

AutumnTECH Spam Fighting Hardware Appliance

Quick Setup and Installation Guide

Overview

The Spam Fighting Hardware (SFH) series by AutumnTECH is self-contained antispam, antivirus, and Internet content filtering hardware that installs at the perimeter of the corporate network. This approach protects by blocking significant amounts of spam and e-mail attached viruses, before they reach the corporate messaging system. This isolation greatly improves system and application confidentiality, integrity, and availability.

The SFH series appliance filters for and will correctly identify spam using the latest techniques, blocks over 100,000 e-mail viruses and phishing scams, and prevents unauthorized Internet access requests. The SFH series has no user limit licensing requirement, is self-updating, and requires minimum administration.

Requirements

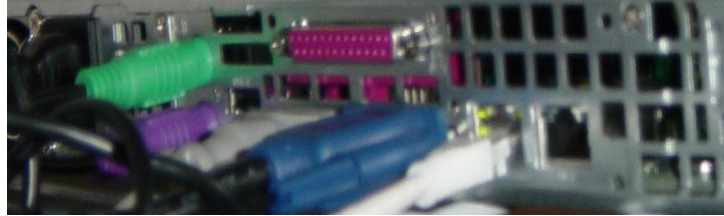
- AutumnTECH SFH Series Appliance
- User Manual Available Online:
www.autumntech.com/Autumntech_SFH_Series_User_Manual.pdf
- A running TFTP/FTP server. A freeware TFTP version is available at:
www.solarwinds.net
- A running Syslog server. A freeware version is available at:
www.kiwisyslog.com
- A SSH client. A freeware version is available at:
<ftp://ftp.autumntech.com/putty.exe> or search the web for: PuTTY

SFH Series Appliance Installation

1. Install the appliance in an environmental controlled room. Appliance should be mounted in a standard 19" equipment rack or placed on a shelf. Care should be taken to keep all chassis ventilation holes free and clear of obstruction. Hardware is included to physically secure appliance to rack or shelf. An optional complete rack mount kit is available for purchase at <http://www.Autumntech.com>
2. Attach a video monitor and keyboard to the back of the appliance. This will allow you to view startup information.

3. Plug in the provided power cable. The appliance should be plugged into an uninterrupted power supply with adequate battery backup and surge protection.

4. Attach a 10/100/1000 MB CAT5 cable to the Ethernet port **closest** to the power supply. This port is the active communication port. The Ethernet port to the right is not used. Attached a monitor and keyboard if available.



5. Use the appliance front panel and the button to the far right to start the appliance. If you correctly attached the console cable as described above, you should see appliance startup information in the console window.

SFH Series Appliance Configuration

SFH Series Appliance will start with the following network instructions:

- Internet Protocol (IP) address: 192.168.200.254
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.200.1
- DNS Servers: 192.168.200.5

Changing the network information is performed with Webtivity. Webtivity is a web-based management utility. Webtivity is used to configure all of the features of SFH Series Appliance, as-well-as used to review reports and update SFH Series Appliance.

Changing the default network information

Open a web browser; use the following information to access Webtivity:

Address/URL: **https://192.168.200.254**
Username: **admin**
Password: **password**





If you are having problems accessing Webtility, check that the appropriate network routes are created. For example, at a Windows command prompt the following command will temporarily add a route to the default Webtility network:

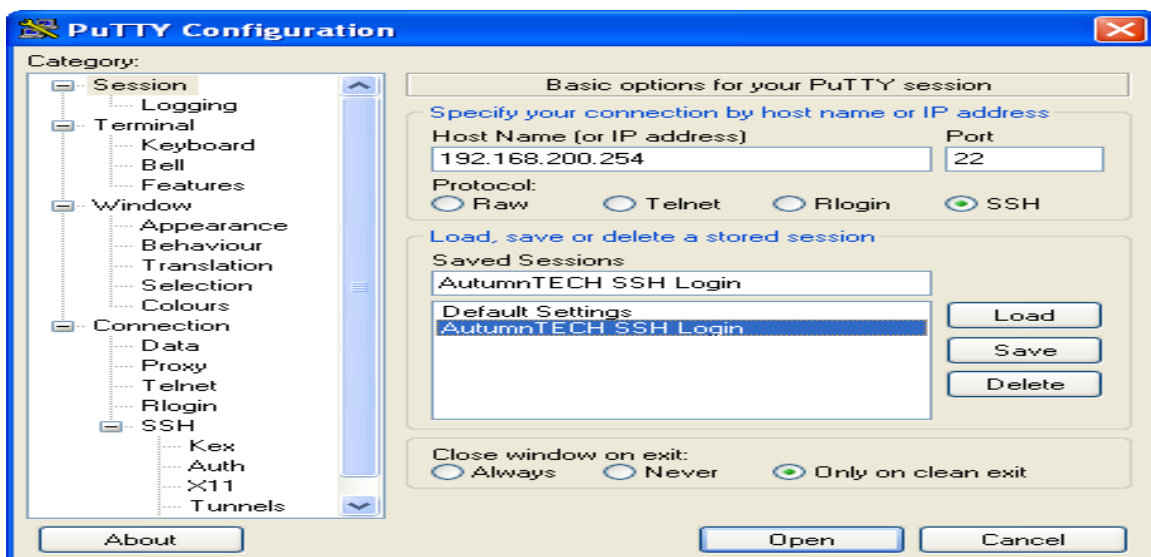
route add 192.168.200.0 mask 255.255.255.0 <your computer's IP address here>

Hit <Enter> to add the route

Issue a **route print** <Enter> to verify the above default network was created.

In the same command window, issue a **ping 192.168.200.254** <Enter> to verify connectivity.

With Webtility open, click the General Tab > Network Settings Tools. Follow the instructions on this page. Submit your changes. Changes will take effect during the next reboot. To reboot the appliance, click the General Tab > Reboot or Halt System. Click Reboot System button. Rebooting SFH Series Appliance takes approximately two minutes.



Changing the default Webtility and SFH Series Appliance Console Passwords

Open Webtility, select General > Update Passwords. In demo mode, console has been disabled and root and spam's passwords have been changed from their default. Thus, changing root and spam's password are not applicable. In registered mode, you will need to establish a SSH session to SFH Series Appliance to change root and spam's passwords. To establish a SSH session, open a SSH client, create a new session to SFH Series Appliance using the following information (we assume here you're using PuTTY):

Hostname/IP address:	Use the network information assigned above
Protocol:	SSH
Protocol Version:	2

Click “Open”, accept Security Alert, when asked for login information and use the following:

Username: **root**
Password: **password**

You should now be at “#” command prompt; indicating that you’re now root.

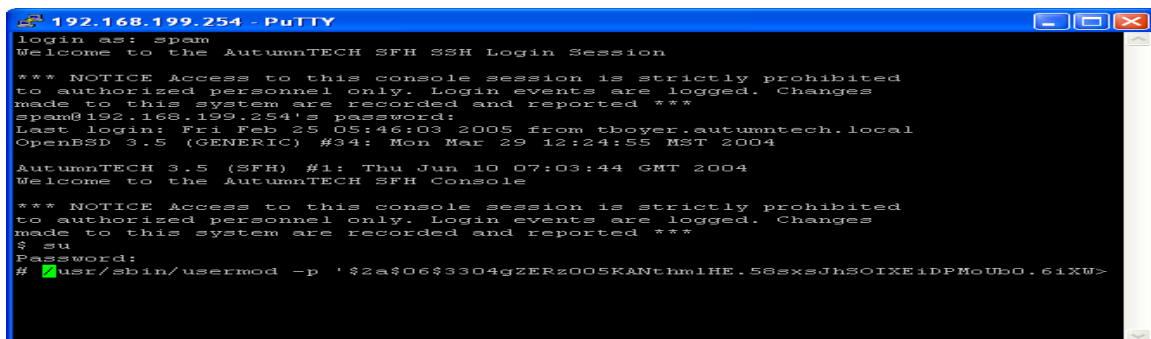
Return to Webtivity, use the password form to create an encrypted password value that will be pasted into your SSH “#” session. Create a new root password, hit “Generate.” The result screen will include a string value in-between two horizontal bars. Copy the value to your clipboard (highlight and hit Ctrl V to copy). Return to your SSH window, at the “#” prompt, click the right mouse button to paste the string value. Hit <Enter> to change root’s password.

General

General : Password Update Tool : Hash Result

Cut-and-paste the result below into your serial console session. You must be logged in as root to update passwords.

```
_____  
/usr/sbin/usermod -p '$2a$06$3304gZERa005KAnHm1HE.58xsxJhSOIXEiDPMoUb0.6iXUhrYr12' root  
_____
```



```
192.168.199.254 - PuTTY  
login as: spam  
Welcome to the AutumnTECH SFH SSH Login Session  
*** NOTICE Access to this console session is strictly prohibited  
to authorized personnel only. Login events are logged. Changes  
made to this system are recorded and reported ***  
spam@192.168.199.254's password:  
Last login: Fri Feb 25 05:46:03 2005 from tboyer.autumntech.local  
OpenBSD 3.5 (GENERIC) #34: Mon Mar 29 12:24:55 MST 2004  
AutumnTECH 3.5 (SFH) #1: Thu Jun 10 07:03:44 GMT 2004  
Welcome to the AutumnTECH SFH Console  
*** NOTICE Access to this console session is strictly prohibited  
to authorized personnel only. Login events are logged. Changes  
made to this system are recorded and reported ***  
# su  
Password:  
# █usr/sbin/usermod -p '$2a$06$3304gZERa005KAnHm1HE.58xsxJhSOIXEiDPMoUb0.6iXW>
```

The procedure to change spam’s password is exactly the same as root’s, instead using the spam password field. When root and spam’s passwords have been change, you can close your SSH session to SFH Series Appliance.

Return to the Webtivity window. Use the password form, to change the default Webtivity admin access password. Once submitted, this password takes effect immediately. You will be prompted for the new admin password before returning back to Webtivity.

Setting up SFH Series Appliance E-mail Relay Domains

By default, the SFH Series Appliance **will not** relay e-mail sent from anyone to anywhere. The default installation is not useful until you configure acceptable domains to relay e-mail for and the mail system that is the final destination for those domains. To configure the domains to relay e-mail for, open Webtivity and Select Advanced > Update the E-mail Engine's Relay Lists. Follow the instructions found on this page. To create

final destination mail delivery, click Advanced > Final Destination and Delivery E-mail Server Settings. SFH Series Appliance can use internal DNS nameservers (method is called Split or Horizon DNS) and their associated zone files and MX records to locate final mail system destinations. In addition, SFH Series Appliance can be configured to use its own lookup engine to locate final mail system destinations. Follow the instructions found on the page and the user's manual for detailed instructions.

Setting up the SFH Series Appliance Syslog Logging Output

SFH Series Appliance generates and reports real-time data about e-mail traffic and other system information by sending syslog data to a running syslog server. We assume you've installed and tested a syslog daemon and have it configured to accept logging traffic from SFH Series Appliance. Open Webtility, select General > Logging Settings. Change the default IP address of 192.168.200.3 to the IP address or hostname running syslog in your network. Once changed, review the syslog window for logging information. If no logging information is displayed, make sure the syslog service is started.

Setting Up SFH Series Appliance E-mail Report Notification

Open Webtility, select General > E-mail Notifications. Add e-mail addresses, one per line to send daily, weekly, and monthly e-mail, spam, and virus reports.

A Note About Greylisting

Greylisting is a new method of blocking significant amounts of spam at the mailserver level, but without resorting to heavyweight statistical analysis or other heuristical (and error-prone) approaches. Consequently, implementations are fairly lightweight, and may even decrease network traffic and processor load on your mailserver.

Greylisting relies on the fact that most spam sources do not behave in the same way as "normal" mail systems. Although it is currently very effective by itself, it will perform best when it is used in conjunction with the other forms of spam prevention included in the appliance.

The term Greylisting is meant to describe a general method of blocking spam based on the behavior of the sending server, rather than the content of the messages.

When the appliance is configured to accept e-mail for your domain, each and every single connection from that point forward is subject to the Greylisting rule. The rule states that you will temporarily fail the first connection by a sender's IP address. You will allow the sender if they resend the message in a timeframe defined by the appliance threshold rule. To configure the threshold, or to disable Greylisting, open Webtility > General > System Startup Settings.

Establishing Bayesian Training "Spam" and "NotSpam" E-mail Aliases

The ability to “train” SFH Series Appliance with messages your organization designates as spam or not, is one of the most powerful features of SFH Series Appliance. This is accomplished by setting the training e-mail addresses in Webtivity. Click Advanced > Update Spam Engine Settings. These e-mail addresses are then added to your Global Address Book inside of your mail system. When a message arrives that is spam and is not tagged spam (false-negative), forward the message to the “Spam” mailbox contact. If a message arrive that’s tagged spam that is not spam (false-positive), forward the message to the “Not Spam” mailbox contact.

Backup and Restoring SFH Series Appliance

Included in Webtivity is a tool for backing up and restoring a SFH Series Appliance snapshot. We assume you’ve installed and tested a TFTP server and have configured it to accept backup and restore requests from the SFH Series Appliance application. From Webtivity, select General > Backup tools. Instructions are found on this page for backup and restore procedures.

Updating SFH Series Appliance

AutumnTECH will periodically create new revisions to SFH Series Appliance and Webtivity. These updates are available for download through the Webtivity > Updates screen. Demo users can requests updates by e-mail, registered users receive an update username and password. Use this information and the instructions found on this screen to update SFH Series Appliance.

**** Important Notes about Starting and Stopping SFH Series Appliance ****

SFH Series Appliance is started from the power button on the appliance and halted in Webtivity. Failure to properly shutdown will cause inconsistencies in the filesystem which may not be recoverable.

**** ALWAYS HALT REBOOT THE SFH SERIES APPLIANCE IN WEBTILITY ****

Congratulations!

At this point SFH Series Appliance is ready to accept and filter e-mail. In addition to the settings defined above, you will need to make some network related modifications too. First, familiarize yourself with the user manual and the rest of the Webtivity screens. You **must** have a thorough understanding of SFH Series Appliance and how it handles e-mail traffic before going “live.”

Train your end users! SFH Series Appliance can be configured with the tightest of restrictions which can cause confusion in your end-user population. Inform your users of this application and its impact on e-mail arriving in their mailboxes.

When you're ready to go live, update your firewall's access control rules to forward e-mail traffic to SFH Series Appliance. Instructions for performing this request are beyond the scope of this document. With the syslog server running, you should begin to see real-time output from e-mail traffic directed at the SFH Series Appliance.

How to receive support

If you experience problems running SFH Series Appliance, contact AutumnTECH support by any of the following methods:

Phone: 301-498-7654

Fax: 301-498-6543

E-mail: Support@AutumnTECH.com

Web: www.AutumnTECH.com