HP SECPATH5000FS_5000FC-CMW520-R3811P10 Release Notes

© Copyright 2017 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.
The information in this document is subject to change without notice.

Contents

List of Tables

This document describes the features, restrictions and guidelines, open problems, and workarounds for version R3811P10. Before you use this version in a live network, back up the configuration and test the version to avoid software upgrade affecting your live network.

Use this document in conjunction with *HP 5000FS_5000FC-CMW520-R3811P10 Release Notes (Software Feature Changes)* and the documents listed in "Related documents."

Version information

Version number

Comware software, Version 5.20, Release 3811P10

Note: You can see the version number by using the command **display version** in any view. Please see **Note 1**.

Version history

IMPORTANT:

The software feature changes listed in the version history table for each version are not complete.

To obtain complete information about all software feature changes in each version, see the Software Feature Changes document for this release notes.

Version history

Version number	Last version	Release date	Release type	Remarks
5000FS_5000FC-CMW520-R3811P10	R3811P09	2017-09-26	Release version	Fixed bugs
5000FS_5000FC-CMW520-R3811P09	R3811P08	2017-04-18	Release version	Fixed bugs
5000FS_5000FC-CMW520-R3811P08	R3811P05	2016-12-26	Release version	None
5000FS_5000FC-CMW520-R3811P05	R3811P03	2015-12-17	Release version	CVE-2015-1788
5000FS_5000FC-CMW520-R3811P03	R3811P02	2015-1-29	Release version	CVE-2014-3566/ CVE-2014-9295
5000FS_5000FC-CMW520-R3811P02	R3811	2014-10-24	Release version	CVE-2014-3508/ CVE-2008-5161
5000FS_5000FC-CMW520-R3811	R3810P04	2014-07-08	Release version	CVE-2014-0224
5000FS_5000FC-CMW520-R3810P04	R3810P02	2014-05-4	Release version	None
5000FS_5000FC-CMW520-R3810P02	R3808	2014-02-12	Release version	None
5000FS_5000FC-CMW520-R3808	First release	2013-08-29	Release version	None

Hardware and software compatibility matrix

CAUTION:

To avoid an upgrade failure, use Table 2 to verify the hardware and software compatibility before performing an upgrade.

Table 1 Hardware and software compatibility matrix

Item	Specifications	
Product model	F5000-C	F5000-S
Memory	4 GB	
Flash	4 MB	
Boot ROM version	Version 1.21 or higher (To see version information, use the **display version** command in any view. Please see **Note 2**)	
System image	SECPATH5000FS-CMW520-R3811P10.bin SECPATH5000FC-CMW520-R3811P10.bin	
IMC version	iMC EAD 7.3 (E0502) iMC EIA 7.3 (E0503) iMC IVM 7.3 (E0501) iMC PLAT 7.3 (E0504) iMC UBA 7.3（E0502）	
Inode version	iNode 7.3 (E0504)	

For example, display version information for F5000-C.

```
<Sysname> display version
HP Comware Platform Software
Comware Software, Version 5.20, Release 3811P10                    ------- Note 1
Copyright (c) 2010-2017 Hewlett-Packard Development Company, L.P.
HP F5000-S uptime is 0 week, 0 day, 0 hour, 3 minutes

 CPU type: xxx
 4094M bytes DDR3 SDRAM Memory
 8M bytes Flash Memory
 247M bytes CF0 Card
 Board PCB        Version:Ver.A
 BackBoard PCB    Version:Ver.A
 FAN PCB          Version:Ver.A
 CPLD_A           Version:  1.0
 CPLD_B           Version:  1.0
 Basic  BootWare  Version:  1.13                              ------ Note 2
 Extend BootWare  Version:  1.13                              ------ Note 2
 [FIXED PORT] CON        (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
 [FIXED PORT] AUX        (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
 [FIXED PORT] GE0/0      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
```

```
[FIXED PORT] GE0/1      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/2      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
 ......
[FIXED PORT] XGE0/27    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[SUBCARD  1] NSQ1G24XS60(Hardware)Ver.A,  (Driver)3.0,  (Cpld)131.
```

Upgrade restrictions and guidelines

Before performing a software upgrade, it is important to refer to the Software Feature Changes document for any feature changes in the new version. Also check the most recent version of the related documents (see “Related documents”) available on the HP website for more information about feature configuration and commands.

Hardware feature updates

None.

Software feature and command updates

For information about the software feature and command update history, see *HP 5000FS_5000FC-CMW520-R3811P10 Release Notes (Software Feature Changes*).

MIB updates

Table 2 MIB updates

Item	MIB file	Module	Description
R3811P10			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3811P09			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3811P08			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3811P05			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3811P03			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A

Item	MIB file	Module	Description
R3811P02			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3811			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3810P04			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3810P02			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A
R3808			
New	N/A	N/A	N/A
Modified	N/A	N/A	N/A

Operation changes

None.

Restrictions and cautions

- The Web configuration summary page can display a maximum of 5000 configuration entries. If the configuration entries exceed 5000, the Web page cannot display all information. You can use a filter to get wanted information.
- The software does not support the USB module for SecBlade III, which is reserved for future use.
- Steps to change certificates：

  The certificate is valid for November 9,2017.Please change the certificate as follows.

  First, change the properties of hostkey and hostkey_V3.

  [HP]_h

  [HP -hidecmd]attrib hostkey -h

  [HP -hidecmd]attrib hostkey_v3 -h

  And then, delete the certificates, and then, delete hostkey and hostkey_V3.

  The last, change version.

Open problems and workarounds

HSD109369

- Symptom: If a VPN instance name that contains uppercase letters is bound to an NQA ICMP operation, the uppercase letters are automatically changed to lowercase letters.

- Condition: This symptom occurs if a VPN instance name that contains uppercase letters is bound to an NQA ICMP operation.
- Workaround: Use lowercase letters in the VPN instance name.

HSD112168

- Symptom: Configurations such as IPsec and NAT on a subinterface cannot be synchronized to the standby device after the two devices enter synchronization state.
- Condition: This symptom occurs if the Layer-3 subinterface or Layer-3 aggregate subinterface are created before the two devices enter synchronization state.
- Workaround: Configure the two devices to enter synchronization state, and then create a Layer-3 subinterface or Layer-3 aggregate subinterface for configurations.

HSD110063

- Symptom: Batch configuration synchronization for physical interface types succeeds but real-time configuration synchronization for physical interface types fails.
- Condition: This symptom can be seen when configuration synchronization between active and standby firewalls is enabled.
- Workaround: When configuration synchronization between active and standby firewalls is enabled, if you modify the type for a physical interface on the active firewall, you must manually modify the type for the physical interface on the standby firewall.

HSD100621

- Symptom: After attack defense settings are deleted from the Web interface, the settings still exist and take effect on the firewall.
- Condition: This symptom can be seen if you configure attack defense settings at the CLI and then delete the settings in the Web interface.
- Workaround: Delete the attack defense settings at the CLI.

HSD113033

- Symptom: The firewall unexpectedly reboots when the **display current-configuration** command is executed.
- Condition: This symptom occurs when the following conditions exist:
  - The configuration file exceeds 100 KB.
  - The **display current-configuration** command with a regular expression is executed, such as the **display current-configuration | include .*.*.*/.** command.
- Workaround: Do not include a regular expression in the **display current-configuration** command. If a regular expression must be used, do not use any asterisk "*", or use as few asterisks as possible.

HSD113815

- Symptom: A ping operation through a Layer 2 subinterface fails.
- Condition: This symptom occurs when a Layer 2 subinterface is used to forward packets.
- Workaround: Do not use any Layer subinterface to forward packets.

HSD113787

- Symptom: A firewall discards VRRP packets, resulting in two active VRRP devices.
- Condition: This symptom occurs if VRRP is configured on an aggregate interface. VRRP packets that the aggregate interface in VRRP initialization state sends to the virtual MAC address are discarded by the switch chip because of MAC learning error on the switching chip.
- Workaround: Do not configure VRRP on an aggregate interface.

List of resolved problems

Resolved problems in HP 5000FS_5000FC-CMW520-R3811P10

201708170503

- Symptom: A memory leakage occurs on the device.
- Condition: Acceleration is enabled for inter-zone policies. Later the inter-zone policies are modified through Web GUI, and acceleration is enabled again.

201706290426

- Symptom: Warning messages are not generated in SNMP trap.
- Condition: One of the power module failed when dual power module are used.

201705310338

- Symptom: The device reboots abnormally.
- Condition: The memory used by packet-filter is corrupted.

201705180652

- Symptom: The default certificate in the device will expire at November 2017.
- Condition: None.

201704130220

- Symptom: The device reboots abnormally.
- Condition: A local authentication user and a remote SSL VPN authentication user share a same user name. The two users log in at the same time and later the SSL VPN user is forced to be offline by the radius server.

201707210608

- Symptom: CVE-2012-2110.
- Condition:The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8 v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which a llows remote attackers to conduct buffer overflow attacks, and cause a denial of service (mem ory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstra ted by an X.509 certificate or an RSA public key.

201707210688

- Symptom: CVE-2017-6458.
- Condition: NTP are prone to a buffer-overflow vulnerability because it fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.

Resolved problems in HP 5000FS_5000FC-CMW520-R3811P09

201507290353

- Symptom: CVE-2015-3195

- Condition: Fixed vulnerability with malformed OpenSSL X509_ATTRIBUTE structure used by the PKCS#7 and CMS routines which may cause memory leak.

201703100806

- Symptom: CVE-2009-3238
- Condition: The get_random_int function in the Linux kernel before 2.6.30 produces insufficiently random numbers, which allows attackers to predict the return value, and possibly defeat protection mechanisms.

201610310294

- Symptom: CVE-2013-0169
- Condition: The TLS protocol and the DTLS protocol do not properly consider timing side-channel attacks on a MAC check requirement during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, aka the "Lucky Thirteen" issue.

201703100837

- Symptom: CVE-2014-9751.
- Condition: The read_network_packet function in ntp_io.c in ntpd in NTP 4.x before 4.2.8p1 on Linux and OS X does not properly determine whether a source IP address is an IPv6 loopback address, which makes it easier for remote attackers to spoof restricted packets, and read or write to the runtime state, by leveraging the ability to reach the ntpd machine's network interface with a packet from the ::1 address.

201703100866

- Symptom: CVE-2015-5219
- Condition: NTP is prone to a denial-of-service vulnerability. A remote attacker may exploit this issue to cause an infinite loop, resulting in a denial-of-service condition.

201612050296

- Symptom: CVE-2016-7428
- Condition: An attacker with access to the NTP broadcast domain can send specially crafted broadcast mode NTP packets to the broadcast domain which, while being logged by ntpd, will cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.

201612050296

- Symptom: CVE-2016-7427
- Condition: An attacker with access to the NTP broadcast domain can periodically inject specially crafted broadcast mode NTP packets into the broadcast domain which, while being logged by ntpd, can cause ntpd to reject broadcast mode packets from legitimate NTP broadcast servers.

201701170630

- Symptom: CVE-2016-8610
- Condition: OpenSSL is prone to denial-of-service vulnerability.Successful exploitation of the issue will cause excessive memory or CPU resource consumption, resulting in a denial-of-service condition.

Resolved problems in HP 5000FS_5000FC-CMW520-R3811P08

201606010065

- Symptom: The iMC did not respond to the ICMP message.
- Condition: Do same set operation for the nodes of ipForwarding and ipDefaultTTL.

201610180402

- Symptom: CVE-2016-1409.
- Condition: The Neighbor Discovery (ND) protocol implementation in the IPv6 stack in Cisco I OS XE 2.1 through 3.17S, IOS XR 2.0.0 through 5.3.2, and NX-OS allows remote attackers to cause a denial of service (packet-processing outage) via crafted ND messages, aka Bug ID CSCuz66542, as exploited in the wild in May 2016.

201610240474

- Symptom: CVE-2015-7974.
- Condition: Fixed vulnerability in NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key.

201610240474

- Symptom: CVE-2015-7973.
- Condition: Fixed vulnerability when NTP is configured in broadcast mode, a man-in-the-middle attacker or a malicious client could replay packets received from the broadcast server to all (other) clients, which cause the time on affected clients to become out of sync over a longer period of time.

201610140014

- Symptom: CVE-2016-4954.
- Condition: Fixed vulnerability in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service by sending spoofed packets from source IP addresses in a certain scenario.

201605260280

- Symptom: CVE-2016-1550.
- Condition: Fixed vulnerability in ntpd function allow an attacker to conduct a timing attack to compute the value of the valid authentication digest causing forged packets to be accepted by ntpd.

201605260280

- Symptom: CVE-2016-1551.
- Condition: Fixed vulnerability in ntpd allows unauthenticated network attackers to spoof refclock packets to ntpd processes on systems that do not implement bogon filtering.

Resolved problems in HP 5000FS_5000FC-CMW520-R3811P05

201507290353

- Symptom:CVE-2015-1788

- Condition: When processing an ECParameters structure OpenSSL enters an infinite loop. This can be used to perform denial of service against any system which processes public keys, certificate requests or certificates.

Resolved problems in HP 5000FS_5000FC-CMW520-R3811P03

201501050340

- Symptom: CVE-2014-9295
- Condition: Stack-based buffer overflows in ntpd in NTP before 4.2.8 allows remote attackers to execute arbitrary code via a crafted packet.

201410230409

- Symptom: SSL 3.0 Fallback protection
- Condition: OpenSSL has added support for TLS_FALLBACK_SCSV to allow applications to block the ability for a MITM attacker to force a protocol downgrade. Some client applications (such as browsers) will reconnect using a downgraded protocol to work around interoperability bugs in older servers. This could be exploited by an active man-in-the-middle to downgrade connections to SSL 3.0 even if both sides of the connection support higher protocols. SSL 3.0 contains a number of weaknesses including POODLE (CVE-2014-3566).

Resolved problems in HP 5000FS_5000FC-CMW520-R3811P02

201408150034

- Symptom: CVE-2014-3508
- Condition: A flaw in OBJ_obj2txt may cause pretty printing functions such as X509_name_oneline, X509_name_print_ex et al. to leak some information from the stack. Applications may be affected if they echo pretty printing output to the attacker.

201408280243

- Symptom: CVE-2008-5161
- Condition: Error handling in the SSH protocol in several SSH servers/clients, including OpenSSH 4.7p1 and possibly other versions, when using Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data.

Resolved problems in HP 5000FS_5000FC-CMW520-R3811

201407020278

- Symptom:CVE-2014-0224
- Condition:When Open SSL Server or Client is used.

Resolved problems in HP 5000FS_5000FC-CMW520-R3810P4

201403140300

- Symptom: The device unexpectedly reboots.
- Condition: This symptom can be seen when IPsec requires the CPU to generate a random number during SA negotiation.

Resolved problems in HP 5000FS_5000FC-CMW520-R3810P2

201401140211

- Symptom: The device can't startup normally.
- Condition: Test under the ESS (Environment Stress Screen) low temperature lab.

201308300271

- Symptom: A PC running Win7 obtains an incorrect DNS server address from the DHCP server on the Firewall device.
- Condition: This symptom occurs if multiple DHCP address pools are configured, and the PC's MAC address is bound to a static address pool on the Firewall device.

201308290004

- Symptom: The device unexpectedly reboots during a CRL acquisition operation.
- Condition: This symptom occurs if the CRL acquisition operation is performed when the memory usage exceeds 95% because of large amounts of TCP and UDP traffic.

201309100016

- Symptom: The device unexpectedly reboots when multiple voice NQA operations that have the same source but different destinations are configured.
- Condition: This symptom occurs when multiple voice NQA operations that have the same source but different destinations are configured.

201309040150

- Symptom: An inter-zone policy can never be matched.
- Condition: This symptom occurs if the following conditions exist:
  - There are two inter-zone policies that have the same information except for their bound content filtering policies.
  - The inter-zone policy that can never be matched has a lower match priority.

201304220334

- Symptom: Memory leaks occur after the device has received large numbers of fragment packets in an asymmetric stateful failover scenario.
- Condition: This symptom occurs after the device has received large numbers of fragment packets in an asymmetric stateful failover scenario.

Resolved problems in HP 5000FS_5000FC-CMW520-R3808

First release.

Related documents

Documentation set

- HP F5000-S[F5000-C] VPN Firewall Appliances Installation Guide-6W105
- HP F5000-S[F5000-C] NSQ1G24XS60 Card Manual-AP101
- HP F5000-S[F5000-C] VPN Firewall Appliances Compliance and Safety Manual-APW102
- HP VPN Firewall Appliances Configuration Guides-6PW101
- HP VPN Firewall Appliances Command References-6PW101

Obtaining documentation

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Appendix A Feature list

Hardware features

Hardware features

Item	F5000-C	F5000-S
Dimensions (H × W × D)	88.1 × 440 × 443.1 mm (3.47 × 17.32 × 17.44 in)	
Weight	15.7 kg (34.61 lb)	
Power consumption	260 W	
SDRAM	4 GB	
Fixed interfaces	1 console port 12 ×10/100/1000Base-T Ethernet copper interfaces 12 ×1000Base-X SFP fiber interfaces 6 × 10GBase-R SFP+ fiber interfaces	
CF card	• 256 MB (default) • 1 GB (maximum)	
Temperature	Operating: 0°C to 45°C (32°F to 113°F) Non-operating: -40°C to 70°C (-104°F to 158°F)	
Relative humidity (noncondensing)	Operating: 10% to 90% Non operating: 5% to 95%	

Software features

Software features

Category	Features	
Security	AAA	RADIUS/HWTACACS+ CHAP authentication PAP authentication Domain-based authentication

Category	Features	
	Firewall	Packet filtering Security zone-based access control Time-based access control ASPF status-based packet filtering Virtual firewall Attack detection and protection, against attacks including Land, Smurf, Fraggle, WinNuke, Ping of Death, Tear Drop, IP Spoofing, IP fragments, packet fragments, TCP Flag, large ICMP, address scanning, port scanning, SYN flood, and ICMP flood attacks URL filtering Control of ICMP redirect or unreachable packets Control of Tracert packets Control of packets with the route record option Static and dynamic blacklist functions P2P rate limit Content filtering for HTTP, SMTP, POP3, FTP, and Telnet
	Security management	Real-time attack logs Blacklist logs Session logs Binary logs Traffic statistics and analysis Security event statistics
	NAT	Address translation based on address pools Using ACL to control address translation Easy IP NAT server NAT aging time ALG for protocols including FTP, DNS, QQ, MSN, H323, NBT, ILS, RTSP, SQLNET, and SIP NAT444
VPN	IPSec/IKE	AH and ESP Manually configured SAs and SAs negotiated by IKE ESP support for the DES, 3DES, and AES encryption algorithms MD5 and SHA-1 authentication algorithms IKE main mode and aggressive mode DPD NAT traversal
	L2TP	L2TP
	GRE	GRE
Network connection	LAN protocols	Ethernet_II VLAN

Category	Features	
	IP services	ARP Static domain name resolution IP unnumbered DHCP relay DHCP server DHCP client
	IP routing	Static routes RIP-1/RIP-2 OSPF BGP PBR Routing policy
IPv6	Basic IPv6	Protocol processing Ethernet link layer ICMPv6 IPv6 address management PMTU Socket TCP6 UDP6 RAWIP6 Ping6 DNS6 TraceRT6 Telnet6 FIB6 DHCPv6 client DHCPv6 relay
	IPv6 routing and multicast	RIPng OSPFv3 BGP4+ Static routing PBR PIM-SM PIM-DM
	IPv6 security	NAT-PT Manual tunnel IPv6 over IPv4 GRE tunnel (RFC2784) 6to4 tunnel (RFC3056) ISATAP Tunnel IPv6 Packet Filter RADIUS DS-Lite
HA	VRRP	VRRP

Category	Features	
	Stateful failover	Stateful failover for sessions IPSec stateful failover Asymmetric paths Configuration synchronization
Configuration management	CLI	Local login through the console port Local or remote login through Telnet or SSH Command privilege levels, which help prevent unauthorized access to the device Debugging information that is helpful for network troubleshooting Network test tools, including tracert and ping commands Using Telnet to log in to another network device to manage the device FTP server and FTP client for uploading or downloading configuration files or images. TFTP for file uploading and downloading Logging File system management User interfaces configuration for login authentication and authorization
	Web interface	Web session idle timeout Web user login and authentication Device management, device monitoring, and firewall policy configuration
	SNMPv3, compliant with SNMP v2C and SNMP v1 NTP	

Appendix B Upgrading software

The software upgrade procedure is the same for F5000-C and F5000-S vpn firewalls. This chapter uses the F5000-S vpn firewall to describe how to upgrade software from the CLI, Web interface, and BootWare menus.

Software types

The following software types are available:

- **BootWare image**—A .btw file that contains a basic segment and an extended segment. The basic segment is the minimum code that bootstraps the system. The extended segment enables hardware initialization and provides system management menus. You can use these menus to load software and the startup configuration file or manage files when the firewall cannot start up correctly.
- **System software image**—A .bin file that contains software features. You can assign the following attributes to a system software image:
  - **Main**—The image is the primary image. The system always attempts to load the main image at startup in preference to the backup image.
  - **Backup**—The image is the backup image. It is used only if the primary image is corrupt or not available.

- **Secure**—The image is the secure image. If both the main and backup system software images are corrupt or not available, the device starts up with the secure system software image. If no secure system software image is available, the firewall displays a failure prompt.

When you upgrade the system software, the BootWare is upgraded automatically. You do not need to upgrade BootWare separately.

Configuration files

You can save settings you made to a configuration file so they can survive a reboot.

The firewall supports .cfg and .xml configuration files. The .cfg configuration file saves settings made at the CLI and in the Web interface. The .xml saves only settings made in the Web interface.

Upgrade methods

To upgrade system software, use one of the following methods:

- Upgrading system software from the CLI
- Upgrading system software from the Web interface
- Upgrading system software from BootWare menus

To upgrade the BootWare, use either of the following methods:

- Upgrading the BootWare from the CLI
- Upgrading the BootWare from BootWare menus

You must reboot the firewall after a system software or BootWare upgrade. A device reboot interrupts services.

Before a software upgrade, read the release notes to identify the command changes. Some commands in the configuration file might not be supported after a software upgrade.

Preparing for the upgrade

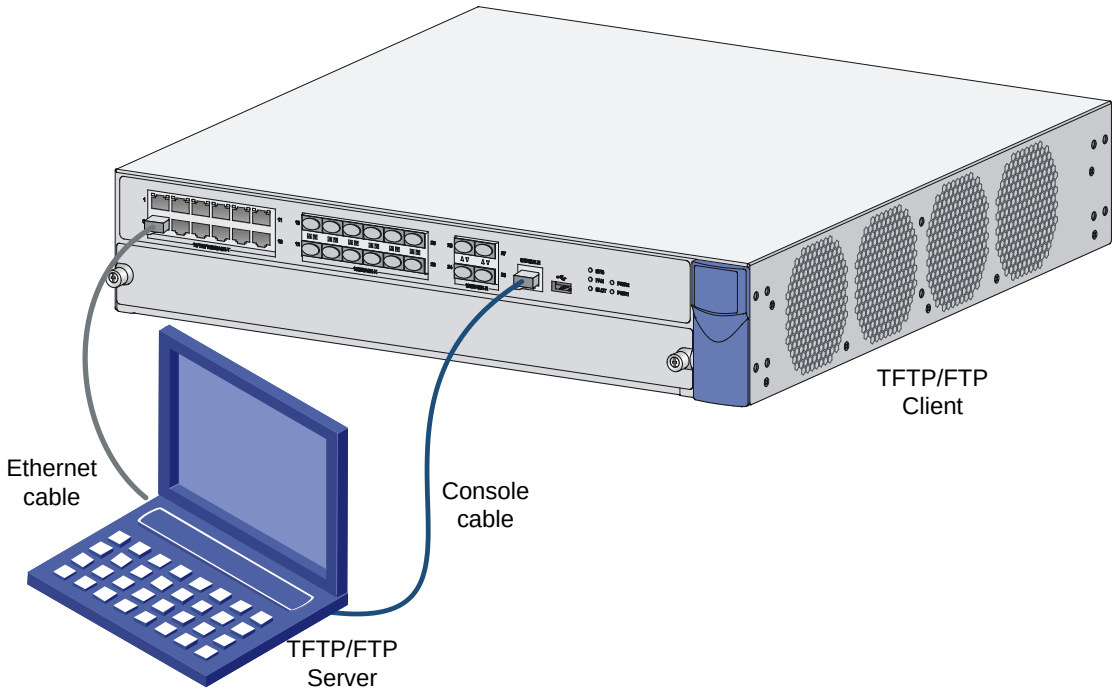
Before you upgrade system software, complete the following tasks:

- Set up the upgrade environment as shown in Figure 1.
- Run a TFTP or FTP server on the file server. (Skip this task if you upgrade software from the Web interface.)

  The firewall does not come with TFTP or FTP server software. Prepare the software yourself.
- Assign an IP address to the file server. Make sure the management Ethernet port on the firewall and the file server can reach each other.

  By default, the IP address of the management Ethernet port GigabitEthernet 0/0 is 192.168.0.1/24.
- Transfer the software upgrade file to the file server and set the working directory on the TFTP or FTP server.
- Log in to the CLI of the firewall through the console port. (Skip this task if you upgrade software from the Web interface.)
- Make sure the upgrade has minimal impact on the network services. During the upgrade, the firewall cannot provide any services.

Setting up the upgrade environment



Upgrading system software

Upgrading system software from the CLI

You can use TFTP or FTP on the firewall to access the TFTP or FTP server to back up or download software files for software upgrades.

Using TFTP to upgrade system software

Back up the system software image and configuration files:

Use the **save** command in any view to save the running configuration to the .cfg startup configuration file.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait....
 Configuration is saved to device successfully.
<Sysname>
```

Use the **dir** command in user view to display files.

Identify the startup system software image and configuration files, and verify that the CF card has enough space for the new system software image.

```
<Sysname> dir
Directory of cfa0:/

   0     -rw-     10715  Jul 30 2013 15:59:42   system.xml
   1     -rw-       891  Jul 04 2013 11:32:04   default_ca.cer
```

```
  2     -rw-      1411  Jul 04 2013 11:32:04   default_local.cer
  3     -rw-      3154  Jul 30 2013 15:59:46   startup.cfg
  4     drw-         -   Jul 04 2013 11:32:12   logfile
  5     drw-         -   Jul 04 2013 11:32:12   seclog
  6     -rw-    334945  Jul 29 2013 13:33:26   default.diag
  7     -rw-  23446448  Jul 29 2013 14:20:24   main.bin

252164 KB total (228906 KB free)

File system type of cfa0: FAT32

<Sysname>
```

Use the **tftp put** command in user view to upload **main.bin** to the TFTP server.

```
<Sysname> tftp 192.168.0.2 put main.bin

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... /
  TFTP: 23446448 bytes sent in 66 second(s).
  File uploaded successfully.

<Sysname>
```

Use the **tftp put** command in user view to upload **startup.cfg** and **system.xml** to the TFTP server.

```
<Sysname> tftp 192.168.0.2 put startup.cfg

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP:     3154 bytes sent in 0 second(s).
  File uploaded successfully.
<Sysname> tftp 192.168.0.2 put system.xml

  File will be transferred in binary mode
  Sending file to remote TFTP server. Please wait... \
  TFTP:    10715 bytes sent in 0 second(s).
  File uploaded successfully.

<Sysname>
```

Upgrade the system software:

This configuration example was created and verified on the firewall that runs Ess 3807. The system software image file name is **f5000-s.bin**.

To upgrade the system software:

Use the **tftp get** command in user view to download the system software image file to the CF card on the firewall.

```
<Sysname> tftp 192.168.0.2 get f5000-s.bin

  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait...\
  TFTP: 23446448 bytes sent in 66 second(s).
  File downloaded successfully.
```

```
<Sysname>
```

Use the **boot-loader** command in user view to specify **f5000-s.bin** as the main startup image file.

```
<Sysname> boot-loader file f5000-s.bin main
  This command will set the boot file. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot
0!
<Sysname>
```

Use the **display boot-loader** command in user view to verify that the file has been specified as the main startup system software image file.

```
<Sysname> display boot-loader
 The boot file used this time:cfa0:/main.bin attribute: main
 The boot file used next time:cfa0:/f5000-s.bin attribute: main
 Failed to get the backup boot file used next time!
 Failed to get the secure boot file used next time!
<Sysname>
```

Use the **reboot** command in user view to reboot the firewall.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.
........DONE!
 This command will reboot the device. Continue? [Y/N]:y
System is starting...
```

After the reboot is complete, use the **display version** command to verify that the system software image is correct.

```
<Sysname> display version
HP Comware Platform Software
Comware Software, Version 5.20, Ess 3807
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
HP F5000-S uptime is 0 week, 0 day, 0 hour, 3 minutes

CPU type: XXX
4094M bytes DDR3 SDRAM Memory
8M bytes Flash Memory
247M bytes CF0 Card
Board PCB        Version:Ver.A
BackBoard PCB    Version:Ver.A
FAN PCB          Version:Ver.A
CPLD_A           Version:  1.0
CPLD_B           Version:  1.0
Basic  BootWare  Version:  1.19
Extend BootWare  Version:  1.19
[FIXED PORT] CON        (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] AUX        (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/0      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/1      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/2      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/3      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/4      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/5      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
```

```
[FIXED PORT] GE0/6      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/7      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/8      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/9      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/10     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/11     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/12     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/13     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/14     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/15     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/16     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/17     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/18     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/19     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/20     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/21     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/22     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/23     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/24    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/25    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/26    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/27    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[SUBCARD  1] NSQ1G24XS60(Hardware)Ver.A,  (Driver)1.0,  (Cpld)129.0

<Sysname>
```

Using FTP to upgrade system software

Back up the startup system software image and configuration files:

Use the **save** command in any view to save the running configuration to the .cfg startup configuration file.

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait....
 Configuration is saved to device successfully.
<Sysname>
```

Use the **dir** command in user view to display files.

Identify the startup system software image and configuration files, and verify that the CF card has enough space for the new system software image.

```
<Sysname> dir
Directory of cfa0:/

   0     -rw-     10715  Jul 30 2013 15:59:42   system.xml
   1     -rw-       891  Jul 04 2013 11:32:04   default_ca.cer
   2     -rw-      1411  Jul 04 2013 11:32:04   default_local.cer
   3     -rw-      3154  Jul 30 2013 15:59:46   startup.cfg
   4     drw-         -   Jul 04 2013 11:32:12   logfile
   5     drw-         -   Jul 04 2013 11:32:12   seclog
```

```
   6     -rw-    334945  Jul 29 2013 13:33:26   default.diag
   7     -rw-  23446448  Jul 29 2013 14:20:24   main.bin

252164 KB total (228906 KB free)

File system type of cfa0: FAT32

<Sysname>
```

Use the **ftp** command in user view to access the FTP server.

```
<Sysname> ftp 192.168.0.2
Trying 192.168.0.2 ...
Press CTRL+K to abort
Connected to 192.168.0.2.
220 3Com 3CDaemon FTP Server Version 2.0
User(192.168.0.2:(none)):user123
331 User name ok, need password
Password:
230 User logged in

[ftp]
```

Use the **put** command in FTP client view to upload **main.bin** to the FTP server.

```
[ftp] put main.bin
227 Entering passive mode (192,168,0,2,26,0)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 23446448 byte(s) sent in 14.605 second(s), 1355.00Kbyte(s)/sec.

[ftp]
```

Use the **put** command in FTP client view to upload **startup.cfg** and **system.xml** to the FTP server.

```
[ftp] put startup.cfg
227 Entering passive mode (192,168,0,2,26,3)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 3154 byte(s) sent in 0.187 second(s), 6.00Kbyte(s)/sec.

[ftp] put system.xml
227 Entering passive mode (192,168,0,2,26,6)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 10715 byte(s) sent in 0.203 second(s), 50.00Kbyte(s)/sec.

[ftp]
```

Upgrade the system software:

This configuration example was created and verified on the firewall that runs Ess 3807. The system software image file name is **f5000-s.bin**.

To upgrade the system software:

Use the **get** command in FTP client view to download the system software image file to the CF card on the firewall.

```
[ftp] get f5000-s.bin

227 Entering passive mode (192,168,0,2,26,77)
125 Using existing data connection
226 Closing data connection; File transfer successful.
FTP: 23446448 byte(s) received in 88.243 second(s), 224.00K byte(s)/sec.

[ftp]
```

Use the **quit** command in FTP client view to return to user view.

```
[ftp] quit
221 Service closing control connection

<Sysname>
```

Use the **boot-loader** command in user view to specify **f5000-s.bin** as the main startup image file.

```
<Sysname> boot-loader file f5000-s.bin main
  This command will set the boot file. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot
0!
<Sysname>
```

Use the **display boot-loader** command in user view to verify that the file has been specified as the main startup system software image file.

```
<Sysname> display boot-loader
 The boot file used this time:cfa0:/main.bin attribute: main
 The boot file used next time:cfa0:/f5000-s.bin attribute: main
 Failed to get the backup boot file used next time!
 Failed to get the secure boot file used next time!
<Sysname>
```

Use the **reboot** command in user view to reboot the firewall.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file, please wait.
........DONE!
 This command will reboot the device. Continue? [Y/N]:y
System is starting...
```

After the reboot is complete, use the **display version** command to verify that the system software image is correct.

```
<Sysname> display version
HP Comware Platform Software
Comware Software, Version 5.20, Ess 3807
Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.
HP F5000-S uptime is 0 week, 0 day, 0 hour, 3 minutes

 CPU type: XXX
 4094M bytes DDR3 SDRAM Memory
 8M bytes Flash Memory
 247M bytes CF0 Card
 Board PCB        Version:Ver.A
 BackBoard PCB    Version:Ver.A
 FAN PCB          Version:Ver.A
```

```
CPLD_A           Version:  1.0
CPLD_B           Version:  1.0
Basic  BootWare  Version:  1.19
Extend BootWare  Version:  1.19
[FIXED PORT] CON        (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] AUX        (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/0      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/1      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/2      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/3      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/4      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/5      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/6      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/7      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/8      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/9      (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/10     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/11     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/12     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/13     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/14     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/15     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/16     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/17     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/18     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/19     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/20     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/21     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/22     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] GE0/23     (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/24    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/25    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/26    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[FIXED PORT] XGE0/27    (Hardware)Ver.A,  (Driver)1.0,  (Cpld)1.0
[SUBCARD  1] NSQ1G24XS60(Hardware)Ver.A,  (Driver)1.0,  (Cpld)129.0

<Sysname>
```

Upgrading system software from the Web interface

CAUTION:

- Do not perform any operation on the Web interface while the system is upgrading software.
- The first time you log in to the firewall from the Web interface, you can use the default login information. After login, create a Web login account of the management level and delete the default Web login account to ensure device security. For more information, see *HP VPN Firewall Appliances Getting Started Guide*.

Table 6 describes the default settings used to log in to the Web interface.

Default login information

Login information	Default setting
Username	admin
Password	admin
IP address of GigabitEthernet 0/0	192.168.0.1/24

To upgrade the system software from the Web interface:

Use an Ethernet cable to connect the F5000-S vpn firewall to the PC.

Assign an IP address on the same subnet as the management port GigabitEthernet 0/0 to the PC.

In this example, assign 192.168.0.2 to the PC.

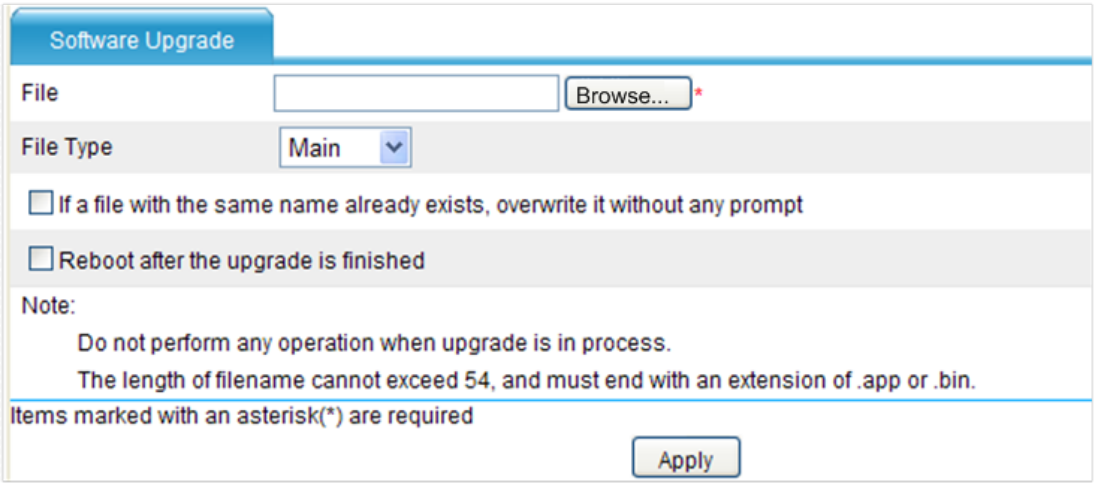
Launch the Web browser, and enter 192.168.0.1 in the address bar.

The Web login page appears.

Type the default username and password, and click **Login**.

Select **Device Management** > **Software Upgrade** from the navigation tree.

Upgrading the software



Specify the software upgrading configuration items as described in Table 7.

Configuration items

Item	Description
File	Click **Browse** to set the path to the .bin system software image file.
File Type	Set the file attribute: **Main**—The image is the primary image. The system always attempts to load the main image at startup in preference to the backup image. **Backup**—The image is the backup image. It is used only if the primary image is corrupted or not available.
If a file with the same name already exists, overwrite it without any prompt	If you do not select this option, you must make sure the upgrade file uses a file name that is different from any software file on the firewall.
Reboot after the upgrade is finished	If you select this option, the firewall automatically reboots to complete the software upgrade.

Click **Apply**.

Upgrading system software from BootWare menus

You can use the following methods to upgrade software from BootWare menus:

- Using TFTP/FTP to upgrade software through an Ethernet port
- Using Xmodem to upgrade software through the console port

Upgrading through an Ethernet port is faster than through the console port.

Accessing the EXTEND-BOOTWARE menu

Power on the firewall.

```
System is starting...
Press Ctrl+D to access BASIC-BOOTWARE MENU
Press Ctrl+T to start heavy memory test
Booting Normal Extend BootWare........
The Extend BootWare is self-decompressing......Done!

********************************************************************************
*                                                                              *
*               HP SecPath Series BootWare, Version 1.19                       *
*                                                                              *
********************************************************************************
Compiled Date       : Jun 20 2013
CPU Type            : XXX
CPU Clock Speed     : 1400MHz
Memory Type         : DDR3 SDRAM
Memory Size         : 4096MB
Memory Speed        : 1333MHz
BootWare Size       : 768KB
Flash Size          : 8MB
cfa0 Size           : 247MB
CPLD_A Version      : 1.0
CPLD_B Version      : 1.0
PCB Version         : Ver.A


BootWare Validating...
Press Ctrl+B to enter extended boot menu...
BootWare password: Not required. Please press Enter to continue.
```

Press **Ctrl**+**B** at the prompt.

The following message appears:

```
BootWare password: Not required. Please press Enter to continue.
```

Press Enter to access the EXTEND-BOOTWARE menu.

```
 Password recovery capability is enabled.
Note: The current operating device is cfa0
Enter < Storage Device Operation > to select device.

==========================<EXTEND-BOOTWARE MENU>==========================
```

```
|<1> Boot System                                                              |
|<2> Enter Serial SubMenu                                                     |
|<3> Enter Ethernet SubMenu                                                   |
|<4> File Control                                                             |
|<5> Restore to Factory Default Configuration                                 |
|<6> Skip Current System Configuration                                        |
|<7> BootWare Operation Menu                                                  |
|<8> Clear Super Password                                                     |
|<9> Storage Device Operation                                                 |
|<0> Reboot                                                                   |
==============================================================================
Ctrl+Z: Access EXTEND-ASSISTANT MENU
Ctrl+C: Display Copyright
Ctrl+F: Format File System
Enter your choice(0-9):
```

EXTEND-BOOTWARE menu options

Item	Description
<1> Boot System	Boot the system software image.
<2> Enter Serial SubMenu	Access the Serial submenu (see Table 11) for upgrading system software through the console port or changing the serial port settings.
<3> Enter Ethernet SubMenu	Access the Ethernet submenu (see Table 9) for upgrading system software through an Ethernet port or changing Ethernet settings.
<4> File Control	Access the File Control submenu (see Table 15) to manage files stored on the firewall.
<5> Restore to Factory Default Configuration	Restore the factory defaults. This option is available only if password recovery capability is disabled. △ CAUTION: Use this option with caution. This option will delete the current configuration file and restarts the firewall with the factory configuration.
<6> Skip Current System Configuration	Start the firewall with the factory default configuration. This is a one-time operation and takes effect only for the first system boot or reboot after you choose this option. You use this option when you forget the console login password. This option is available only if password recovery capability is enabled.
<7> BootWare Operation Menu	Access the BootWare Operation menu for backing up, restoring, or upgrading BootWare.
<8> Clear Super Password	Clear all super passwords used for changing to higher user privilege levels. By default, no super password is required for changing to a higher user privilege level. This option is available only if password recovery capability is enabled.
<9> Storage Device Operation	Access the Storage Device Operation menu to manage storage devices.

Item	Description
<0> Reboot	Restart the firewall.

To enable password recovery capability, use the password-recovery enable command. To disable password recovery capability, use the undo password-recovery enable command. For more information, see *HP VPN Firewall Appliances System Management and Maintenance Configuration Guide*.

Using TFTP/FTP to upgrade software through an Ethernet port

Enter **3** in the EXTEND-BOOTWARE menu to access the Ethernet submenu.

```
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is cfa0                                         |
|<1> Download Application Program To SDRAM And Run                         |
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Ethernet Parameter                                             |
|<0> Exit To Main Menu                                                     |
|<Ensure The Parameter Be Modified Before Downloading!>                    |
============================================================================
Enter your choice(0-5):
```

Ethernet submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download a system software image to the SDRAM through the Ethernet port and run the image. This option is available only if password recovery capability is enabled.
<2> Update Main Application File	Upgrade the main system software image.
<3> Update Backup Application File	Upgrade the backup system software image.
<4> Update Secure Application File	Upgrade the secure system software image.
<5> Modify Ethernet Parameter	Configure FTP or TFTP file transfer settings.
<0> Exit To Main Menu	Return to the EXTEND-BOOTWARE menu.

Enter **5** in the Ethernet submenu to configure the network settings.

```
=========================<ETHERNET PARAMETER SET>=========================
|Note:       '.' = Clear field.                                          |
|            '-' = Go to previous field.                                 |
|          Ctrl+D = Quit.                                                |
============================================================================
Protocol (FTP or TFTP) :tftp
Load File Name         :main.bin
                       :
Target File Name       :main.bin
                       :
Server IP Address      :192.168.0.2
Local IP Address       :192.168.0.1
Gateway IP Address     :0.0.0.0
```

Network parameter fields and shortcut keys

Field	Description
'.' = Clear field	Press a dot (.), and then press **Enter** to clear the setting for a field.
'-' = Go to previous field	Press a hyphen (-), and then press **Enter** to return to the previous field.
Ctrl+D = Quit	Press **Ctrl**+**D** to exit the ETHERNET PARAMETER SET menu.
Protocol (FTP or TFTP)	Set the file transfer protocol to FTP or TFTP.
Load File Name	Set the name of the file to be downloaded.
Target File Name	Set a file name for saving the file on the firewall. By default, the target file name is the same as the source file name.
Server IP Address	Set the IP address of the FTP or TFTP server.
Local IP Address	Set the IP address of the Ethernet interface that connects to the TFTP or FTP server.
Gateway IP Address	Set a gateway IP address if the firewall is on a different network from the server.

Choose an option from options **1** to **4** in the Ethernet submenu. For example, to upgrade the main system software image, enter **2**.

```
Loading.....................................................................
.....................................................................
.....................Done!
23446448 bytes downloaded!
Updating File cfa0:/main.bin.....................................
................................................Done!
==========================<Enter Ethernet SubMenu>==========================
|Note:the operating device is cfa0                                          |
|<1> Download Application Program To SDRAM And Run                          |
|<2> Update Main Application File                                           |
|<3> Update Backup Application File                                         |
|<4> Update Secure Application File                                         |
|<5> Modify Ethernet Parameter                                              |
|<0> Exit To Main Menu                                                      |
|<Ensure The Parameter Be Modified Before Downloading!>                     |
=============================================================================
Enter your choice(0-5):
```

If a file with the same file name as the upgrade file exists, the system prompts you to overwrite the existing file. If you do not overwrite the file, the existing software file is not changed, and the upgrading fails.

Enter **0** in the Ethernet submenu to return to the EXTEND-BOOTWARE menu.

Enter **1** in the EXTEND-BOOTWARE menu to run the new software.

Using Xmodem to upgrade software through the console port

Enter **2** in the EXTEND-BOOTWARE menu to access the Serial submenu.

```
==========================<Enter Serial SubMenu>==========================
|Note:the operating device is cfa0                                        |
|<1> Download Application Program To SDRAM And Run                        |
```

```
|<2> Update Main Application File                                          |
|<3> Update Backup Application File                                        |
|<4> Update Secure Application File                                        |
|<5> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
============================================================================
Enter your choice(0-5):
```

Serial submenu options

Item	Description
<1> Download Application Program To SDRAM And Run	Download a system software image to the SDRAM through the serial port and run the image. This option is available only if password recovery capability is enabled.
<2> Update Main Application File	Upgrade the main system software image.
<3> Update Backup Application File	Upgrade the backup system software image.
<4> Update Secure Application File	Upgrade the secure system software image.
<5> Modify Serial Interface Parameter	Modify serial port parameters.
<0> Exit To Main Menu	Return to the EXTEND-BOOTWARE menu.

Enter **5** in the Serial submenu to change the baud rate of the serial port.

If you use the baud rate of 9600 bps, skip this step and go to step 10.

Make sure the terminal and the serial port use the same baud rate.

```
==============================<BAUDRATE SET>==============================
|Note:'*'indicates the current baudrate                                  |
|     Change The HyperTerminal's Baudrate Accordingly                    |
|-------------------------<Baudrate Available>-------------------------|
|<1> 9600(Default)*                                                      |
|<2> 19200                                                               |
|<3> 38400                                                               |
|<4> 57600                                                               |
|<5> 115200                                                              |
|<0> Exit                                                                |
============================================================================
Enter your choice(0-5):
```

Enter an appropriate baud rate option. For example, enter **5** to select 115200 bps.

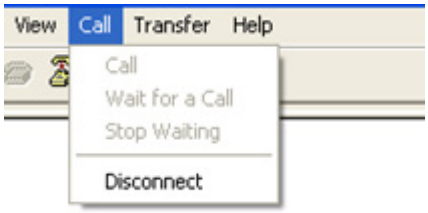
```
Baudrate has been changed to 115200 bps.
Please change the terminal's baudrate to 115200 bps, press ENTER when ready.
```

NOTE:

The size of a .bin file is typically over 10 MB. Even at 115200 bps, the download takes about 30 minutes.

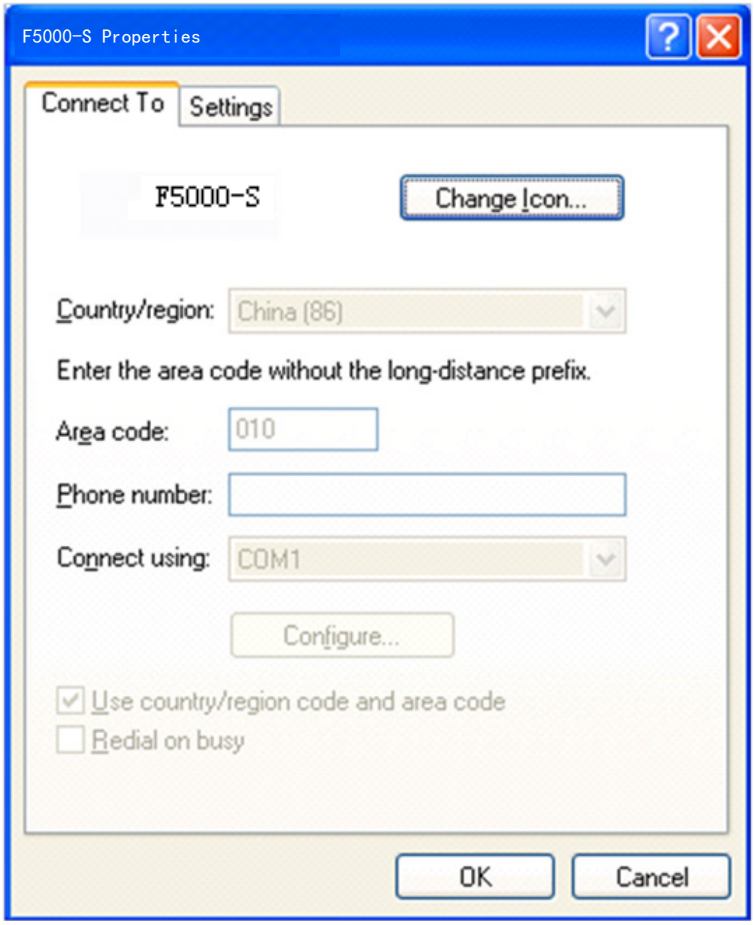
Select **Call** > **Disconnect** in the HyperTerminal window to disconnect the terminal from the firewall.

Disconnecting the terminal



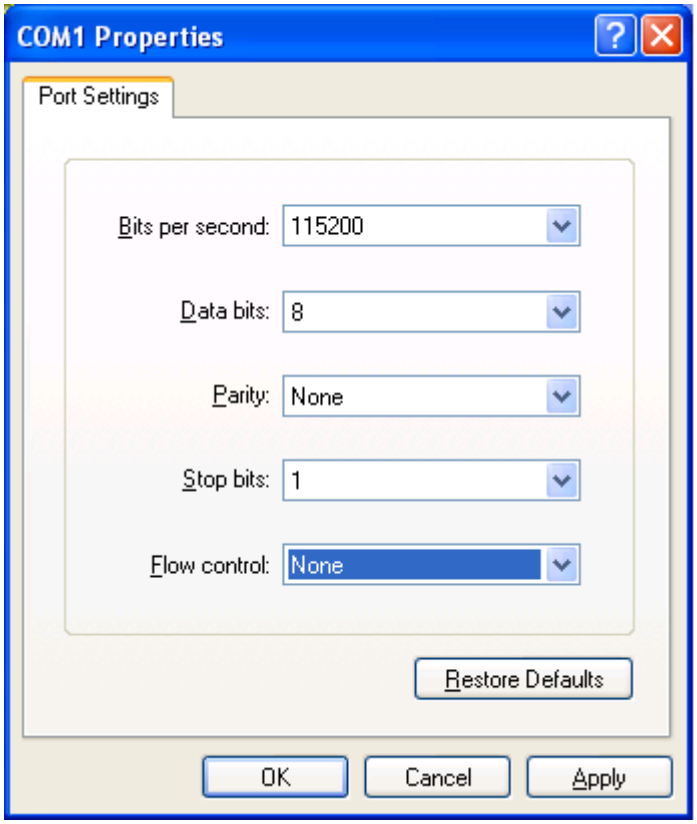
Select **File** > **Properties**, and in the **Properties** dialog box, click **Configure**.

Setting firewall properties



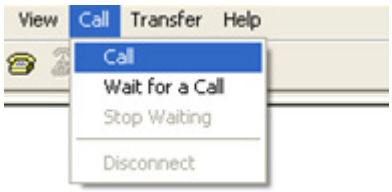
Select **115200** from the **Bits per second** list, and click **OK**.

Modifying the baud rate



Select **Call** > **Call** to reestablish the connection.

Reestablishing the connection



Press **Enter** in the BootWare interface.

```
The current baudrate is 115200 bps
==============================<BAUDRATE SET>==============================
|Note:'*'indicates the current baudrate                                  |
|     Change The HyperTerminal's Baudrate Accordingly                    |
|-------------------------<Baudrate Available>-------------------------|
|<1> 9600(Default)                                                       |
|<2> 19200                                                               |
|<3> 38400                                                               |
|<4> 57600                                                               |
|<5> 115200*                                                             |
|<0> Exit                                                                |
==========================================================================
Enter your choice(0-5):
```

Enter **0** to return to the Serial submenu.

```
==========================<Enter Serial SubMenu>==========================
```

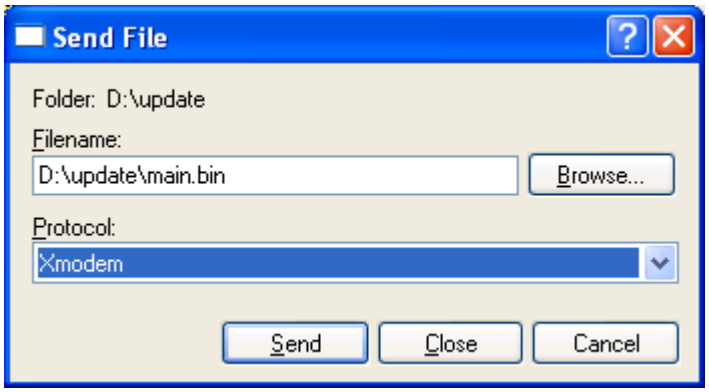
```
|Note:the operating device is cfa0                                          |
|<1> Download Application Program To SDRAM And Run                          |
|<2> Update Main Application File                                           |
|<3> Update Backup Application File                                         |
|<4> Update Secure Application File                                         |
|<5> Modify Serial Interface Parameter                                      |
|<0> Exit To Main Menu                                                      |
==============================================================================
Enter your choice(0-5):
```

Choose an option from options **2** to **4**. For example, to upgrade the main system software image, enter **2**.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCC
```

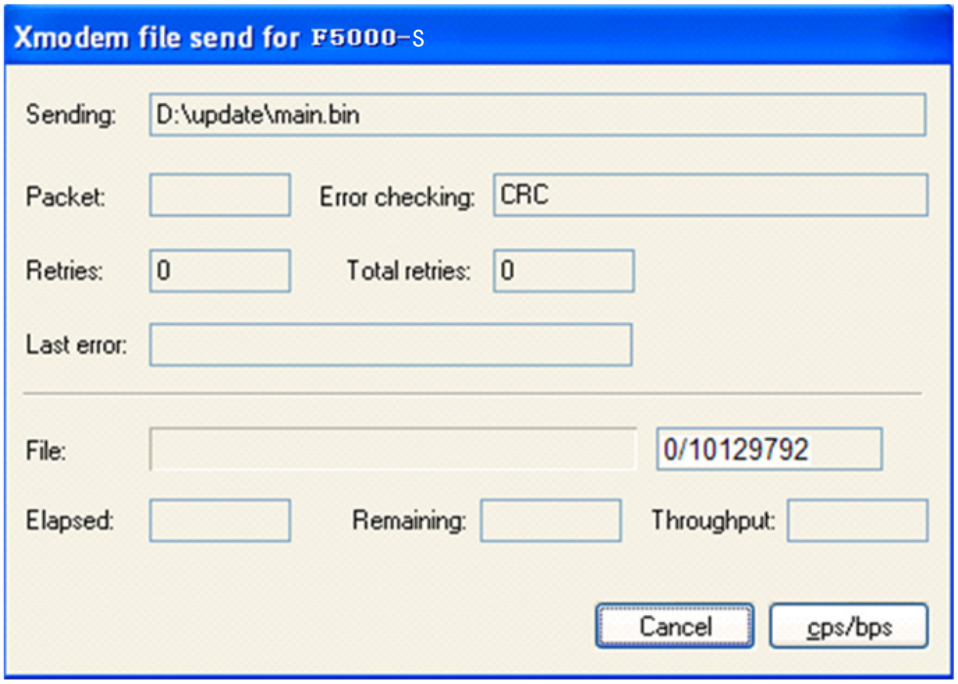
Select **Transfer** > **Send File** in the HyperTerminal window. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

File transmission dialog box



Click **Send**.

File transfer progress



When the Serial submenu appears after the file transfer is complete, enter **0** at the prompt to return to the EXTEND-BOOTWARE menu.

```
Download successfully!
23446448 bytes downloaded!
Input the File Name:main.bin
Updating File cfa0:/main.bin.........................................
.................................................Done!

============================<Enter Serial SubMenu>============================
|Note:the operating device is cfa0                                          |
|<1> Download Application Program To SDRAM And Run                          |
|<2> Update Main Application File                                           |
|<3> Update Backup Application File                                         |
|<4> Update Secure Application File                                         |
|<5> Modify Serial Interface Parameter                                      |
|<0> Exit To Main Menu                                                      |
==============================================================================
Enter your choice(0-5):
```

Enter **1** in the EXTEND-BOOTWARE menu to boot the system.

If you are using a download rate other than 9600 bps, change the baud rate of the terminal to 9600 bps. If the baud rate has been set to 9600 bps, skip this step.

Upgrading the BootWare

You can upgrade the BootWare from the CLI or BootWare menus.

Upgrading the BootWare from the CLI

Whether a .btw file is compressed together with a .bin file depends on the software release. Please check it with HP technical support. This section describes only how to upgrade the BootWare from the CLI.

To upgrade the BootWare from the CLI:

Use FTP or TFTP to download or upload the new BootWare image file to the root directory of the storage medium on the firewall.

Use the bootrom upgrade command to upgrade the BootWare.

```
<System> bootrom update file cfa0:/main.btw
  This command will update bootrom file, Continue? [Y/N]:y
  Now updating bootrom, please wait...

 Updating basic bootrom!

 Update basic bootrom success!
 Updating extended bootrom!

 Update extended bootrom success!
 Update bootrom success!
<System>
```

Use the reboot command to reboot the firewall.

Upgrading the BootWare from BootWare menus

This BootWare upgrade method is available only if password recovery capability is enabled.

Accessing the EXTEND-BOOTWARE menu

See "Accessing the EXTEND-BOOTWARE menu."

Using TFTP/FTP to upgrade the BootWare through an Ethernet port

Enter **7** in the BootWare menu to access the BootWare operation submenu.

```
=========================<BootWare Operation Menu>=========================
|Note:the operating device is cfa0                                        |
|<1> Backup Full BootWare                                                 |
|<2> Restore Full BootWare                                                |
|<3> Update BootWare By Serial                                            |
|<4> Update BootWare By Ethernet                                          |
|<0> Exit To Main Menu                                                    |
===========================================================================
Enter your choice(0-4):
```

BootWare operation submenu options

Item	Description
<1> Backup Full BootWare	Back up the entire BootWare.
<2> Restore Full BootWare	Restore the entire BootWare.
<3> Update BootWare By Serial	Upgrade the BootWare through the serial port.
<4> Update BootWare By Ethernet	Upgrade the BootWare through the Ethernet port.

Item	Description
<0> Exit To Main Menu	Return to the BootWare menu.

Enter **4** to enter the Ethernet submenu.

```
==================<BOOTWARE OPERATION ETHERNET SUB-MENU>==================
|<1> Update Full BootWare                                                 |
|<2> Update Extend BootWare                                               |
|<3> Update Basic BootWare                                                |
|<4> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
==========================================================================
Enter your choice(0-4):
```

Ethernet submenu options

Item	Description
<1> Update Full BootWare	Upgrade the entire BootWare.
<2> Update Extend BootWare	Upgrade the extended section of the BootWare.
<3> Update Basic BootWare	Upgrade the basic section of the BootWare.
<4> Modify Ethernet Parameter	Modify Ethernet settings.
<0> Exit To Main Menu	Return to the BootWare menu.

Enter **4** to configure the network settings.

```
=========================<ETHERNET PARAMETER SET>=========================
|Note:       '.' = Clear field.                                           |
|            '-' = Go to previous field.                                  |
|          Ctrl+D = Quit.                                                 |
==========================================================================
Protocol (FTP or TFTP) :TFTP
Load File Name           :main.btw
                            :
Target File Name         :main.btw
                            :
Server IP Address       :192.168.0.2
Local IP Address        :192.168.0.1
Gateway IP Address      :0.0.0.0
```

For more information about the fields, see Table 10.

To upgrade the entire BootWare, enter **1** on the Ethernet submenu.

```
==================<BOOTWARE OPERATION ETHERNET SUB-MENU>==================
|<1> Update Full BootWare                                                 |
|<2> Update Extend BootWare                                               |
|<3> Update Basic BootWare                                                |
|<4> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
==========================================================================
Enter your choice(0-4): 1
Loading............Done!
485756 bytes downloaded!
```

```
Updating Basic BootWare? [Y/N]Y
Updating Basic BootWare...........Done!
Updating Extend BootWare? [Y/N]Y
Updating Extend BootWare...........Done!
==================<BOOTWARE OPERATION ETHERNET SUB-MENU>==================
|<1> Update Full BootWare                                                 |
|<2> Update Extend BootWare                                               |
|<3> Update Basic BootWare                                                |
|<4> Modify Ethernet Parameter                                            |
|<0> Exit To Main Menu                                                    |
==========================================================================
Enter your choice(0-4):
```

After the upgrade is complete, enter 0 twice to return to the BootWare menu, and then enter 0 to reboot the system.

Using XMODEM to upgrade the BootWare through the console port

Enter **3** in the BootWare menu to access the Serial submenu.

```
====================<BOOTWARE OPERATION SERIAL SUB-MENU>====================
|<1> Update Full BootWare                                                 |
|<2> Update Extend BootWare                                               |
|<3> Update Basic BootWare                                                |
|<4> Modify Serial Interface Parameter                                    |
|<0> Exit To Main Menu                                                    |
==========================================================================
Enter your choice(0-4):
```

Serial submenu options

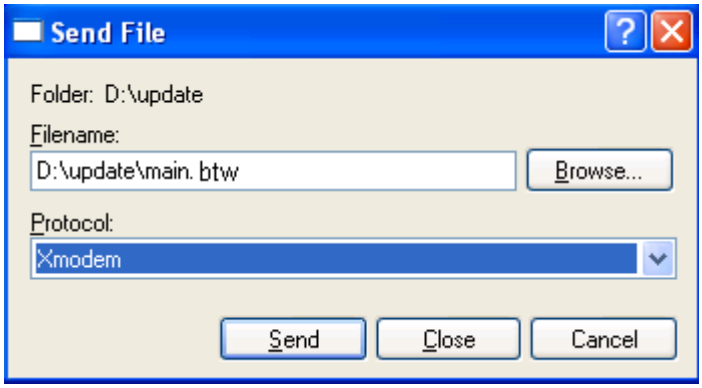
Item	Description
<1> Update Full BootWare	Upgrade the entire BootWare.
<2> Update Extend BootWare	Upgrade the extended section of the BootWare.
<3> Update Basic BootWare	Upgrade the basic section of the BootWare.
<4> Modify Serial Interface Parameter	Modify Serial port settings.
<0> Exit To Main Menu	Return to the BootWare menu.

Enter **1** to upgrade the entire BootWare.

```
Please Start To Transfer File, Press <Ctrl+C> To Exit.
Waiting ...CCCCCCCCCCCCCCCCCCCCCCCCC...
```

In the HyperTerminal window, select **Transfer** > **Send File**. In the dialog box that appears, click **Browse** to select the source file, and select **Xmodem** from the **Protocol** list.

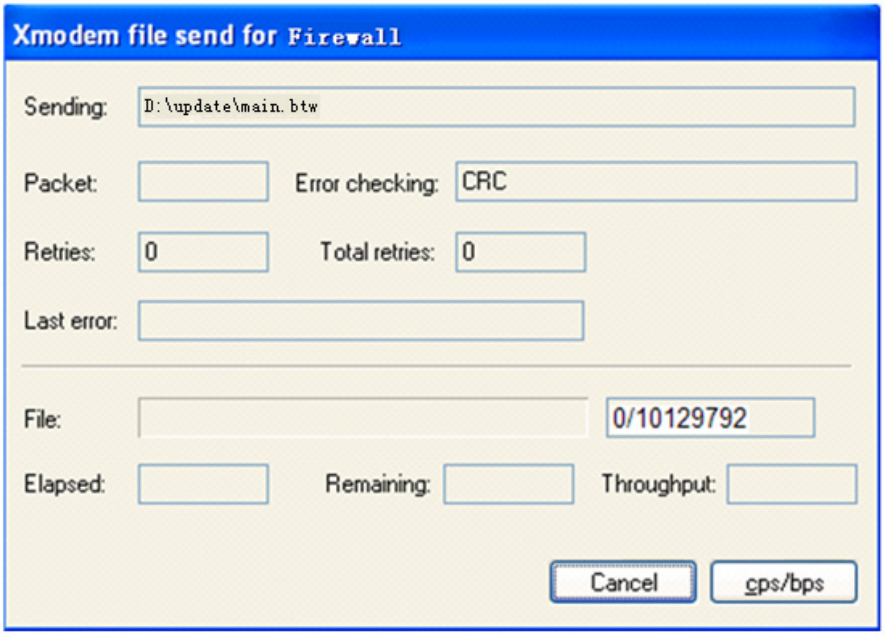
File transmission dialog box



Click **Send**.

The following dialog box appears:

File transfer progress



After the file transfer is complete, the following messages appear:

```
Download successfully!
485756 bytes downloaded!
Updating Basic BootWare? [Y/N]Y
Updating Basic BootWare..........Done!
Updating Extend BootWare? [Y/N]Y
Updating Extend BootWare..........Done!

====================<BOOTWARE OPERATION SERIAL SUB-MENU>====================
|<1> Update Full BootWare                                                  |
|<2> Update Extend BootWare                                                |
|<3> Update Basic BootWare                                                 |
|<4> Modify Serial Interface Parameter                                     |
|<0> Exit To Main Menu                                                     |
```

```
================================================================================
Enter your choice(0-4):
```

After the upgrade is complete, enter **0** twice to return to the BootWare menu and then enter **0** in the BootWare menu to reboot the system.

Managing files from BootWare menus

To change the attribute of a system software image, retrieve files, or delete files, enter **4** in the EXTEND-BOOTWARE menu.

The following File Control submenu appears:

```
==============================<File CONTROL>==================================
|Note:the operating device is cfa0                                           |
|<1> Display All File(s)                                                     |
|<2> Set Application File type                                               |
|<3> Delete File                                                             |
|<0> Exit To Main Menu                                                       |
================================================================================
Enter your choice(0-3):
```

File Control submenu options

Item	Description
<1> Display All File(s)	Display all files.
<2> Set Application File type	Change the attribute of a system software image.
<3> Delete File	Delete files.
<0> Exit To Main Menu	Return to the EXTEND-BOOTWARE menu.

Displaying all files

To display all files on the storage medium, enter **1** in the File Control submenu:

```
Display all file(s) in cfa0:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
================================================================================
|NO. Size(B)   Time                    Type   Name                           |
|1   10715     Jul/31/2013 08:59:06    N/A    cfa0:/system.xml               |
|2   891       Jul/04/2013 11:32:04    N/A    cfa0:/default_ca.cer           |
|3   1411      Jul/04/2013 11:32:04    N/A    cfa0:/default_local.cer        |
|4   3178      Jul/31/2013 08:59:08    N/A    cfa0:/startup.cfg              |
|5   334945    Jul/29/2013 13:33:26    N/A    cfa0:/default.diag             |
|6   23446448  Jul/30/2013 17:17:52    M      cfa0:/f5000-s.bin              |
================================================================================

==============================<File CONTROL>==================================
|Note:the operating device is cfa0                                           |
|<1> Display All File(s)                                                     |
|<2> Set Application File type                                               |
|<3> Delete File                                                             |
```

```
|<0> Exit To Main Menu                                                        |
==============================================================================
Enter your choice(0-3):
```

Changing the attribute of a system software image

System software image file attributes include main (M), backup (B), and secure (S). You can store only one main image, one backup image, and one secure image on the firewall. A system software image can have any combination of the M, B, and S attributes. If the file attribute you are assigning has been assigned to an image, the assignment removes the attribute from that image, and the image is marked as N/A if it has only that attribute. The file of the N/A type cannot be used at device startup.

For example, the file main.bin has the M attribute, and the file update.bin has the S attribute. After you assign the M attribute to update.bin, the attribute of update.bin changes to M+S and the attribute of main.bin changes to N/A.

NOTE:

You cannot remove or assign the S attribute in the File Control submenu.

To change the attribute of a system software image:

Enter **2** in the File Control submenu.

```
'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
==============================================================================
|NO. Size(B)   Time                    Type   Name                          |
|1   23446448  Feb/18/2013 09:14:24    M      cfa0:/main.bin                |
|2   23446448  Feb/17/2013 16:34:14    N/A    cfa0:/f5000-s.bin             |
|0   Exit                                                                   |
==============================================================================
Enter file No:
```

Enter the number of the file you are working with, and press **Enter**.

```
Modify the file attribute:
==============================================================================
|<1> +Main                                                                   |
|<2> -Main                                                                   |
|<3> +Backup                                                                 |
|<4> -Backup                                                                 |
|<0> Exit                                                                    |
==============================================================================
Enter your choice(0-4):
```

Enter a number in the range of 1 to 4 to add or delete a file attribute for the file.

```
Set the file attribute success!
```

Deleting files

When storage space is insufficient, you can delete files to free up storage space.

To delete files:

Enter **3** in the File Control submenu.

```
Deleting the file in cfa0:
 'M' = MAIN      'B' = BACKUP      'S' = SECURE      'N/A' = NOT ASSIGNED
```

```
==========================================================================
|NO. Size(B)   Time                    Type   Name                       |
|1   10715     Jul/31/2013 08:59:06    N/A    cfa0:/system.xml           |
|2   891       Jul/04/2013 11:32:04    N/A    cfa0:/default_ca.cer       |
|3   1411      Jul/04/2013 11:32:04    N/A    cfa0:/default_local.cer    |
|4   3178      Jul/31/2013 08:59:08    N/A    cfa0:/startup.cfg          |
|5   3178      Jul/29/2013 13:33:26    N/A    cfa0:/test.cfg             |
|6   334945    Jul/29/2013 13:33:26    N/A    cfa0:/default.diag         |
|7   23446448  Jul/30/2013 17:17:52    M      cfa0:/f5000-s.bin          |
|0   Exit                                                               |
==========================================================================
Enter file No:
```

Enter the number of the file you want to delete and press **Enter**.

When the following prompt appears, enter **Y**.

```
The file you selected is cfa0:/test.cfg,Delete it? [Y/N]Y
Deleting.............Done!
```

Handling software upgrade failures

If a software upgrade fails, the system runs the old software version. To handle a software failure:

Check the physical ports for a loose or incorrect connection, and verify that the LEDs are reflecting the correct port status.

If you are using the console port for file transfer, check the HyperTerminal settings (including the baud rate and data bits) for any wrong setting.

Check the file transfer settings:

- If XMODEM is used, you must set the same baud rate for the terminal as for the console port.
- If TFTP is used, you must enter the same server IP addresses, file name, and working directory as those set on the TFTP server.
- If FTP is used, you must enter the same FTP server IP address, source file name, working directory, and FTP username and password as those set on the FTP server.

Check the FTP or TFTP server for incorrect settings.

Check that the CF card has enough space for the upgrade file.

If the message "Something is wrong with the file" appears, check the file for file corruption.

HP SECPATH5000FS_5000FC-CMW520-R3811P10

Release Notes

Software Feature Changes

© Copyright 2017 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.
The information in this document is subject to change without notice.

Contents

Release R3811P10

This release has no feature changes.

Release R3811

This release has the following changes:

- New feature: Tiny TCP fragment attack protection

New feature: Tiny TCP fragment attack protection

Enabling tiny TCP fragment attack protection

The tiny TCP fragment attack protection function enables the device to drop tiny TCP fragments to prevent attacks that use tiny TCP fragments. As defined in RFC 1858, tiny TCP fragments refer to first fragments smaller than 20 bytes and non-first fragments with an offset no larger than 8.

To enable tiny TCP fragment attack protection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable tiny TCP fragment attack protection.	**attack-defense tcp fragment enable**	By default, tiny TCP fragment attack protection is enable.

Command reference

attack-defense tcp fragment enable

Use **attack-defense tcp fragment enable** to enable tiny TCP fragment attack protection.

Use **undo attack-defense tcp fragment enable** to disable tiny TCP fragment attack protection.

Syntax

attack-defense tcp fragment enable

undo attack-defense tcp fragment enable

Default

Tiny TCP fragment attack protection is enable.

Views

System view

Default command level

2: System level

Usage guidelines

This command enables the device to drop tiny TCP fragments to prevent attacks that use tiny TCP fragments.

Examples

Enable tiny TCP fragment attack protection.

```
<Sysname> System-view
[Sysname] attack-defense tcp fragment enable
```