



WatchGuard®

Firebox® SSL

QUICKSTART GUIDE

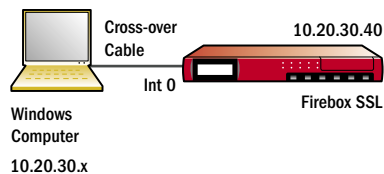
with **CITRIX®** Secure Access

1 Set Up the Firebox[®] SSL Hardware

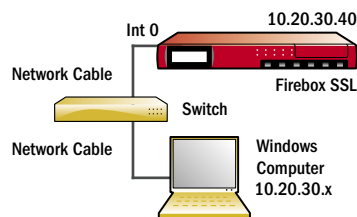
The Firebox[®] SSL server software is pre-installed.

- 1 If your Firebox SSL hard drive is not installed, install the hard drive using the included instructions.
- 2 If you are configuring the Firebox SSL with an Ethernet connection, set your configuration computer to an IP address on the 10.20.30.x network. (The Firebox SSL uses 10.20.30.40, so do not use that address.)
- 3 Connect the power cord to the AC power receptacle.
- 4 Connect the Firebox SSL so you can do the initial configuration. The preconfigured IP address of the Firebox SSL is 10.20.30.40. To change the IP address of the Firebox SSL, refer to "Configuring the Firebox SSL with the Serial Console" after Step 5.

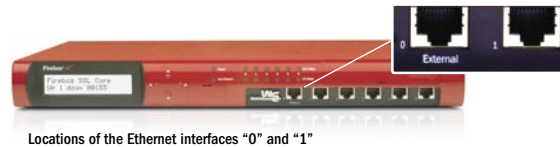
Connecting Directly



Connecting over a Network



- 5 Power on the Firebox SSL.
After the Firebox SSL starts, you can configure the Firebox SSL on your network.



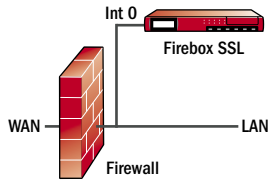
2 Start the Administration Tool

- 1 From a web browser on the computer connected to the Firebox SSL, point to the default IP address of the Firebox SSL (Interface 0):
<https://10.20.30.40:9001>
9001 is the administration port.
- 2 If a Security Alert dialog box appears, click **Yes**.
When prompted, type **root** for username and **rootadmin** for password.
The Firebox SSL Administration Portal appears.
- 3 Click **Launch Firebox SSL Administration Tool**. (If you see a Security Warning dialog, click **Yes** to download the required ActiveX Helper client.)
- 4 When prompted, type **root** for username and **rootadmin** for password.
The Administration Tool opens inside of the **Firebox SSL Admin Terminal** window.

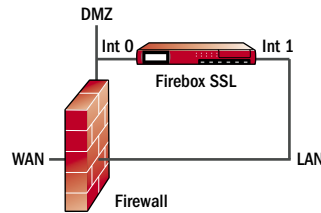
3 Configure the Firebox® SSL for Your Network

- 1 Determine how your Firebox SSL will be connected to your network. The most common configurations are shown.

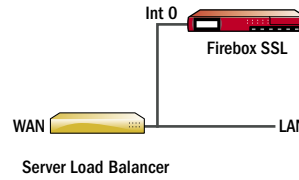
Connected to a LAN behind a firewall



Straddling a firewall



Connected to a LAN behind a server load balancer



- 2 In the Firebox SSL Administration Tool, complete the **General Networking** fields as follows:

If the Firebox SSL will be inside the firewall, select **Use only interface 0**. Type the Firebox SSL internal IP address.

Type the Firebox SSL external IP address or host name (used for NAT).

Type the port to use for VPN connections.

If the Firebox SSL will straddle the firewall, select **Use both interfaces**. Type the IP addresses for Interfaces 0 and 1. Use Interface 0 to connect to your DMZ and use Interface 1 to connect to your LAN.

Type the IP address of the default gateway device, such as the main router, firewall, or server load balancer. This should be the same as the Default Gateway on computers on the same subnet.

- 3 Click **Submit**, but do not restart.
- 4 Go to the **DNS/WINS** tab, specify the DNS server(s), and click **Submit**.
- 5 If the Firebox SSL straddles the firewall and is in front of a router, go to the **Routes** tab. If your site uses RIP, select **Dynamic Routing** so that the Firebox SSL can use your routing tables. Otherwise, you must add the routes necessary for the Firebox SSL to reach the subnets that are not automatically available through your Default Gateway.
- 6 Click the reboot button. Your computer loses the connection to the Firebox SSL.
- 7 Using network cables, connect the Firebox SSL to your network, according to the decision that you made in Step 1 at the start of this section.

You can now open the Administration Tool from any computer with network access to the Access Gateway.

Note:

We recommend that you change the root administrator password to protect your Firebox SSL from unauthorized changes. Open the Firebox SSL Administration Portal (<https://ipAddress:9001>) and go to the **Admin Users** tab.

4

Get and Install Licenses

- 1 To get your licenses, register your appliance on the WatchGuard LiveSecurity® Service Web site at www.watchguard.com/activate and follow instructions on screen.
- 2 To install a license, go to the Administration > Licensing tab and click Browse.
- 3 Navigate to the license file and click Open to upload it.
Note: When you save the Firebox SSL configuration, your license information is included in the backup. We recommend that you retain the original licenses in the event that you are unable to restore the configuration.

5

Test Your Configuration

- 1 Create a test user:
 - In the Administration Tool, go to the **Authentication and Local Users > Local Users** tab and add a user. By default, this user has full network access.
- 2 To verify that you can establish a VPN tunnel to the Firebox SSL:
 - Use a browser to view the Firebox SSL external IP address: **https://externalIP**.
 - You are prompted to authenticate and then you see the Access Portal page.
 - Click **My own computer**.
- 3 In the File Download window, click **Open**. Enter your user name and password, and then click **Connect**. The Secure Access icon displays in the system tray, indicating a successful connection.
You have now completed the initial configuration.

Configuring the Firebox SSL with the Serial Console

- 1 The Firebox SSL serial console is useful for troubleshooting and for quick configuration of Interface 0. Connect the null-modem cable to the 9-pin serial port on the Firebox SSL and connect the cable to a computer that is capable of running terminal emulation software.
- 2 On the computer, start a terminal emulation application. For example, start HyperTerminal.
- 3 Set the serial connection to 115200 bits per second, 8 data bits, no parity, 1 stop bit. Hardware flow control is optional.
- 4 Power on the Firebox SSL. The serial console appears on the computer terminal after the Firebox SSL has started.
- 5 In the serial console, type the default login **root** and the default password **rootadmin**. (If you have already changed the administrator credentials using the Administration Tool, type those credentials instead.)
 - To set the IP address/netmask and the default gateway device for Interface 0, type **0** and press **Enter** to choose Express Setup. After you respond to the prompts, the information you typed appears. To commit your changes, type **y**; the Firebox SSL restarts.
 - To verify that the Firebox SSL can ping a connected network device, type **1** and the IP address of the device.
- 6 If you need to configure the Firebox SSL, connect the Firebox SSL to a Windows computer using one of the setups described in section 1, and power up the Firebox SSL. Continue the configuration starting with section 2.

More About Configuration

Firewall Configuration

Configure your firewall so that port 443 is opened for the external IP address of the Firebox SSL. Map the external IP address of the Firebox SSL to its internal IP address.

Firebox SSL Configuration

Please refer to the *Firebox SSL Administration Guide* for information on configuration options.

Configuration Task	Tab in Administration Tool
<ul style="list-style-type: none">Specify failover servers	Networking
<ul style="list-style-type: none">Enable split tunneling, split DNS, session timeoutSpecify networks that the Firebox SSL can accessDeny access to users with no ACLEnable internal failover for the VPN Remote clientForce user re-login and enable single sign-on	Global Policies
<ul style="list-style-type: none">Set up realms corresponding to authentication serversUse an LDAP server for group authorizationCreate local users and assign local users to groups	Authentication and Local Users
<ul style="list-style-type: none">Define the resource groups used to create per-group Access Control Lists (ACLs)	Network Resources
<ul style="list-style-type: none">Load portal pages used to customize group access	Portal Page Configuration
<ul style="list-style-type: none">Define host check rules used to create per-group policies	Host Checks
<ul style="list-style-type: none">Define shared network resources for kiosk sessions	Share Mounts
<ul style="list-style-type: none">Create and manage groups and group-based policies	User Groups
<ul style="list-style-type: none">Determine group priority when group-based policies are applied to a user who belongs to multiple groups	Group Priority

WatchGuard Support

support@watchguard.com
866.382.2171 (toll-free within the USA)
408.382.4941 (outside the USA)



ADDRESS:

505 Fifth Avenue South, Suite 500
Seattle, WA 98104-3892

E-MAIL:

information@watchguard.com

U.S. SALES:

1.800.734.9905

FAX:

+1.206.521.8342

WEB:

www.watchguard.com

INTERNATIONAL SALES:

+1.206.613.0895



WatchGuard Technologies, Inc. All rights reserved. WatchGuard, Firebox, LiveSecurity and the WatchGuard logo are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks are the properties of their respective owners. P.N. 2241-001 WGPE66271_0605

