[c\]](#)): A table with columns: Local DNS, TotalRequest, SuccessRequest, Unauthoritative, FirstRequestTime, and IPSEG.
- SDNS HOST STATISTICS** (Callout [\[e\]](#)): A table with columns: Domain_name, Method, TTL, Num_vips_up, Num_vips_down, and Total_traffic. It lists statistics for www.gr.com, www.vwgr.com, and www.glc.com.
- SDNS VIP STATISTICS** (Callout [\[g\]](#)): A table with columns: VIP, Traffic(current/max), TCP_Connections, and Status. It shows statistics for VIP 172.16.63.5.
- SDNS QUERY STATISTICS** (Callout [\[i\]](#)): A table with columns: Host, Requests, Success, Failed, Lastminhits, Lasthourhits, and Peakminhit. It shows statistics for host forti.

Callouts [\[a\]](#) through [\[i\]](#) point to specific elements: [\[a\]](#) points to the Statistics tab; [\[b\]](#) points to the Local DNS sub-tab; [\[c\]](#) points to the LOCAL DNS STATISTICS table; [\[d\]](#) points to the SDNS Host sub-tab; [\[e\]](#) points to the SDNS HOST STATISTICS table; [\[f\]](#) points to the VIP Address sub-tab; [\[g\]](#) points to the SDNS VIP STATISTICS table; [\[h\]](#) points to the Query sub-tab; and [\[i\]](#) points to the SDNS QUERY STATISTICS table.

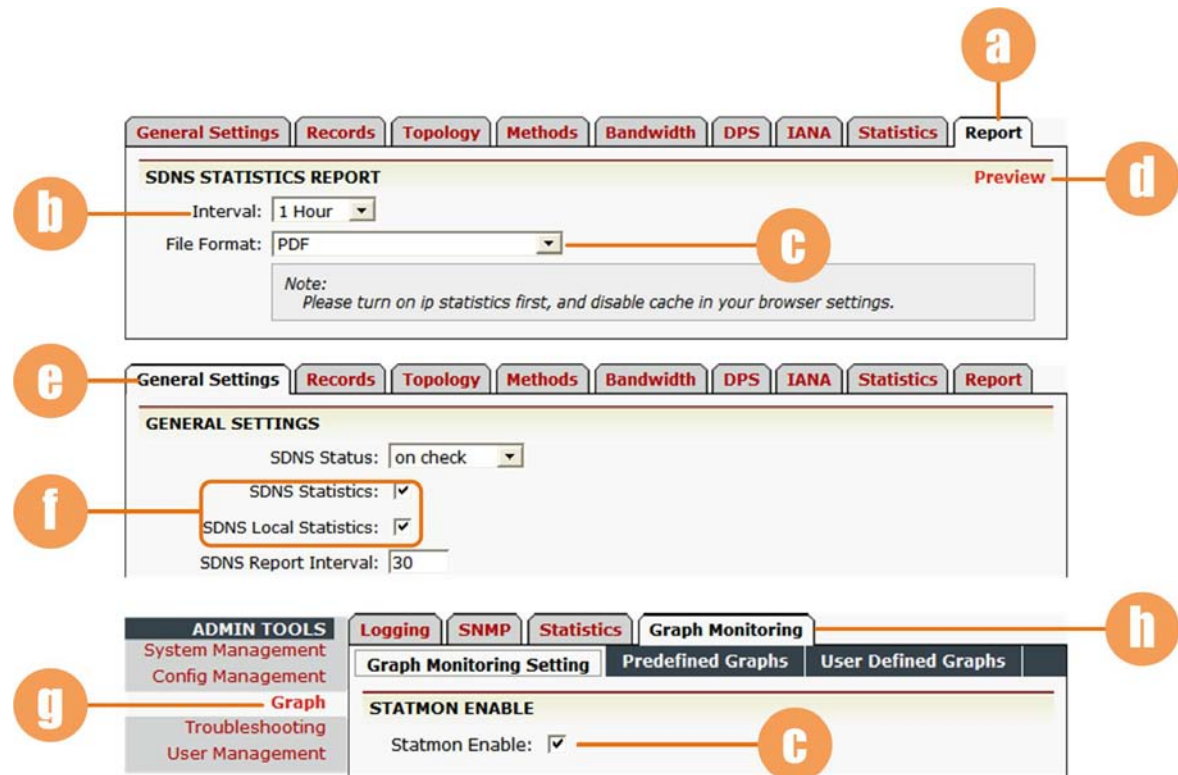
Report

Select the “**Report**” tab [a]. To view the report, you just need to enter the Enable mode.

Specify the interval of the report via the selector [b] and select the desired report format [c]. Click on the action link “**Preview**” [d]. Then, you will be presented with an SDNS Statistics Report file in the format you have specified.

Note that the contents on the Report page are available only after you have made the following configurations.

- Go to the General Settings page [e], and enable the SDNS Statistics and SDNS Local Statistics functions [f].
- Select the Graph feature link [g] under the Admin Tools feature group, and go to the Graph Monitoring Setting page under the “Graph Monitoring” tab [h]. Then, enable the statmon function via the check box [i].



Monitoring

FortiBalancer appliance allows users to monitor real-time SDNS query and pool SNMP statistics.

SDNS

To use this feature, you just need to enter the Enable mode.

Select the feature link **Monitoring** from the sidebar [a].

Select the “SDNS” tab [b], and the window will display the monitoring information about SDNS queries in the table [c].

SERVER LOAD BALANCE

- Real Services
- Virtual Services
- Check Lists
- Groups
- Application Setting
- Monitoring

PROXY

- Compression
- Caching Proxy
- Monitoring

ADVANCED LOAD BALANCE

- Link Load Balance
- Global Load Balance
- Monitoring**

ADMIN TOOLS

- System Management
- Config Management
- Graph

SDNS **Pool SNMP Statistics**

SDNS QUERY MONITORING OVERVIEW

Query	Success	Unauthoritative	Fail
0	0	0	0

SDNS QUERY SECOND MONITORING

	Query	Success	Unauthoritative	Fail
Last Second	0	0	0	0
Peak	0	0	0	N/A

SDNS QUERY MINUTE MONITORING

	Query	Success	Unauthoritative	Fail
Last Minute	0	0	0	0
Peak	0	0	0	N/A

SDNS QUERY HOUR MONITORING

	Query	Success	Unauthoritative	Fail
Last Hour	0	0	0	0
Peak	0	0	0	N/A

SDNS QUERY DAY MONITORING

	Query	Success	Unauthoritative	Fail
Last Day	0	0	0	0
Peak	0	0	0	N/A

Pool SNMP Statistics

Select the “Pool SNMP Statistics” tab [d]. The window will display the monitoring information about pool SNMP statistics in the table [e].

SDNS **Pool SNMP Statistics**

POOL SNMP STATISTICS

Host Name	Pool	Order Type	Service Type	Weight	Service Type	Weight

Admin Tools

System Management

In this section, we will discuss various configuration management functions available for the FortiBalancer appliance.

System Info

Make certain you are in **Config mode** and have selected the **System Management** feature link from the sidebar [a]. The configuration window will present a page with five navigational tabs [b].

Under the “**System Info**” tab, there are three sub tabs: **Version**, **Memory** and **Statistics**. By default, the **Version** page is displayed [c].

Version

On this page, the window displays the current running version and related information of the FBLOS powering the FortiBalancer appliance [d].

The screenshot shows the FortiBalancer Admin Tools interface. On the left is a sidebar with various configuration categories. On the right is the main configuration window.

Sidebar (Left):

- Basic Networking
- Advanced Networking
- Clustering
- Monitoring
- SERVER LOAD BALANCE**
 - Real Services
 - Virtual Services
 - Check Lists
 - Groups
 - Application Setting
 - Monitoring
- PROXY**
 - Compression
 - Caching Proxy
 - Monitoring
- ADVANCED LOAD BALANCE**
 - Link Load Balance
 - Global Load Balance
 - Monitoring
- ADMIN TOOLS**
 - System Management** (highlighted with 'a')
 - Config Management
 - Graph
 - Troubleshooting
 - User Management

Main Window (Right):

At the top of the main window is a tabbed interface with the following tabs: **System Info**, **Access Control**, **Update**, **Shutdown/Reboot**, and **License**. The **System Info** tab is selected. Below this is a sub-tabbed interface with **Version**, **Memory**, and **Statistics**. The **Version** sub-tab is selected.

The **SYSTEM VERSION** page displays the following information:

```

FBLOS Rel.FBL.8.2.0.2 build on Fri Jun 10 13:18:05 2011

Host name : AN
System CPU : Intel(R) Core(TM)2 Quad CPU   Q6600   @ 2.40GHz
System Module : PDSMi-LN4+
System RAM : 3991824 kbytes.
System boot time : Mon Jun 27 07:46:27 GMT (+0000) 2011
Current time : Mon Jun 27 09:17:42 GMT (+0000) 2011
System up time : 1:31
Platform Bld Date : Fri Jun 10 13:17:54 UTC 2011
SSL HW : HW ( 1X16C ) Initialized
Compression HW : No HW Available
Network Interface : 4 x Gigabit Ethernet copper
Model : Array APV 3520 B
Serial Number : 0437A3345903520003011044723476
Licensed Features : WebWall Clustering L4SLB L7SLB Caching
                   SSL tProxy AppGateway SwCompression LLB GSLB
                   QoS MultiLang DynRoute IPv6
License Key : 1bleaad9-67af1899-8cd7b083-fd37c0b1-0f85f7f8-00000000

FORTINET Customer Support
Telephone : please go to URL support.fortinet.com
Email : please go to URL support.fortinet.com
Update : please contact support for instructions
Website : http://www.fortinet.com

Other Root Version
Rel.TM.8.2.0.5 build on Thu Jun 23 11:36:51 2011
    
```

System Info (Continue)

Memory

Select the “**Memory**” sub tab [\[a\]](#), and the window will display all data about current memory usage in the box [\[b\]](#).

Statistics

Select the “**Statistics**” sub tab [\[c\]](#), and the window will display all information about current configuration in the box [\[d\]](#).

The screenshot shows the Fortinet System Info page with the following tabs: System Info, Access Control, Update, Shutdown/Reboot, License, Version, Memory, and Statistics. The Memory tab is selected, showing the SYSTEM MEMORY USAGE table. The Statistics tab is also shown, displaying system configuration details.

a points to the **Memory** sub tab.

b points to the **SYSTEM MEMORY USAGE** table.

c points to the **Statistics** sub tab.

d points to the **SYSTEM STATISTICS** section.

ITEM	SIZE	LIMIT	USED	FREE	REQUESTS
FastSLB nat entry:	328,	4000000,	0,	0,	0
FastSLB hash node:	40,	4400000,	0,	0,	0
FastSLB syncache:	80,	131072,	0,	0,	0
Fastslb bitmap:	40,	4000,	0,	0,	0
hw compression data:	688,	2048,	0,	0,	0
compression event:	48,	5120,	0,	0,	0
compression data:	104,	2048,	0,	0,	0
Cache filter host queue:	24,	500,	0,	0,	0

SYSTEM STATISTICS

```

<<<< Version >>>>

FBLOS Rel.FBL.8.2.0.2 build on Fri Jun 10 13:18:05 2011

Host name : AN
System CPU : Intel(R) Core(TM)2 Quad CPU    Q6600  @ 2.40GHz
System Module : PDSMi-LN4+
System RAM : 3991824 kbytes.
System boot time : Mon Jun 27 07:46:27 GMT (+0000) 2011
Current time : Mon Jun 27 09:24:18 GMT (+0000) 2011
System up time : 1:38
Platform Bld Date : Fri Jun 10 13:17:54 UTC 2011
SSL HW : HW ( 1X16C ) Initialized
Compression HW : No HW Available
Network Interface : 4 x Gigabit Ethernet copper
Model : Array APV 3520 B
Serial Number : 0437A3345903520003011044723476
Licensed Features : WebWall Clustering L4SLB L7SLB Caching
    
```

Access Control

Select the “Access Control” tab [a], where you can perform settings about access control.

Enable or disable WebUI via the check box [b], and change WebUI IP or port settings via text fields [c]. Please read the Note messages [d] before making configuration here.

Enable or disable XMLRPC via the check box [e]. Supply the desired port number in the text field [f].

Enable or disable SSH access to the FortiBalancer appliance via the check box [g]. You can click on the action link [h] to regenerate SSH host keys.

Enable or disable the external authentication via the check box [i]. Then, specify the authentication method, server, host name, port number and secret key in the area [j]. To delete or clear AAA configuration, you can click on the desired action link [k].

To change the enable mode password, you can input the new password in the text field [l]. The default password is null.

You can set the Config Mode timeout value in the text field [m], or reset the Config Mode immediately by clicking on the “Reset” button [n]. Note that resetting Config Mode will terminate the current WebUI session.

Remember to click on the “SAVE CHANGES” button [o] to save the changes made.

The screenshot shows the Fortinet web interface for the 'Access Control' tab. The page has a top navigation bar with tabs: System Info, Access Control (selected), Update, Shutdown/Reboot, License, and buttons for RESET and SAVE CHANGES. The main content area is divided into several sections:

- WEBUI SETTINGS:** Contains a note about session disabling, a checkbox for 'Enable WebUI' (checked), and text fields for 'IP (Optional)' and 'Port' (8888).
- XMLRPC SETTINGS:** Contains a checkbox for 'Enable XMLRPC' (unchecked) and a 'Port' field (9999).
- SSH SETTINGS:** Contains a checkbox for 'Enable SSH Access' (checked) and a 'Regenerate SSH Host Keys' link.
- ADMIN AAA SETTINGS:** Contains a checkbox for 'Enable Admin AAA' (unchecked), a 'Method' dropdown (RADIUS), and fields for 'Server' (es01), 'Host', 'Port', and 'Secret'. It also has links for 'Delete AAA Server Configuration' and 'Clear AAA Configuration'.
- ENABLE MODE SETTINGS:** Contains a 'New Enable Password' field.
- CONFIG MODE SETTINGS:** Contains a 'Config Mode Timeout' field (180) and a 'Config Mode' dropdown (Reset).

Annotations a through o point to specific elements: a (Access Control tab), b (Enable WebUI checkbox), c (WebUI IP/Port fields), d (WebUI settings note), e (Enable XMLRPC checkbox), f (XMLRPC Port field), g (Enable SSH Access checkbox), h (Regenerate SSH Host Keys link), i (Enable Admin AAA checkbox), j (AAA configuration fields), k (AAA action links), l (New Enable Password field), m (Config Mode Timeout field), n (Reset button), and o (SAVE CHANGES button).

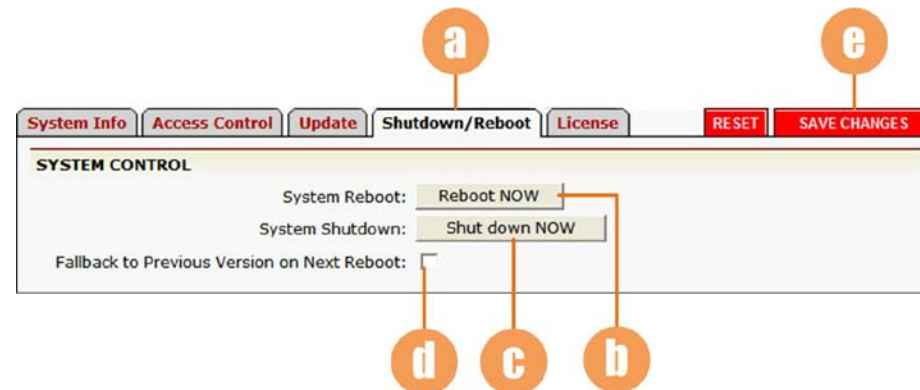
Update

Select the “**Update**” tab [a], and the window will present a new configuration page. You can update the system by using a local host file or a URL. To update via a local host file, select the radio button and specify the file path [b] (a browse button is present to help locate files). To update via a URL, select the radio button and specify the URL [c]. Once the file path is located or the URL path is specified, click on the “Apply Update” action link [d].

The screenshot shows the 'Update' tab in the Fortinet Admin Tools interface. The tab is selected, as indicated by the orange circle 'a' pointing to the 'Update' tab label. Below the tabs, there are two sections for system updates. The top section is titled 'SYSTEM UPDATE' and shows 'Using: Local Host File' selected with a radio button. It has a text input field for 'Local Host File Path:' with a 'Browse...' button next to it, and an 'Apply Update' link. An orange circle 'b' points to the 'Local Host File Path:' input field. The bottom section is also titled 'SYSTEM UPDATE' but shows 'URL' selected with a radio button. It has a text input field for 'URL:' and an 'Apply Update' link. An orange circle 'c' points to the 'URL:' input field. An orange circle 'd' points to the 'Apply Update' link in the bottom section. A note below the URL input field states: '* Note: Include http:// or ftp:// in the source URL.'

Shutdown/Reboot

Select the “**Shutdown/Reboot**” tab [a], and the window will present a new configuration page. You can reboot the system by clicking on the “Reboot NOW” button [b], and shut down the system by clicking on the “Shut down NOW” button [c]. The check box [d] can be selected to fall back to the previous software version on the next reboot. Remember to click on the “SAVE CHANGES” button [e] when it appears to save your configuration.



License

Select the “**License**” tab [a], and a new configuration page will be displayed. In the text field [b], the current license for the FortiBalancer appliance is displayed. If you want to replace the license with a new license, input the new one in the field [b] and click on the desired action link [c].



Config Management

In this section, we will discuss the configuration management functions available for the FortiBalancer appliance.

View

Make certain you are in **Config mode** and have selected the **Config Management** feature link from the sidebar [a]. The window will present a configuration page with seven navigational tabs. The View page is displayed by default [b].

Under the “View” tab, there are three sub tabs: Running Config, Startup Config and Saved File [c].

Running Config

The **Running Config** page displays information about the current running configurations [d].

Startup Config

Select the “**Startup Config**” sub tab [e], and the configuration window will display the startup configuration information [f].

Saved File

Select the “**Saved File**” sub tab [g], and the configuration window will display all configuration files currently saved in the sort ready table [h]. Double click on a file entry to view the file details.

The screenshot shows the FortiBalancer Config Management interface. The sidebar on the left contains a tree view with categories: Advanced Networking, SERVER LOAD BALANCE, PROXY, ADVANCED LOAD BALANCE, and ADMIN TOOLS. The main panel has a top navigation bar with tabs: View, Backup, Load, Clear, Synchronization, Synchronization Sdns, and Command Timeout. Below this is a sub-tab bar with Running Config, Startup Config, and Saved File. The main content area displays the configuration for the selected sub-tab.

Callouts:

- a:** Points to the **Config Management** link in the sidebar.
- b:** Points to the **View** tab in the top navigation bar.
- c:** Points to the **Running Config** sub-tab.
- d:** Points to the **Running Config** content area.
- e:** Points to the **Startup Config** sub-tab.
- f:** Points to the **Startup Configuration** content area.
- g:** Points to the **Saved File** sub-tab.
- h:** Points to the **CONFIGURATION ON SAVED FILE** table.

Running Configuration Content:

```
#command timeout configuration
system command timeout 120

#admin aaa configuration
admin aaa off
admin aaa method RADIUS

#hostname configuration
hostname "FBL"
config timeout 180
```

Startup Configuration Content:

```
Current configuration on disk

#Last configuration change at Mon Jun 27 08:44:25 2011 by admin
#version Rel.FBL.8.2.0.2 build on Fri Jun 10 13:18:05 2011

#command timeout configuration
system command timeout 120
```

Configuration on Saved File Table:

	Saved File Name on Server	Date	Time	Size
1	sync_sdns4321	Jan 09 2009	17:15:52	430
2	aa2	Jan 24 2010	02:52:09	7796

Backup

Select the “Backup” tab [a], and the configuration window will present several options for backing up configuration files.

To simply back up the existing running configuration and retain this as the “Startup Config”, simply select the radio button [b] and click on the action link “Backup” [c].

To back up the configuration file using SCP [d], supply the SCP server name, user name, password and server path in the text fields [e] and click on the action link “Backup” to begin the backup.

To back up the configuration file using TFTP [f], supply the TFTP server IP address and file name in the text fields [g] and click on the action link “Backup” to begin the backup.

To save the configuration in a local file [h], supply the file name in the text field [i] and click on the action link “Backup” to begin the backup. A list of previously saved files will be displayed in the sort ready table [j]. You may select one of these files to be updated or deleted.

The screenshot shows the 'Backup' tab in the Fortinet Admin Tools interface. It contains four sections for backing up the running configuration, each with a 'Backup' link. The sections are: 1. Startup Config (selected), 2. SCP, 3. TFTP, and 4. Saved File. Each section has a 'Backup Using' dropdown and a 'Backup' link. The 'Saved File' section includes a table of previously saved files.

Callouts:

- a:** Backup tab
- b:** Backup Using: Startup Config
- c:** Backup link
- d:** Backup Using: SCP
- e:** Server Name, User Name, Password, Path text fields
- f:** Backup Using: TFTP
- g:** Server IP, File Name text fields
- h:** Backup Using: Saved File
- i:** File Name text field
- j:** CONFIGURATION ON SAVED FILE table

	Saved File Name on Server	Date	Time	Size
1	sync_sdns4321	Jan 09 2009	17:15:52	430
2	aa2	Jan 24 2010	02:52:09	7796

Load

Select the “Load” tab [a], and the configuration window will present several options for loading configuration files.

To load the last running configuration, select the “Startup Config” radio button [b] and click on the action link “Load” [c].

To load a file from an SCP server [d], supply the SCP server name, user name, password and server path in the text fields [e] and click on the action link “Load” to begin loading.

To load a file using TFTP [f], supply the TFTP server IP address and file name in the text fields [g] and click on the action link “Load” to begin loading.

To load a file from an HTTP server [h], supply the HTTP URL in the text field [i] and click on the action link “Load”.

To load a locally saved file [j], select the file name from a list of previously saved files [k] and click on the action link “Load”.

To load a file from a network location [l], supply the file name in the field [m] or click on the “Browse” button to locate the file. Then click on the action link “Load”.

The screenshot shows the 'Load' tab in the Fortinet Admin Tools interface. The window is titled 'RUNNING CONFIGURATION LOAD' and has a 'Load' button in the top right corner. The interface is divided into several sections, each with a 'Load Using' dropdown menu and a 'Load' button. The sections are: 'Startup Config', 'SCP', 'TFTP', 'HTTP', 'Saved File', and 'Upload File'. The 'Startup Config' section is selected. The 'SCP' section has fields for 'Server Name', 'User Name', 'Password', and 'Path'. The 'TFTP' section has fields for 'Server IP' and 'File Name'. The 'HTTP' section has a field for 'URL'. The 'Saved File' section has a table of saved files and a 'File Name' field. The 'Upload File' section has a 'File Name' field and a 'Browse...' button. Annotations a through m point to various elements in the interface.

Annotations:

- a: Load tab
- b: Startup Config radio button
- c: Load button (top right)
- d: SCP radio button
- e: SCP fields (Server Name, User Name, Password, Path)
- f: TFTP radio button
- g: TFTP fields (Server IP, File Name)
- h: HTTP radio button
- i: HTTP URL field
- j: Saved File radio button
- k: Saved File table
- l: Upload File radio button
- m: File Name field (Upload File)

	Saved File Name on Server	Date	Time	Size
1	sync_sdns4321	Jan 09 2009	17:15:52	430
2	aa2	Jan 24 2010	02:52:09	7796

Clear

Caution should be taken when clearing configurations from the FortiBalancer appliance. Make certain that you only clear those configurations you wish to clear. If you have any questions with clearing a running or saved configuration, please contact Fortinet Customer Support.

Select the “Clear” tab [\[a\]](#) and the configuration window will present four buttons for clearing various configurations.

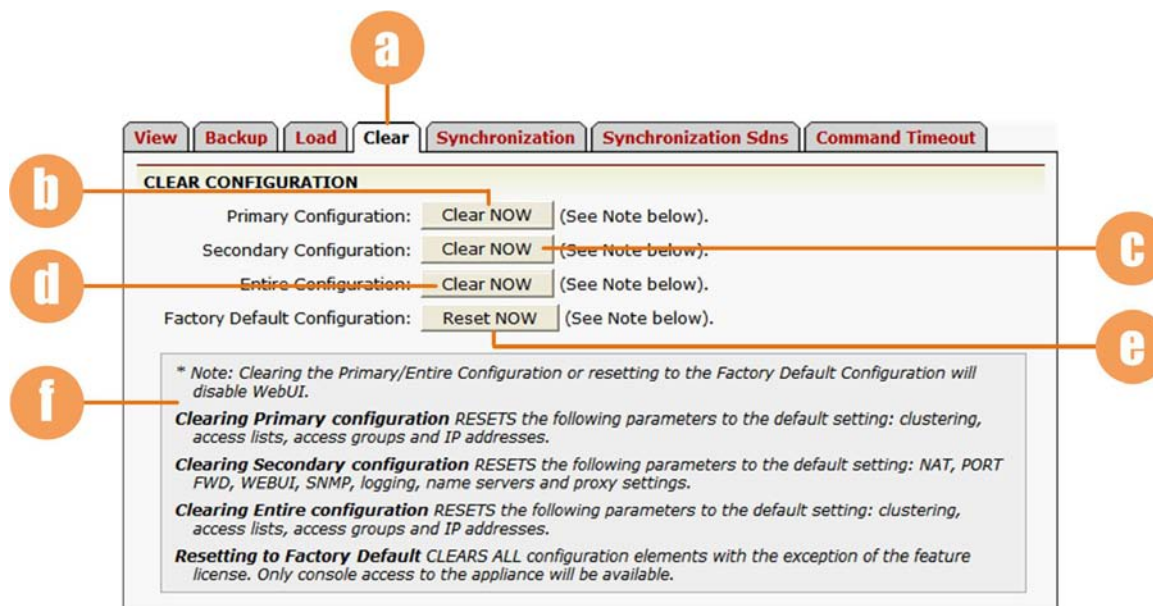
To reset the primary networking functions of the FortiBalancer appliance to the default, including all access lists and groups, IP addresses, clustering and synchronization, click on the “Clear NOW” button [\[b\]](#) for primary configuration.

To reset those secondary network functions of the configuration such as WebUI, NAT, proxy settings, SNMP and logging, click on the “Clear NOW” button for secondary configuration [\[c\]](#).

To clear and delete all locally saved configuration files, except for the default startup file, click on the “Clear NOW” button for entire configuration [\[d\]](#).

To reset the FortiBalancer appliance to factory default allowing for console connectivity only, click on the “Reset NOW” button for factory default configuration [\[e\]](#).

Read the notes [\[f\]](#) carefully before clearing.



Synchronization

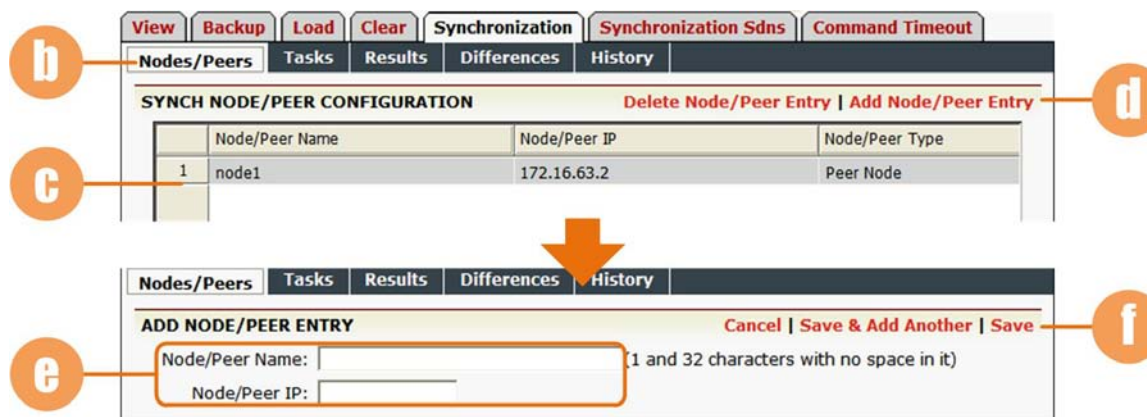
The synchronization feature allows you to transfer configuration information among separate FortiBalancer appliances (referred to as Peers or Nodes) on the same network. Using configuration synchronization, you can also setup an active-standby configuration for failover support. The basic configuration must be completed before configuring the virtual clustering functionality.

Nodes/Peers

Make certain you have selected the “**Synchronization**” tab [a], and the window presents five sub tabs. The Nodes/Peers page is displayed by default [b]. Here, all peers previously configured will be displayed in the sort ready table [c]. The first step with synchronization is to define the name and IP address for each peer. To do this, you can click on the action link “Add Node/Peer Entry” [d].

In the new configuration window, supply the node/peer name and IP address in the texts fields [e] and click on the “Save” action link [f].

All newly added peers will be displayed in the sort ready table [c].



Synchronization (Continue)

Tasks

Select the “Tasks” sub tab [a]. The configuration window will display all configured peers in the table under “Configuration Synchronization” [b] where all individual FortiBalancer appliances share the same configuration, and also in the table under “Synchronization Rollback” [c], where you can pull a specific FortiBalancer appliance back out of a clustered group and rollback the configuration to the pre-synchronized status (refer to the following “Synchronization Rollback” section).

Configuration Synchronization: This feature allows you to either “push” a configuration onto other FortiBalancer appliances in the network via the “TO” radio button [d] or “pull” a configuration from a specific appliance and place the configuration on the appliance being setup via the “FROM” radio button [e]. Note that you may “push” a configuration onto all existing appliances, but you can only “pull” a configuration from one appliance at a time. Once you have selected the appliances to synchronize, click on the link [f].

Synchronization Rollback: To reset to a previously synchronized configuration that was received from another peer appliance on the network, select the “LOCAL” radio button [g], select the peer appliance that originated the configuration from the list [c] and click on the “Rollback” action link [i]. To reset a peer that received the configuration from the current appliance, select “REMOTE” [h], specify the destination appliance from the list [c] and click on the action link [i].

The screenshot shows the FortiBalancer Admin Tools interface for Synchronization. The top navigation bar includes tabs: View, Backup, Load, Clear, Synchronization, Synchronization Sdms, and Command Timeout. The Synchronization tab is active, showing sub-tabs: Nodes/Peers, Tasks, Results, Differences, and History. The Tasks sub-tab is selected, indicated by callout [a].

A note at the top states: “* Note: If you change the local configuration by synchronization or rollback, this WebUI session might be terminated. If this happens, you need to use the CLI to enable the WebUI after the config mode timeout (180 seconds).”

The main section is titled “CONFIGURATION SYNCHRONIZATION”. It features a “Synchronization Direction” section with two radio buttons: “TO” [d] and “FROM” [e]. Below this is a table with three columns: “Node/Peer Name”, “Node/Peer IP”, and “Node/Peer Type”. The table contains two rows: “1 All Nodes/Peers All Nodes/Peers -” and “2 node1 172.16.63.2 Peer Node”. Callout [b] points to the table header, and callout [c] points to the table body. To the right of the table is a “Synchronize” link [f].

Below the synchronization section is the “SYNCHRONIZATION ROLLBACK” section. It has a “Rollback Location” section with two radio buttons: “LOCAL” [g] and “REMOTE” [h]. Below this is another table with the same columns as the first. It contains one row: “1 node1 172.16.63.2 Peer Node”. Callout [c] points to the table header, and callout [i] points to the “Rollback” link [i] on the right.

Synchronization (Continue)

Results

Select the “**Results**” sub tab [a], and the configured peers are displayed in the sort ready table [b]. You can view the synchronization results of a peer by double clicking on it in the table or selecting it and clicking on the action link “View Synch Summary” [c]. Then, the results will be displayed in the table below [d].

Differences

Select the “**Differences**” sub tab [e], and all configured peers are displayed in the sort ready table [f]. Double click on a desired peer to view the configuration differences between the selected remote peer FortiBalancer appliance and the appliance which you are currently synchronizing from.

History

Select the “**History**” sub tab [g], and the page will display all synchronization events related to the current FortiBalancer appliance being configured in the box [h].

The screenshot shows the Fortinet Admin Tools interface for Synchronization. The top navigation bar includes tabs: View, Backup, Load, Clear, Synchronization, Synchronization Sdms, and Command Timeout. Below this is a sub-tab bar with Nodes/Peers, Tasks, Results, Differences, and History. The 'Results' sub-tab is selected, indicated by annotation 'a'. The main content area displays 'SYNCHRONIZATION RESULTS' with a table containing one row: '1', 'node1', '172.16.63.2', and 'Peer Node'. An annotation 'b' points to this table. To the right of the table is a 'View Synch Summary' link, annotated with 'c'. An orange arrow points from the table to a 'CONFIG SYNCH RESULTS FROM OTHER' section, annotated with 'd'. This section has a sub-tab bar with Nodes/Peers, Tasks, Results, Differences, and History. The 'Differences' sub-tab is selected, indicated by annotation 'e'. The main content area displays 'SYNCHRONIZATION DIFFERENCES' with a table containing one row: '1', 'node1', '172.16.63.2', and 'Peer Node'. An annotation 'f' points to this table. Below this is a 'HISTORY OF SYNCH EVENTS INITIATED ON THIS NODE/PEER' section, annotated with 'g'. This section has a sub-tab bar with Nodes/Peers, Tasks, Results, Differences, and History. The 'History' sub-tab is selected, indicated by annotation 'h'. The main content area displays a list of synchronization events: 'Fri Jan 9 17:15:52 GMT 2009 | 10.3.58.4 | sync to' and 'Fri Jan 9 17:15:52 GMT 2009 | 10.3.58.4 | error missing license key'.

Synchronization Sdns

The SDNS Synchronization feature of the FortiBalancer appliance allows administrators to synchronize SDNS configurations and BIND 9 zone files except SDNS member configurations from a FortiBalancer appliance to its peers.

Select the “**Synchronization Sdns**” tab [a], and the window presents two sub tabs.

Nodes/Peers

Select the “**Nodes/Peers**” sub tab [b]. All peers previously configured will be displayed in the sort ready table [c]. The first step with synchronization is to define the name and IP address for each peer. To do this, you can click on the action link “Add Node/Peer Entry” [d]. In the new configuration window, supply the node/peer name and IP address in the texts fields [e] and click on the “Save” action link [f]. The newly added peers will be displayed in the sort ready table [c].

Tasks

Select the “**Tasks**” sub tab [g]. The configuration window will display all configured peers in the table under “Configuration Synchronization” [h]. Select a desired node or peer in the table and click on the “Synchronization” action link [i] to begin synchronizing.

The screenshot shows the FortiBalancer SDNS Synchronization Sdns interface. It features a top navigation bar with tabs: View, Backup, Load, Clear, Synchronization, Synchronization Sdns (selected), and Command Timeout. Below this is a sub-tab bar with Nodes/Peers (selected) and Tasks. The main content area is divided into two sections: SYNCH NODE/PEER CONFIGURATION and ADD NODE/PEER ENTRY. The SYNCH NODE/PEER CONFIGURATION section contains a table with columns: Node/Peer Name, Node/Peer IP, and Node/Peer Type. It lists one peer: peer1 with IP 172.16.63.2, of type Peer Node. The ADD NODE/PEER ENTRY section contains two text input fields: Node/Peer Name and Node/Peer IP, with a note indicating 1 and 32 characters with no space in it. Below this is a CONFIGURATION SYNCHRONIZATION section with a table similar to the one above, also listing peer1. A Synchronize button is located to the right of this table. A note at the bottom states: '* Note: If you change the local configuration by synchronization or rollback, this WebUI session might be terminated. If this happens, you need to use the CLI to enable the WebUI after the config mode timeout (180 seconds).'.

Callouts:

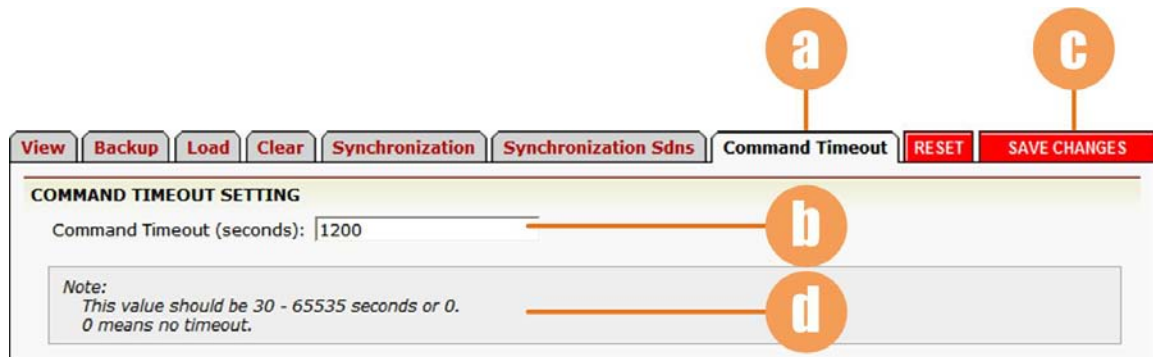
- a**: Synchronization Sdns tab
- b**: Nodes/Peers sub tab
- c**: SYNCH NODE/PEER CONFIGURATION table
- d**: Add Node/Peer Entry link
- e**: Node/Peer Name and Node/Peer IP input fields
- f**: Save button
- g**: Tasks sub tab
- h**: CONFIGURATION SYNCHRONIZATION table
- i**: Synchronize button

Command Timeout

Select the “**Command Timeout**” tab [a], and a new configuration window is displayed.

You can specify the command timeout value (in seconds) in the text field [b]. Remember to click on the “**SAVE CHANGES**” button [c] when it appears to save your configuration.

Please read the notes [d] carefully before you set the timeout value.



The screenshot shows the Fortinet configuration interface for the "Command Timeout" tab. The interface includes a top navigation bar with tabs: View, Backup, Load, Clear, Synchronization, Synchronization Sdns, Command Timeout (selected), RESET, and SAVE CHANGES. Below the tabs, the "COMMAND TIMEOUT SETTING" section contains a text field for "Command Timeout (seconds)" with the value "1200". A note below the field states: "Note: This value should be 30 - 65535 seconds or 0. 0 means no timeout." Callouts are placed as follows: 'a' points to the "Command Timeout" tab, 'b' points to the text field, 'c' points to the "SAVE CHANGES" button, and 'd' points to the note box.

Graph

Make certain you are in **Config mode** and have selected the Graph feature link from the sidebar [a]. The configuration window presents four tabs [b].

Logging

Under the “**Logging**” tab, there are five sub tabs [c]. The **General** page is displayed by default [d].

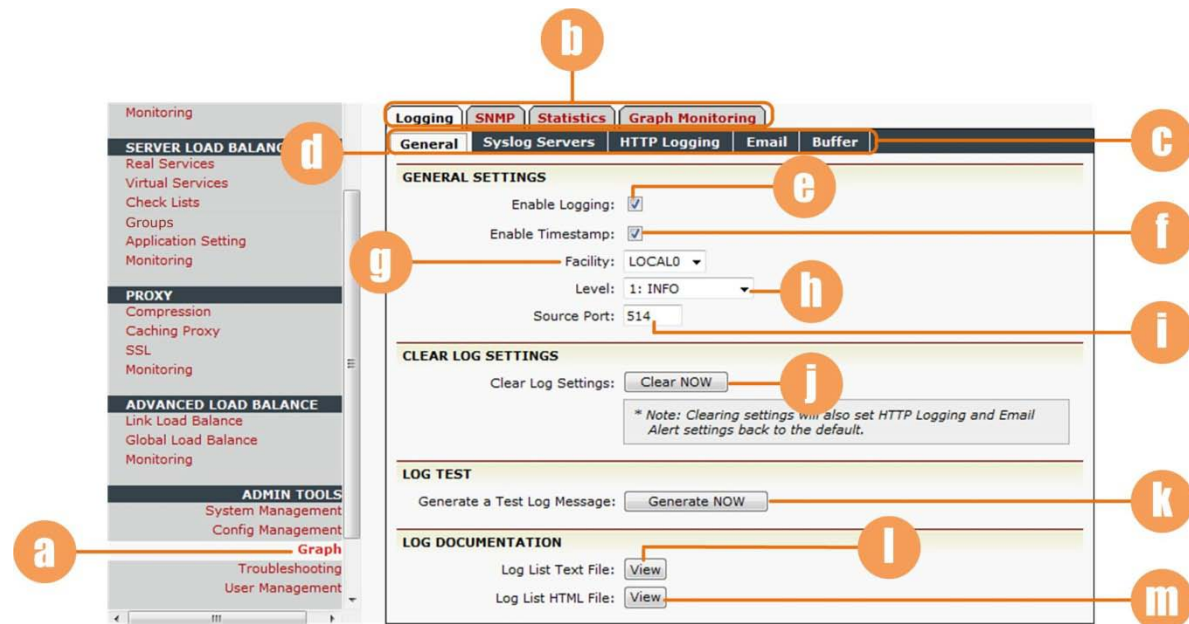
General

Enable the logging feature via the check box [e], and enable the timestamp feature for log entries via the check box [f]. Set the facility from LOCAL0 to LOCAL7 via the selector [g], and set the log level (any message below the specified level will be ignored) via the selector [h]. Set the source port in the text field [i].

You can reset the log setting by clicking on the “Clear NOW” button [j]. Note that this operation will set log setting to the default.

You can generate a test log message by clicking on the “Generate NOW” button [k].

You can view the log list text file or HTML file by clicking on the “View” buttons [l] and [m] respectively.



Logging (Continue)

Syslog Servers

Select the “**Syslog Servers**” sub tab [a]. The log host is the remote Syslog server receiving messages. Up to three servers may be configured (all messages will be sent to all servers). The host port number defaults to 514.

To add a Syslog server, click on the action link “Add Server Entry” [b]. In the new window, set the server host IP, logging protocol, host port and host ID [c]. Then, click on the “Save” action link [d]. The configuration will be displayed in the sort-ready table [e].

You can also configure HTTP log filters to filter undesired logs. To add a log filter, click on the action link “Add” [f]. In the new window, select the server ID, set the filter ID and input the filter string [g]. Then, click on the “Save” action link [h]. The configuration will be displayed in the sort-ready table [i].

HTTP Logging

Select the “**HTTP Logging**” sub tab [j]. You can enable or disable HTTP logging and further set the format via the radio buttons [k]. You can also select to include the VIP and Host in log reports via the check boxes [l]. Then, click on the “Apply” action link [m] to make the configuration take effect.

The screenshot displays the Fortinet Admin Tools interface with several configuration steps highlighted by orange callouts (a-m):

- a**: Select the **Syslog Servers** sub tab.
- b**: Click the **Add Server Entry** action link.
- c**: In the **ADD SERVER ENTRY** window, configure Host IP, Protocol (UDP), Host Port (514), and Host ID (0).
- d**: Click the **Save** action link.
- e**: The configured server entry is displayed in the **REMOTE SYSLOG SERVER CONFIGURATION** table.
- f**: Click the **Add** action link in the **HTTP LOG FILTER CONFIGURATION** section.
- g**: In the **ADD LOG FILTER ENTRY** window, select a Host ID, set a Filter ID (1-3), and input a Filter String.
- h**: Click the **Save** action link.
- i**: The configured filter entry is displayed in the **HTTP LOG FILTER CONFIGURATION** table.
- j**: Select the **HTTP Logging** sub tab.
- k**: Configure HTTP Logging settings, including enabling logging and selecting a format (e.g., Squid).
- l**: Select the **VIP Option** and **Host Option** checkboxes.
- m**: Click the **Apply** action link.

Logging (Continue)

Email

Select the “Email” sub tab [a], and a new configuration page is displayed. You can configure an alert email to report issues. To add an email alert, click on the action link “Add Email Alert Entry” [b] and a new configuration page appears.

Set the log/entry ID in the text field [c], define the message that accompanies the log alert [d] as a message of importance, supply the email address of the recipient [e] and the interval between sending reports (in minutes) [f], and specify the report type via the selector [g]. The report can be either a “data” report or a “count” (number of incidents) report. At last, click on the desired action link [h] to complete configuration.

You can set the “From” header in the mail being sent out via the text field [i], and set the value of the hostname from which the mail is recorded as sent via the text field [j]. Remember to click on “SAVE CHANGES” [k] when it appears to save your configuration.

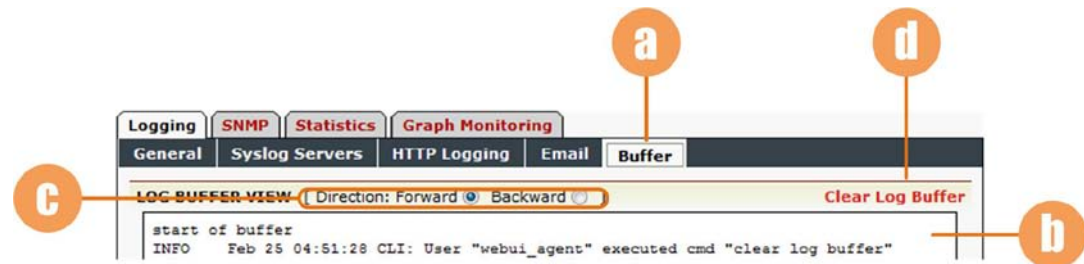
The screenshot displays the Fortinet Admin Tools interface for configuring email alerts. The top navigation bar includes tabs for Logging, SNMP, Statistics, Graph Monitoring, and a sub-tab for Email (labeled 'a'). The Email sub-tab is active, showing the 'EMAIL ALERT CONFIGURATION' page. This page has a table with columns for ID, Regular Expression (String to look for in a message), and Email Address. A table below it is labeled 'SYSTEM EMAIL CONFIGURATION' and contains fields for From: (%h<alert@log.domain>) (labeled 'i'), Host: (%l.alert_pseudo_domain) (labeled 'j'), and a list of format characters for use with above fields. A large orange arrow points from the 'Add Email Alert Entry' link (labeled 'b') to the 'ADD EMAIL ALERT ENTRY' page. This page contains fields for Entry ID: (1 - 32) (labeled 'c'), Regular Expression: look for in a message) (String to) (labeled 'd'), Email Address: abc@xyz.com) (eg: (labeled 'e'), Interval: (0 - 10000 Minutes) (labeled 'f'), and Report Type: data (labeled 'g'). The bottom of the page has action links: Cancel, Save & Add Another, and Save (labeled 'h'). The top right of the interface has buttons for RESET and SAVE CHANGES (labeled 'k').

Logging (Continue)

Buffer

Select the “**Buffer**” sub tab [\[a\]](#) and the configuration window will display a scrolling list [\[b\]](#) (if applicable) of logged events based on the logging configuration to this point. You can set the display order of events in the list via the “Forward” and “Backward” radio buttons [\[c\]](#). Forward means the oldest events are listed on the top, while backward means to display the most recent events on the top.

You may also clear the log buffer by selecting the action link “Clear Log Buffer” [\[d\]](#).



SNMP

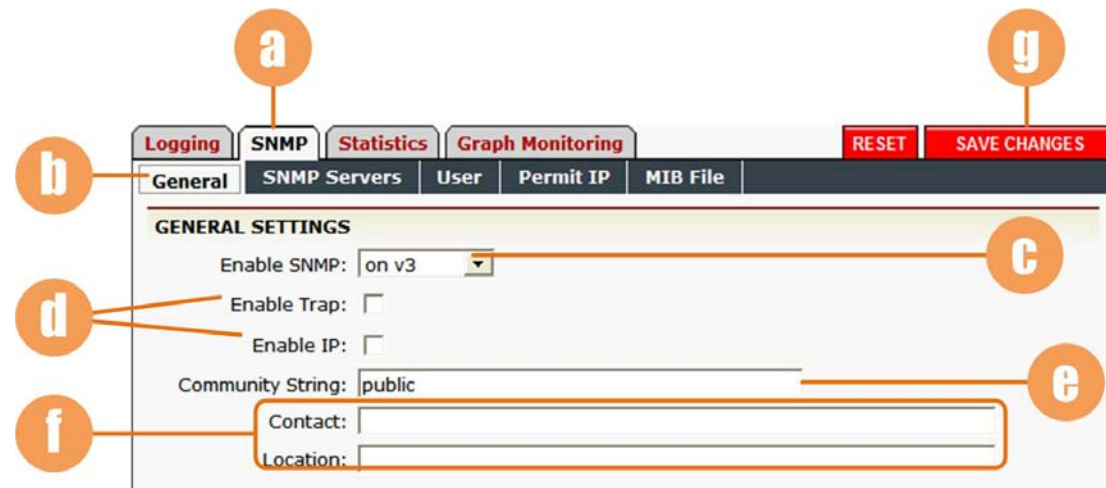
SNMP (Simple Network Management Protocol) is a widely used protocol for network monitoring and control. Data are passed from SNMP agents, which are hardware and/or software processes reporting activity on each network device to the workstation console which oversees the network. At most three SNMP hosts can be configured. Note that SNMP traps must be enabled to view graphs on the FortiBalancer Flight Deck.

Make certain that you are in Config mode and have selected the “SNMP” tab [a]. The window presents five sub tabs. By default, the General page is displayed [b].

General

Enable/disable the SNMP feature via the selector [c]. You can enable the FortiBalancer appliance to send generic and enterprise traps via the “Enable Trap” check box, and enable access control based on the source IP of an SNMP client via the “Enable IP” check box [d]. Define a community string [e] (at most 32 characters) to act as a password to limit or control access from the NMS to the agent. Specify the contact person and FortiBalancer appliance location in the text fields [f] (at most 128 characters for each). Click on the “SAVE CHANGES” button [g] when it appears to save changes made.

Note: For the sake of security, it is strongly recommended to modify the default SNMP community string to avoid possible system information interception.



SNMP (Continue)

SNMP Servers

Select the “SNMP Servers” sub tab [\[a\]](#), and the configuration window will present a list of configured SNMP servers. To add a new entry, click on “Add Server Entry” [\[b\]](#). In the fields provided on the new configuration page, supply the SNMP server IP address [\[c\]](#), specify the SNMP trap version via the selector [\[d\]](#), and supply the community string [\[e\]](#). Complete the configuration by clicking on the desired action link [\[f\]](#). Then, the added entry will be displayed in the table [\[g\]](#).

If you specify the SNMP trap version to be 3 [\[d\]](#), several new parameter fields [\[h\]](#) will appear. Set them properly and click on the desired action link [\[i\]](#). Then, the added entry will be displayed in the table [\[j\]](#). To do this, you can also directly click on the action link add “Add Server Entry” [\[k\]](#).

The screenshot shows the Fortinet Admin Tools interface for configuring SNMP servers. The 'SNMP Servers' sub-tab is selected. The page displays two tables: 'SNMP SERVER CONFIGURATION' and 'SNMP SERVER V3 CONFIGURATION'. Below these tables are two 'ADD SERVER ENTRY' forms. The first form is for Version ID 1, and the second is for Version ID 3. The second form has additional fields for Engine Id, User Name, Security Level, and Authentication Password. An orange arrow points from the 'Add Server Entry' link in the first table to the 'Add Server Entry' form. Orange callout letters a through k point to various elements: a points to the SNMP Servers sub-tab, b points to the 'Add Server Entry' link, c points to the IP Address field, d points to the Version ID selector, e points to the Community String field, f points to the 'Save' button, g points to the first table, h points to the additional fields in the second form, i points to the 'Save' button of the second form, j points to the second table, and k points to the 'Add Server Entry' link in the second table.

SNMP (Continue)

User

Select the “**User**” sub tab [a], and the configuration window will present a list of SNMP V3 users. To add a user, click on the action link “Add User” [b]. In the fields [c] provided on the new configuration page, supply the user name, specify the security level and set the authentication password. Then, click on the desired action link [d]. The added user entry will be displayed in the table [e].

Permit IP

Select the “**Permit IP**” sub tab [f], and the configuration window presents a list of permitted IP addresses. To add an IP address, click on the action link “Add Permit IP” [g]. The window will present a new configuration page. Supply the IP address and netmask [h], and click on the desired action link [i]. Then, the added IP address entry will be displayed in the table [j].

MIB File

Select the “**MIB File**” sub tab [k], and the configuration window will display the user’s MIB file in the box [l] if applicable.

The image displays three sequential screenshots of the Fortinet Admin Tools interface, illustrating the steps to configure SNMP V3 users and permitted IP addresses.

First Screenshot: SNMP V3 USER SETTING

- a**: The **User** sub tab is selected in the top navigation bar.
- b**: The **Add User** action link is located in the top right corner of the configuration window.
- c**: The **ADD USER** form contains fields for **User Name**, **Security Level** (set to **authNopriv**), and **Authentication Password**.
- d**: The **Save** action link is located in the bottom right corner of the form.
- e**: A table below the form displays the list of configured SNMP V3 users.

Second Screenshot: SET PERMIT IP ADDRESS

- f**: The **Permit IP** sub tab is selected in the top navigation bar.
- g**: The **Add Permit IP** action link is located in the top right corner of the configuration window.
- h**: The **ADD PERMIT IP** form contains fields for **IP Address** and **Netmask**.
- i**: The **Save** action link is located in the bottom right corner of the form.
- j**: A table below the form displays the list of configured permitted IP addresses.

Third Screenshot: CUSTOM MIB FILE VIEW

- k**: The **MIB File** sub tab is selected in the top navigation bar.
- l**: The **CUSTOM MIB FILE VIEW** text area displays the MIB file content for the selected user.

Statistics

Make certain that you are in **Config mode** and have selected the “**Statistics**” tab [a]. The configuration window will present four sub tabs, the default sub tab is “**IP**” [b].

IP

Select the “**IP**” sub tab to view the IP statistics. You can enable/disable the collection of IP statistics via the check box [c]. Then, click on the “**SAVE CHANGES**” button [d] when it appears. The IP statistics info will be displayed in this area [e], you can click on the “**Clear Statistics**” action link [f] to remove the statistical information about IP addresses.

The screenshot shows the Fortinet Admin Tools configuration window for IP Statistics. The window has tabs for Logging, SNMP, Statistics, and Graph Monitoring. The Statistics tab is active, showing sub-tabs for IP, SSL, System/CPU, and TCP. The IP sub-tab is selected. A table displays IP statistics for host FBL, including IP address, Pkts In, Bytes In, Pkts Out, Bytes Out, and Start Time. A 'Clear Statistics' link is visible in the top right of the statistics area.

IP	Pkts In	Bytes In	Pkts Out	Bytes Out	Start Time
172.16.85.40	6730	868801	5138	7794527	02/25/11 08:01
Total:	6730	868801	5138	7794527	

Statistics (Continue)

SSL

Select the “SSL” sub tab [\[a\]](#) to view SSL statistics. You can clear the SSL statistics by clicking on the action link [\[b\]](#).

System CPU

Select the “System/CPU” sub tab [\[c\]](#) to view system and CPU statistics.

TCP

Select the “TCP” sub tab [\[d\]](#) to view TCP statistics.

The screenshot displays the Fortinet Admin Tools interface with the 'Statistics' tab selected. The page is divided into three main sections, each with its own sub-tab and a corresponding label (a, b, c, d, e) in an orange circle.

- SSL Statistics (a):** This section shows 'SSL Connection Statistics for "sample"' and 'SSL Session Statistics for "sample"'. The connection statistics include: Open SSL connections: 0, Accepted SSL connections: 0, Requested SSL connections: 0, and 5 minutes requested rate: 0 connections/sec. The session statistics show: Resumed SSL sessions: 0. A 'Clear Statistics' link is located at the top right of this section (b).
- System and CPU Statistics (c):** This section shows 'CPU Utilization 1 %', 'Connection/sec 0', and 'Request/sec 0'.
- TCP Statistics (d):** This section shows 'LISTEN: 1' and various TCP state statistics: SYN_SENT: 0, SYN_RCVD: 0, ESTABLISHED: 0, CLOSE_WAIT: 0, FIN_WAIT_1: 0, CLOSING: 0, LAST_ACK: 0, FIN_WAIT_2: 0, and TIME_WAIT: 157.

The sub-tabs at the top of each section are: IP, SSL (a), System/CPU (c), and TCP (d). The 'Clear Statistics' link (b) is located at the top right of the SSL Statistics section.

Graph Monitoring

Make certain you are in **Config mode** and have selected the “**Graph Monitoring**” tab [a], and the configuration window will present three sub tabs.

Graph Monitoring Setting

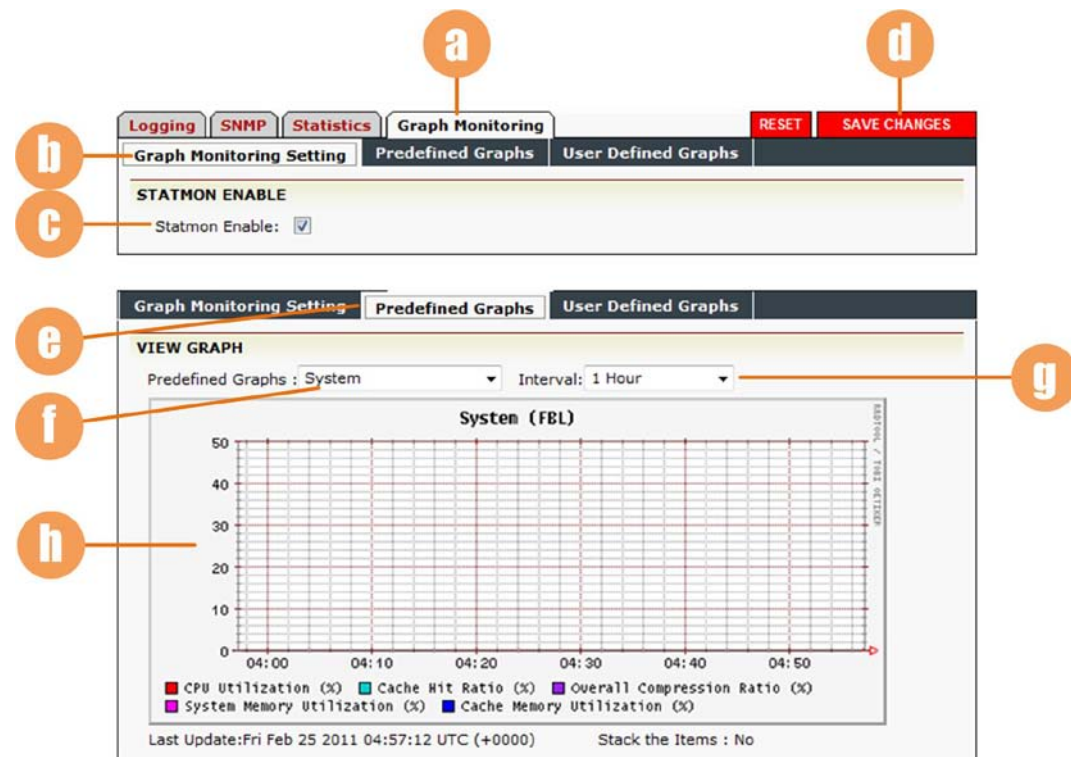
Select the sub tab “**Graph Monitoring Setting**” [b], and the configuration window will present a page where you can enable the Statmon feature via the check box [c]. Remember to click on the “**SAVE CHANGES**” button [d] when it appears to save your configuration.

Note that the **Predefined Graphs** and **User Defined Graphs** pages are available only after the statmon function is enabled.

Predefined Graphs

Select the sub tab “**Predefined Graphs**” [e] and a new configuration window appears. You can view different predefined graphs by selecting from the selector [f]. You can also set the interval via the selector [g].

In different graph types, the numbers on the vertical axis [h] have varied symbols followed with varied meanings. For details, please refer to the right table.



Graph Monitoring (Continue)

Predefined Graphs (Continue)

In the “Predefined Graphs” dropdown list, if one item of the graph types is selected, the number on the vertical axis will have its corresponding symbol followed. For meanings of these symbols, please refer to the right table.

Symbol	Meaning	Symbol	Meaning
a	10e-18 (Ato)	k	10e3 (Kilo)
f	10e-15 (Femto)	M	10e6 (Mega)
p	10e-12 (Pico)	G	10e9 (Giga)
n	10e-9 (Nano)	T	10e12 (Terra)
u	10e-6 (Micro)	P	10e15 (Peta)
m	10e-3 (Milli)	E	10e18 (Exa)
None	Base		

Graph Monitoring (Continue)

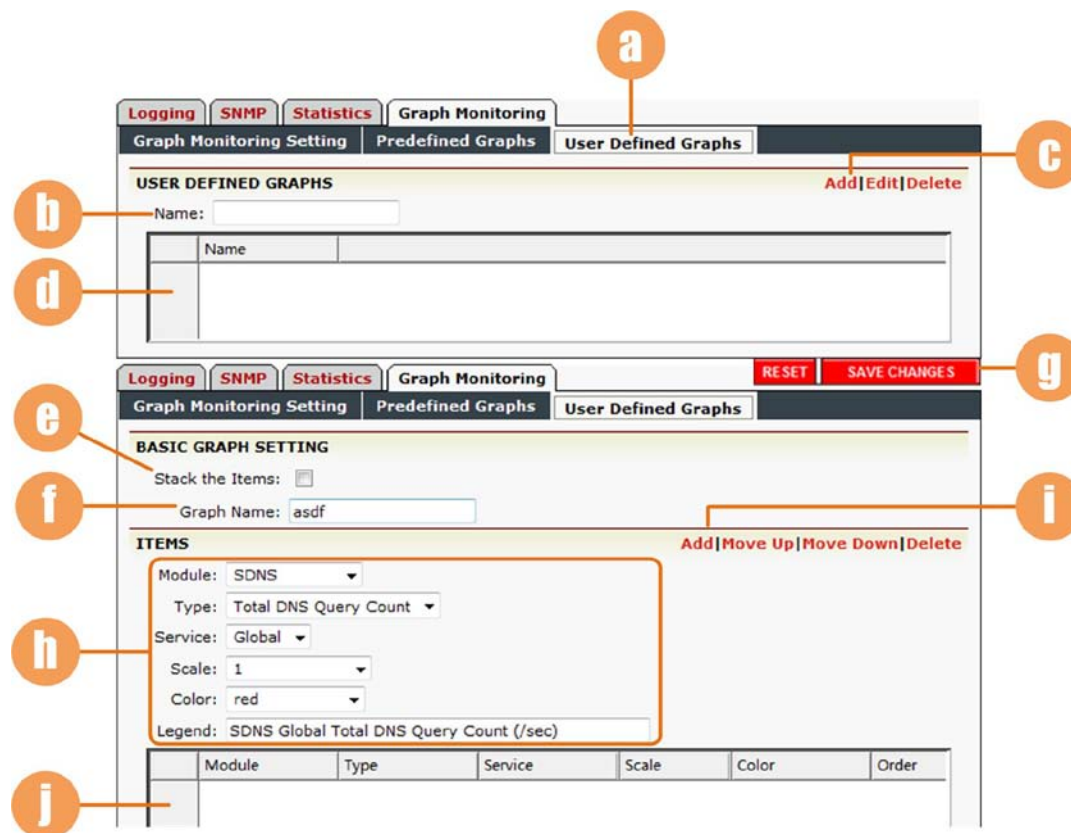
User Defined Graphs

Select the “**User Defined Graphs**” sub tab [a], and the configuration window will present a page allowing you to select to view preferred graphs.

Input a name for your preferred graph in the text field [b], and click on the action link “Add” [c]. Then, the added graph name will be displayed in the list box [d]. You can double click on a name to further define the graph on a new page.

Select the check box [e] to stack the items, and change the graph name if needed in the text field [f]. Then, click on the button [g] when it appears to save changes.

Then, you can define your preferred graph by adding items to the graph through the parameter fields [h]. After setting them properly, click on the action link “Add” [i] and the added module will be displayed in the sort ready table [j].

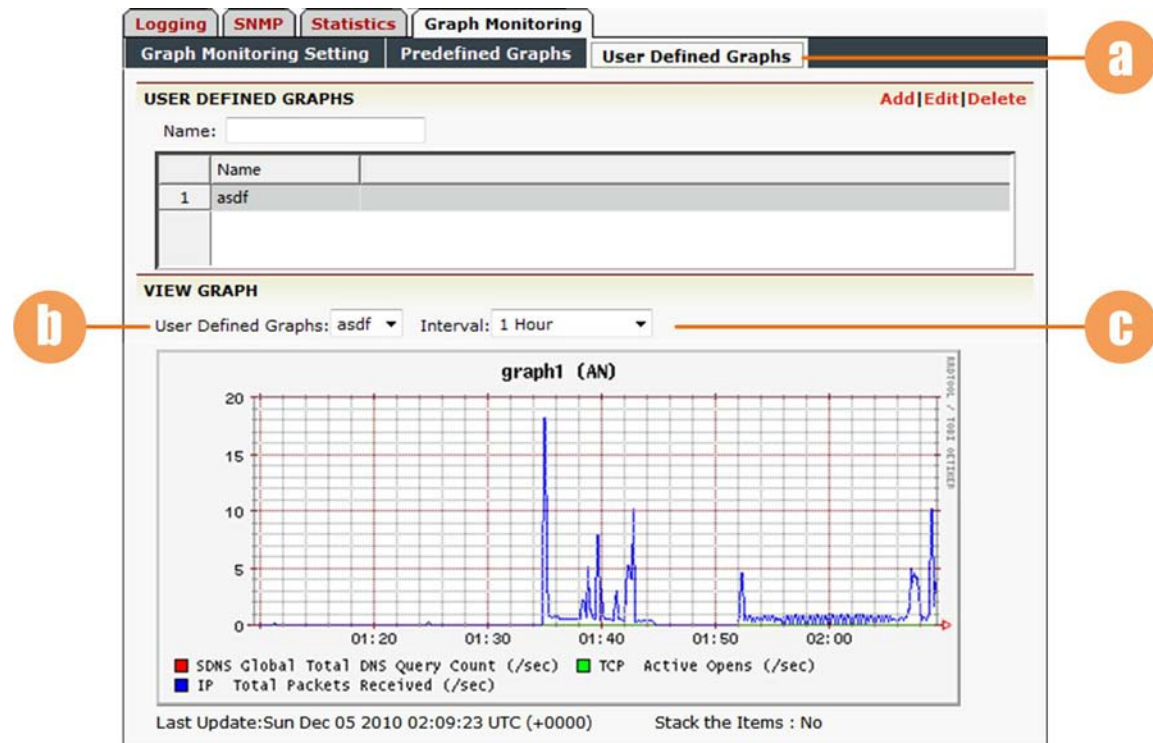


The screenshot shows the Fortinet Admin Tools interface for Graph Monitoring. The top navigation bar includes tabs for Logging, SNMP, Statistics, and Graph Monitoring. Under Graph Monitoring, there are sub-tabs for Graph Monitoring Setting, Predefined Graphs, and User Defined Graphs. The 'User Defined Graphs' sub-tab is selected, indicated by label 'a'. Below the sub-tabs, there is a section titled 'USER DEFINED GRAPHS' with a text field for 'Name' (labeled 'b'), an 'Add|Edit|Delete' action link (labeled 'c'), and a list box (labeled 'd'). Below this is a section titled 'BASIC GRAPH SETTING' with a 'Stack the Items' checkbox (labeled 'e'), a 'Graph Name' text field (labeled 'f'), and 'RESET' and 'SAVE CHANGES' buttons (labeled 'g'). Below the 'BASIC GRAPH SETTING' section is the 'ITEMS' section, which contains a table with columns: Module, Type, Service, Scale, Color, and Order. The table has one row with the following values: Module: SDNS, Type: Total DNS Query Count, Service: Global, Scale: 1, Color: red, and Legend: SDNS Global Total DNS Query Count (/sec). The 'Add|Move Up|Move Down|Delete' action link (labeled 'i') is located to the right of the table. The table itself is labeled 'j'.

Graph Monitoring (Continue)

User Defined Graphs (Continue)

Then, click on “**User Defined Graphs**” [a] again, and you can view your defined graphs on the page. You can further switch among the graphs you have defined via the selector [b], or set the interval as desired via the selector [c].



Troubleshooting

This feature provides simple tools for ping (generate an echo request), packet trace, name server verification and system debugging files exporting.

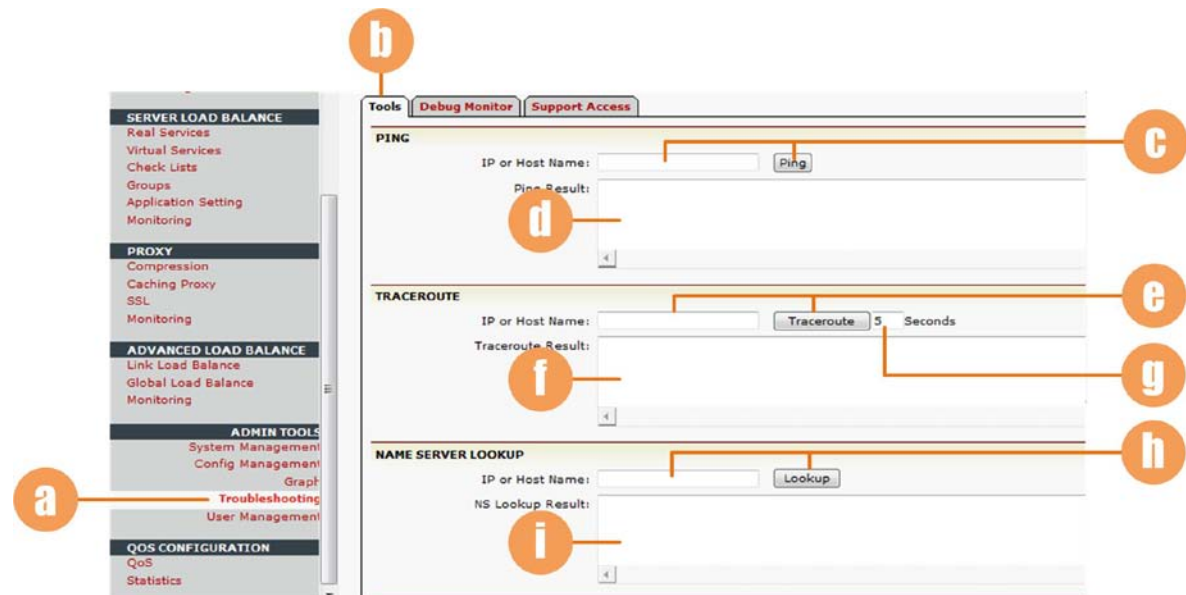
Tools

Make certain you are in Config mode and have selected Troubleshooting from the sidebar [a]. The window will present three tabs. By default, the Tools page is displayed [b].

Ping: To generate a network connectivity echo request directed towards a specified IP address or “ping”, enter the IP address or host name and click on the “Ping” button [c]. The ping result will be displayed in the box [d].

Traceroute: Enter the IP address or host name and click on the “Traceroute” button [e]. The traceroute result will be displayed in the box [f]. Here, you are allowed to set the traceroute timeout value (in seconds, defaults to 5) in the text field [g].

Name server lookup: This feature allows the user to verify the IP address for the given hostname. Enter the IP address or host name for the name server and click on the “Lookup” button [h]. The verification result will be displayed in the box [i].



Tools (Continue)

Build Debug Files: Via this operation, the system will generate four kinds of system debug files which respectively record the system activities information by categories:

sys_snap.tar.gz

sys_log.tar.gz

sys_core.tar.gz

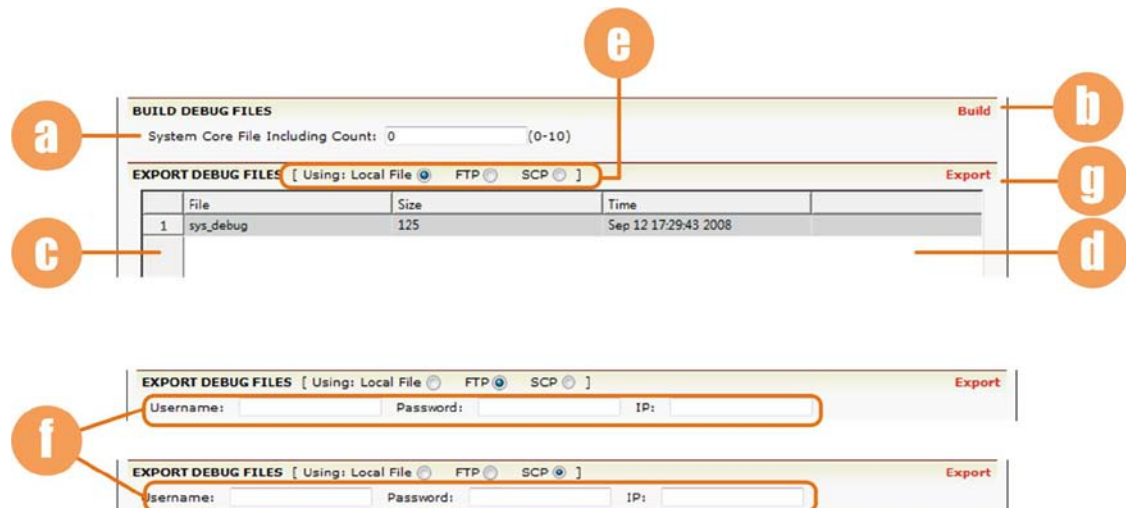
app_core.tar.gz

You can manually generate and obtain these files. First, set the number of the debug files to obtain (0-10, 0 means do not obtain any file) [\[a\]](#), and click on “Build” [\[b\]](#).

After a while, the system debug files obtained successfully will be displayed in the sort ready table [\[c\]](#).

Export debug files: You can export the system debug files via the local file, FTP or SCP method. Select a file to export [\[d\]](#), and specify the export method via the radio buttons [\[e\]](#). For the FTP and SCP method, you need to input the IP address of the FTP or SCP server and the user name and password to access the server [\[f\]](#). Then, click on “Export” [\[g\]](#).

Note: The “sys_debug” system debug file in the list is generated by successively executing the command “debug enable” and “debug disable” via CLI. Users can also export the file here.



BUILD DEBUG FILES

System Core File Including Count: 0 (0-10) Build

EXPORT DEBUG FILES [Using: Local File ☒ FTP ☐ SCP ☐] Export

	File	Size	Time
1	sys_debug	125	Sep 12 17:29:43 2008

EXPORT DEBUG FILES [Using: Local File ☒ FTP ☐ SCP ☐] Export

Username: Password: IP:

EXPORT DEBUG FILES [Using: Local File ☒ FTP ☐ SCP ☐] Export

Username: Password: IP:

Debug Monitor

Select the “**Debug Monitor**” tab [a].

You can enable or disable the debug monitor function via the check box [b], and then click on the “Set” action link [c] to make your configuration take effect. By default, the debug monitor function is enabled.

You can self-define the CLI commands to be executed for monitor purpose in a file, and then import the file via FTP or SCP method. To import the file, input user name, password, IP address of the FTP or SCP server and the file name in the text fields [d], and click on the “Import” action link [e].

After the file is imported successfully, the CLI commands defined in the file will be displayed in the area [f]. The system will execute these commands every 1 minute automatically and further save the monitor data.

You can also export the monitor data via FTP or SCP method. Input user name, password, IP address of the FTP or SCP server in the text fields [g], and click on the “Export” action link [h]. For SCP method, you further need to input the directory path to save the monitor data [i].

The screenshot shows the Fortinet Admin Tools interface for the Debug Monitor configuration. The page has three tabs: Tools, Debug Monitor (selected), and Support Access. The main content area is divided into several sections:

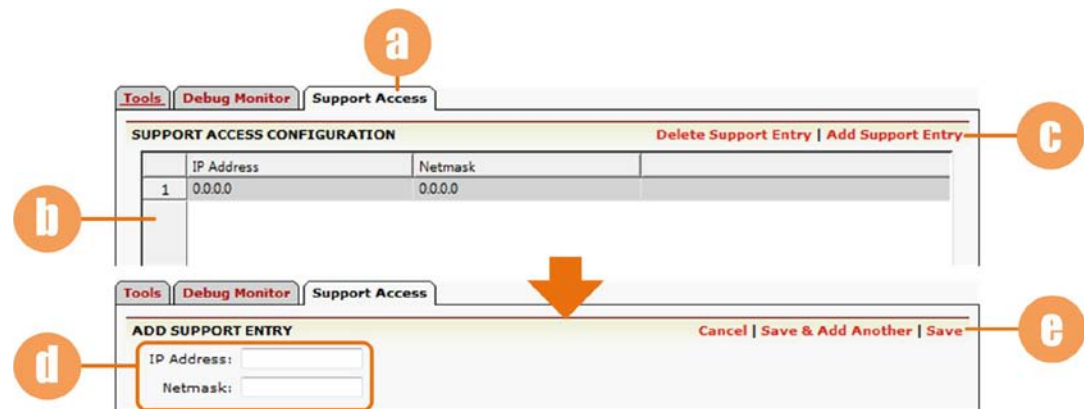
- ENABLE DEBUG MONITOR**: Contains a checkbox labeled "Enable Debug Monitor:" which is checked. To the right of this section is a red "Set" link.
- IMPORT DEBUG MONITOR CLI CONFIGURATION**: Includes radio buttons for "Using: FTP" (selected) and "SCP". To the right is a red "Import" link. Below this are text fields for "Username:", "Password:", "IP:", and "File Name:". This entire section is enclosed in a box labeled 'c'.
- IMPORTED DEBUG MONITOR CLI**: A section for displaying imported CLI commands, labeled 'f'.
- EXPORT DEBUG MONITOR DATA**: Includes radio buttons for "Using: FTP" (selected) and "SCP". To the right is a red "Export" link, labeled 'h'. Below this are text fields for "Username:", "Password:", and "IP:". This section is enclosed in a box labeled 'g'.
- EXPORT DEBUG MONITOR DATA**: A second section for exporting data via SCP, labeled 'i'. It includes the same "Using: FTP" and "SCP" radio buttons, and text fields for "Username:", "Password:", and "IP:". Below these is a "Directory:" text field.

Callouts a-i point to specific elements: [a] points to the Debug Monitor tab; [b] points to the Enable Debug Monitor checkbox; [c] points to the Set link; [d] points to the Username, Password, IP, and File Name fields; [e] points to the Import link; [f] points to the Imported Debug Monitor CLI section; [g] points to the Username, Password, and IP fields of the first Export section; [h] points to the Export link of the first Export section; [i] points to the Directory field of the second Export section.

Support Access

This function allows Fortinet Customer Satisfaction personnel access to the FortiBalancer appliance directly. You should first contact the Customer Satisfaction department at Fortinet before you configure this operation. Select the “**Support Access**” tab [\[a\]](#), and all configured access points are displayed in the sort ready table [\[b\]](#).

To add a support entry, you can click on the action link “Add Support Entry” [\[c\]](#). On the new configuration page, supply the IP address and netmask in the text fields [\[d\]](#) and click on the “Save” action link [\[e\]](#). Then, the entry will be displayed in the sort ready table [\[b\]](#).



User Management

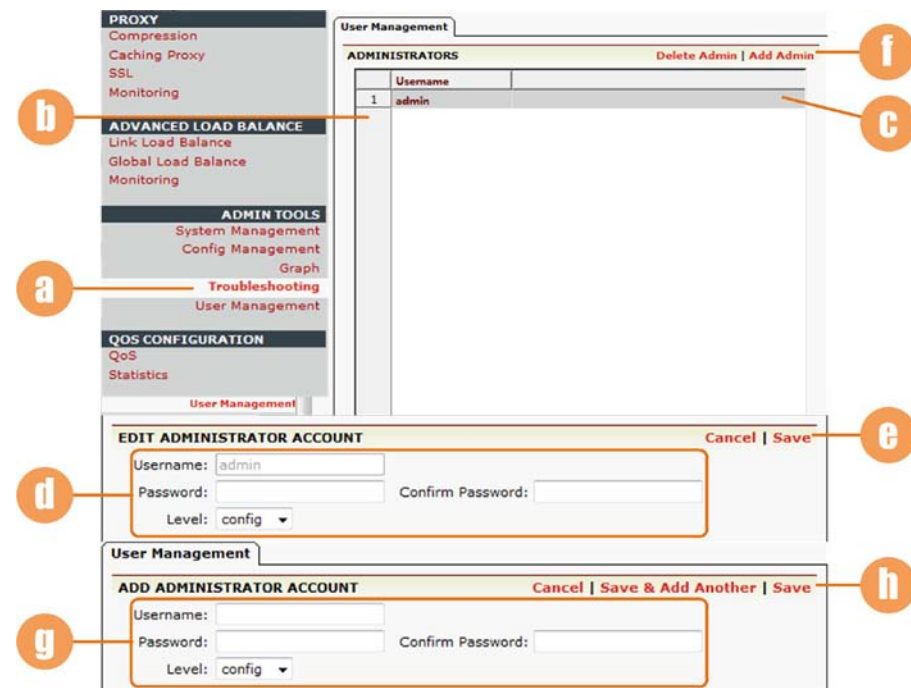
Make certain you are in Config mode and have selected the User Management feature link from the sidebar [a]. The configuration window will display all administrators thus far established in the “Administrators” list [b].

User Management

To edit the account information of an administrator, you can double click on the user name in the list [c], and change the password and user level in the parameter fields and dropdown list [d] as desired on the new configuration page. Then, click on the action link “Save” [e].

Note: The “Username” field does not support special characters like “,;+&#%\$^()!@~*?<>=|\\”. “\$” is just allowed as the final character of the user name.

To add an administrator account, click on the action link “Add Admin” [f], and a new configuration page appears. Set the parameters properly in the text fields [g], and click on the action link “Save” [h]. Then, the newly added administrator will be displayed in the list [b].



QoS Configuration

Quality of Service (QoS) for networks is an industry-wide set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

QoS

QoS enables network administrators to manage TCP, UDP or ICMP flows via queuing mechanism and packet filtering policies. The FortiBalancer appliance has developed a tree-like queue structure.

Make certain you are in Config mode, and have selected the feature link **QoS** from the sidebar [a]. The configuration window will present two new tabs. The QoS Entries page is displayed by default [b].



QoS Entries

When you first enter this page, no QoS entries exist. You need to configure desired QoS queues and filter policies for existing interfaces on your FortiBalancer appliance.

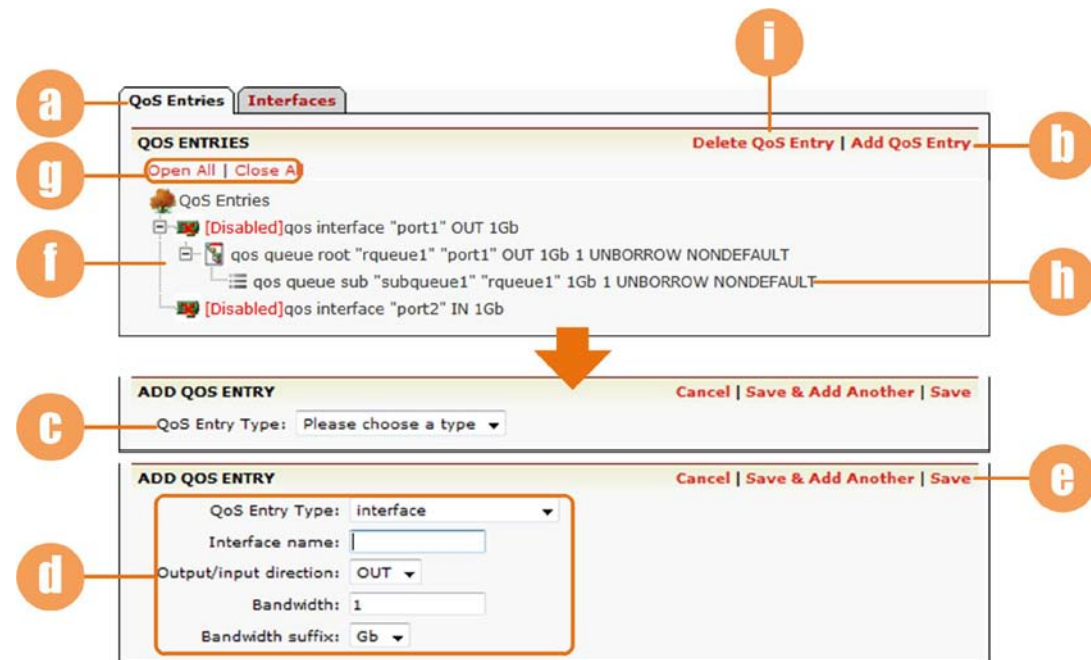
Select the “QoS Entries” tab [a], click on the “Add QoS Entry” action link [b], and a new configuration page appears. Choose an entry type via the selector [c], and new parameter fields will appear [d]. The fields vary with different entry types. Set the fields properly and click on the “Save” button [e].

Note that you have to configure an interface first, and then the root queue, sub queue and filter policy under it.

After you add desired QoS entries, they will be displayed as a QoS tree [f] on the QoS Entries page.

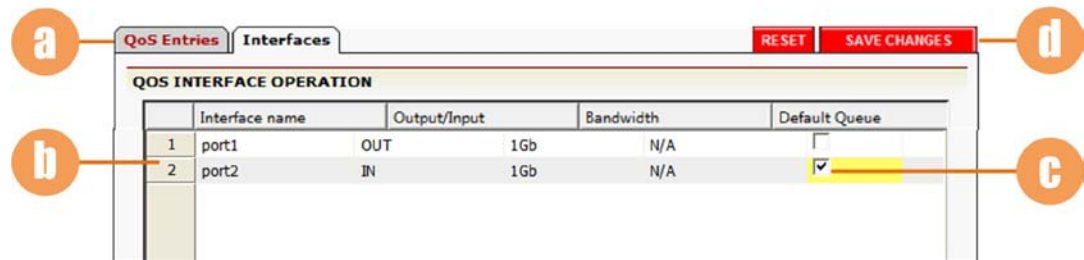
You can click on the action link “Open All” to view all entries, or “Close All” to hide the entries under each QoS interface [g].

To delete an entry from the tree, you can select one [h] and click on the “Delete QoS Entry” action link [i]. Then, all entries under it will be deleted.



Interfaces

Select the “Interfaces” tab [\[a\]](#) and the page will display basic information about the interfaces previously configured on the QoS Entries page in the table [\[b\]](#). You can enable the QoS policies of an interface on OUT or IN direction by selecting the desired check box [\[c\]](#) and clicking on the “SAVE CHANGES” button [\[d\]](#).



QoS Entries		Interfaces		RESET		SAVE CHANGES	
QOS INTERFACE OPERATION							
	Interface name	Output/Input	Bandwidth		Default Queue		
1	port1	OUT	1Gb	N/A	☐		
2	port2	IN	1Gb	N/A	☒		

Statistics

Select the feature link Statistics from the sidebar [a]. To view the statistics, you only need to enter the Enable mode.

The configuration window will present the QoS Interface Statistic page [b]. You can view the QoS statistics of existing interfaces on either in, out, or both directions.

QoS Interface Statistics

Specify an interface via the selector [c], and further specify a direction (IN or OUT) of the interface from the selector [d], where “ANY” means both the IN and OUT directions. Then the desired interface statistics will be displayed in the table [e]. You can click on the action link “Refresh” [f] to view the latest statistics.

To clear the statistics, you need to enter the Config mode and click on the “Clear” action link [g].

