

Quickstart Guide for SSL Offloaders Running 4.1 Firmware

Prepared by SonicWALL, Inc.

01/20/2003

Before you start:

This guide can be used to quickly set up a SonicWALL SSL device with commonly used settings for a testing or pilot environment. All information contained in this guide is also contained in the product documentation, which provides far more detail than this paper. It is advised that you read this guide and refer to the product documentation for in-depth details on commands and configuration.

At present, most recent version of firmware for the SonicWALL SSL device is 4.1.0.12. Please note that this guide is for the 4.1 firmware release only - the commands and settings described in this paper may not work with older firmware versions such as 1.x, 2.x, or 3.x.

SonicWALL recommends that the SSL device have version 3.2.0.28 or later of the firmware installed when used in a testing, pilot, or production environment. Notes on how to upgrade a SSL device are included at the end of this guide. You can verify the firmware version from the console port menu by issuing the 'show version' command. You can obtain SonicWALL firmware via two methods: it's on the CD that came with the SSL devices (inside a plastic envelope inside the shipping box), or you can download it directly from the SonicWALL customer website at <https://www.mysonicwall.com>. You will need a valid username and password to access the site, and the SSL device must be registered first before you download firmware updates.

The SSL device has two modes of operation – a simple 'in-line/two-port' configuration where all traffic is passed across both Ethernet ports of the SSL devices, and an advanced 'one-port' configuration where traffic passes through the 'Network' port only (the 'Server' port is disabled and not used). You should first determine the mode of operation you will be using before continuing with this paper.

Before you install the device into your network environment, it is best to first use the Console port to assign the SSL device an IP address, netmask, default gateway, and set the device for one-port or two-port mode, save the configuration, and reboot the SSL device.

If this is a factory default SSL device, or has had its configuration erased and restored to factory settings, you should perform the following steps to ensure the SSL device is ready to be connected and programmed with keys/certs and server definitions.

Basic SSL Device Settings:

NOTE: To make configuration changes, you must first enter into the 'enable' menu by issuing the command 'enable', and then issuing the command 'configure' to enter into the configuration submenu. To exit the 'configuration' menus and submenus, enter the command 'exit' until you are returned to the 'enable' menu. The prompt will change depending upon what menu or submenu you are in – the basic 'access' menu uses a '>' prompt and the 'enable' menu uses a '#' prompt. All changes become active as soon as they are entered. To save your configuration changes, issue the command 'write flash' when in the 'enable' menu.

1. Power up the SSL device and attach a workstation to the Console port of the SSL device (speed 115200, 8 data bits, parity none, 1 stop bit, flow control none) with a terminal-emulation program such as HyperTerminal, and a standard DB9 null-modem cable that ships with the device. The device should display a command line prompt displaying the device's default name ending in a '>' – this is the basic 'access' menu. Check the firmware version by issuing the command 'show version'. It should report back that the version is "SSL Release 4.1.0.12". If it displays an earlier version than this, you will need to upgrade to the most recent release of 4.1 firmware to utilize the settings in this technote. If the Console port does not display a command-line interface and instead displays a number-based menu, the unit is running 2.x firmware and will need to have several firmware upgrades applied to it before it is capable of running 4.1 firmware. **It is not possible to upgrade a SSL device running 2.x firmware directly to 4.1 firmware.** The firmware upgrade procedures for these scenarios are covered on page 7-8.
2. Set the mode of the device. By default, SSL devices are set to 'two-port' mode, which means that both the Network and Server interfaces are active and the device is acting as a bridging device (i.e. both interfaces belong to the same logical network). In 'one-port' mode, the device will only use its Network port for all incoming/outgoing traffic, and the Server port will be deactivated. Selecting the mode must be done before you connect the device to your network. For deployments utilizing a load-balancing device, the mode will usually be one-port. For deployments where no load-balancing device is utilized, the mode will usually be two-port. Please note that the terms "one-arm" or "single-port" is sometimes used instead of one-port -- all terms mean the same thing. To set the mode of the device, issue the command 'mode one-port' to put the device into one-port mode, by issuing the command 'no mode one-port' to put the device back into two-port mode.
3. Assign the device an IP address, netmask, and default gateway. In one-port mode, the default gateway will usually be the VLAN gateway address of the routing load-balancer that the SSL device will be attached to. In two-port mode, this will usually be the address of the upstream router on the Network side of the device. If this is set incorrectly the device will not be reachable from subnets other than the local subnet. To assign the SSL device an IP address and subnet mask, issue the command 'ip address x.x.x.x netmask x.x.x.x' (replace x.x.x.x with the IP address and proper mask). To assign the SSL device's default gateway, issue the command 'ip route default x.x.x.x' (replace x.x.x.x with the IP address of the SSL device's default gateway).

4. There are sometimes issues associated with speed and duplex auto-negotiation; SonicWALL currently advises locking the SSL device to 100Mbps full duplex whenever possible. Do this step before you hook the Network port of the SSL device up to a load-balancer or switch, since if the SSL detects Ethernet-level connectivity it will sometimes ignore your attempts to override the default ‘auto-negotiate’ setting. Also, if you are hooking the SSL device to a hub, make sure you lock the SSL device to the appropriate speed of the hub, and to half-duplex (since hubs cannot support full-duplex). To set the speed of an interface on the SSL device, switch to the interface submenu of the interface (while in the configuration menu, enter in ‘interface network’ for the Network port and ‘interface server’ for the Server port) and issue the command ‘speed 100’ or ‘speed 10’. To set the duplex of an interface on the SSL device, switch to the interface submenu of the interface (while in the configuration menu, enter in ‘interface network’ for the Network port and ‘interface server’ for the Server port) and issue the command ‘duplex half’ or ‘duplex full’.
5. Assign the device an ‘access’ password. This will password-protect access to the SSL device’s basic access menu via the Console port and via Telnet. To create an access level password, issue the command ‘password access’ when in configuration mode and then hit the enter key. You will be asked to enter in a new password twice – at the prompts, enter the password you wish to use.
6. Assign the device an ‘enable’ password. This will password-protect access to the enable menu and configuration menu and submenus. Please note that once you do this, the web GUI will then expect a username and this enable password – the default username is ‘admin’ and cannot be changed. To create an enable-level password, issue the command ‘password enable’ when in configuration mode and then hit the enter key. You will be asked to enter in a new password twice – at the prompts, enter the password you wish to use.
7. If you will be using the Web GUI, you must first enable it. By default, SSL devices ship with the Web GUI disabled. To enable web management, issue the command ‘web-mgmt enable’.
8. Save all these changes by doing a ‘write flash’, then reboot the box and plug it in. Once you’ve done all these steps you should be able to access the device successfully across the network from a Telnet client or the web GUI.

NOTE: If you have become completely locked out of a SSL device and no longer know the ‘enable’ or ‘access’ passwords, there is a special password that can be entered on the Console port that will totally reset the device, erasing the config and all settings (that password is: *FailSafe*). Use this only as a last-resort mechanism, as it will reset the device to factory defaults and you will lose all programming on the SSL device.

Other Common SSL Device Settings:

Configuring Global Items (type 'config' to access, type 'exit' when done):

- Issue the command 'hostname _____' and then hit enter/return to set the name of your SSL device (replace blank line with the unique name).
- Issue the command 'ip domain-name _____' and then hit enter/return to set the name of the domain suffix to be used in DNS searches (replace blank line with the domain name).
- Issue the command 'ip name-server x.x.x.x' and then hit enter/return to set the IP address of your DNS server (replace the x.x.x.x with the IP address of your DNS server).
- Issue the command 'ntp server x.x.x.x' and then hit enter/return to set the IP address of your NTP server (replace the x.x.x.x with the IP address of your internal or public NTP server). Please note that in two-port mode the NTP server must be reachable via the Server interface.
- Issue the command 'timezone " _____ "' and then hit enter/return to set the name of your timezone (replace blank line with you're the timezone information – as an example, Central Standard Time/UTC Offset/Central Daylight Time is "CST6CDT").
- Issue the command 'syslog x.x.x.x port yy facility zz' and then hit enter/return to set the destination of all Syslog messages from the SSL device (replace the x.x.x.x with the IP address of your Syslog server, replace yy with the TCP port to send to, and replace zz with the facility level).
- Issue the command 'password idle-timeout xx' and then hit enter/return to set the idle timeout of the passwords on the SSL device (replace xx with the number of minutes the device will keep an idle connection open before closing).

Configuring Basic SSL Servers (type 'config' and then 'ssl' to access, type 'exit' when done):

- Issue the command 'server _____ create' and then hit enter/return to set the name of the 'server' definition (replace blank line with the unique name).
- Issue the command 'ip address x.x.x.x' and then hit enter/return to set the IP address of the 'server' definition (replace the x.x.x.x's with the IP address).
- Issue the command 'sslport 443' and then hit enter/return to set the listening port for the 'server' definition.
- Issue the command 'remoteport ___' and then hit enter/return to set the response port for the 'server' definition (replace blank line with the unique port that the web servers will listen on for traffic being redirected from the SSL devices; this is typically something like port 81).
- Issue the command 'key _____' and then hit enter/return to set the predefined private key object that this 'server' object will use (replace blank line with the name of the predefined key/cert object); for testing purposes, you can use 'default-1024'.
- Issue the command 'cert _____' and then hit enter/return to set the predefined certificate object that this 'server' object will use (replace blank line with the name of the predefined key/cert object); for testing purposes, you can use 'default-1024'.
- Issue the command 'secpolicy _____' and then hit enter/return to set the predefined browser security policy that this 'server' definition will use (replace blank line with the name of the predefined browser security policy); for testing purposes, you can use 'default'.

- [Optional] Issue the command 'suspend' to stop the SSL server object from processing traffic. Issue the command 'activate' to restart the SSL server definition.
- [Optional] Issue the command 'no transparent' and then hit enter/return to switch the 'server' object into proxy mode.
- [Optional] Issue the command 'log-url x.x.x.x port yy facility zzzz' and then hit enter/return to set the destination of the Syslog server you want all HTTP requests for this 'server' object to be logged to (replace x.x.x.x with IP address of the Syslog server, replace yy with the TCP port to use, and replace zzzz with the facility level to use).
- [Optional] Issue the command 'keepalive enable' and then hit enter/return to activate a TCP keepalive against the IP address defined for the server object. To adjust the time between TCP keepalives, type 'keepalive frequency xx' and then hit enter/return (replace xx with the number of seconds you wish to use). To adjust the maximum amount of failures before putting the server object into 'suspend' mode, type 'keepalive maxfailure xxx' and then hit enter/return (replace xxx with number of failures before suspending

Configuring SNMP Settings (type 'config' to access, type 'exit' when done):

- Issue the command 'snmp enable' and then hit enter/return to activate SNMP on the device.
- Issue the command 'snmp contact " _____ "' and then hit enter/return to set the SNMP contact (replace underline with name of contact, make sure you enclose name with quotations).
- Issue the command 'snmp location " _____ "' and then hit enter/return to set the SNMP location (replace underline with name of location, make sure you enclose name with quotations).
- Issue the command 'snmp default community " _____ "' and then hit enter/return to set the SNMP community string (replace underline with name of string you wish to use, and make sure you enclose name with quotations; please note the default is 'public').
- Issue the command 'snmp trap-host __ x.x.x.x _____' and then hit enter/return to set the SNMP version (v1 or v2c), the trap destination ip (replace x.x.x.x with IP address of trap receiver), and the SNMP community name to send along (replace underline with name of string you wish to use; please note the default is 'public').
- Issue the command 'snmp trap-type generic' and then hit enter/return to set the device to send generic SNMP traps to the trap-host.
- Issue the command 'snmp trap-type enterprise config-changed' and then hit enter/return to set the device to send SNMP traps to the trap-host when the configuration is modified; please refer to the full manual on how to use the other enterprise traps.

Configuring Access-Lists (type 'config' to access, type 'exit' when done):

- To create an access-list, issue the command 'access-list x.x.x.x x.x.x.x ', replacing the first underline with the number of the access-list you want to use, the second underline with "permit" or "deny", the first x.x.x.x with the IP subnet or specific IP address, the second x.x.x.x with the wildcard mask, the third underline with either the specific TCP port or the range of ports. You can add as many lines to the access-list as you need. Please note there is an implicit 'deny any any' at the end of any access-list created.
- Issue the command 'remote-management access-list ' and then hit/enter return to attach an access-list to restrict 'inxcfg' access (replace underline with number of the access-list).
- Issue the command 'snmp access-list ' and then hit/enter return to attach an access-list to restrict SNMP GET access (replace underline with number of the access-list).
- Issue the command 'telnet access-list ' and then hit/enter return to attach an access-list to restrict Telnet access (replace underline with number of the access-list).
- Issue the command 'web-mgmt access-list ' and then hit/enter return to attach an access-list to restrict Web GUI access (replace underline with number of the access-list).

NOTE: Please pay careful attention to the syntax of SSL access-lists. An inadvertent mistake may lead to the inability to remotely manage the device via Telnet or via the Web GUI.

REMEMBER: Issue the command 'write flash' to save your settings when you are finished configuring the SSL device. If you do not, all changes will be lost on the next reboot.

Managing config files and firmware:

It's possible to manipulate the configuration and firmware of the SSL device using the Web GUI. Below are instructions on how to save copies of the configuration, load a copy of the configuration back onto a SSL device, and how to load new firmware onto a SSL device. You can obtain SonicWALL firmware via two methods: it's on the CD that came with the SSL devices (inside a plastic envelope inside the shipping box), or you can download it directly from the SonicWALL customer website at <https://www.mysonicwall.com>. You will need a valid username and password to access the site, and the SSL device must be registered first before you download firmware updates.

Please note that for security reasons, saving the config does not save any of the private keys or certificates stored on the unit. This may pose an issue when uploading a config, as the config will reference key and cert objects that may not be on the unit. To avoid this issue it is necessary to load any saved keys and certs (from when they were initially created and loaded onto the SSL device) onto the unit first, and give them the same names that are referenced in the config file you are about to upload.

Downloading the config via the Web GUI:

- Click on the 'Tools' button on the left, and then select the 'Preferences' tab at the top. From the 'running config' section, click on the 'download' link. This will bring up the current running config in a new browser window. From this window, you may save a copy of the config.

Uploading a config via the Web GUI:

- Click on the 'Tools' button on the left, and then select the 'Preferences' tab at the top. In the 'Configuration File Upload' section, click on the 'browse' button to specify the location of the new configuration file. Once chosen, click on the 'Open' button, and then the 'Upload' button to transfer the config onto the SSL device.

Loading a new software image via the new Web GUI (versions 3.x and newer):

1. Check to see if the Web GUI is enabled on the unit via the console port or via Telnet (the command to enable it is 'web-mgmt enable').
2. Open up the Web GUI by pointing a web browser (IE 5.5 and newer, Netscape 4.x and newer, Opera 5.x and newer) at the IP address of the SSL Unit. Enter in 'admin' for the username and whatever enable-level password you have configured for the unit.
3. Click the 'Tools' button to change menus, and then select the 'Firmware' tab.
4. Use the 'Browse' button to locate the new version of the software on your local system.
5. Use the 'Upload' button to transfer the new version to the SSL Unit.
6. Use the 'Install' button to install the new version.
7. Once the new version is installed, select the 'Restart' tab and click on the 'Reboot' button. The unit may take up to 5 minutes to reboot and install the new software.
8. Log back into the Web GUI and click on the 'General' button, and select the 'Status' tab. The new version numbers will be shown under the "Firmware Version" and "Release" headings.

Loading a new software image via the 'inxcfg' utility (when upgrading from 2.x):

1. Download and install the version of the 'inxcfg' utility matched to the firmware currently on the device. The matched version will come with the firmware package for that version.
2. Start the 'inxcfg' utility and issue the command 'attach ip x.x.x.x' (replace x.x.x.x with the IP address of your SonicWALL SSL device).
3. At the '>' prompt enter "copy file flash" (note: in some versions, may be "copy to flash")
4. Enter the path to and the file name of the new flash file.
 - NT or Windows 2000: d:\fw\<<filename>
 - Red Hat Linux: /mnt/cdrom/fw/<filename>
 - Solaris: /cdrom/cdrom0/fw/<filename>Where filename = 'sslia_r.phr', 'sslia_r.phz', or 'cisco.phr' for upgrading a unit that has 1.7 or later currently installed.
Where filename = 'sslia_r_upgrade.phr', 'sslia_r_upgrade.phz', or 'cisco.phr' for upgrading a unit that has 1.5 or earlier currently installed (this is rare).
5. Enter "y" at the warning prompt.
6. Press enter and allow five minutes to ensure that the flash has been successfully loaded.
7. Enter "reload" to reboot the device. If you lose connection to the device and cannot re-attach, use the console port to issue a reload.
8. Enter "quit" to exit the configuration manager.

Important notes before you upgrade firmware versions:

- As of firmware version 4.0, all firmware images are signed. Because of this, you will need to use a special upgrade firmware when migrating a SSL device from firmware 3.x to 4.x. And, if it becomes necessary to downgrade a SSL device running firmware 4.1 back to firmware 3.2, you must use a special firmware downgrade image. These images are available from SonicWALL technical support, and from the customer download site at <https://www.mysonicwall.com>.
- Always check to see what version the SSL Device is running before you start. The easiest method to check if you are unsure of what version is currently installed is to attach to the Console port (115200, 8, 1, None for the SonicWALL-branded devices) with the 9-pin null modem cable included with the device. If the console displays a number-based menu, the device is running firmware release 1.x or 2.x. If the console displays a CLI-based menu then it's running firmware release 3.x or newer.
- If you are attempting to upgrade from 1.x or 2.x firmware releases to a 3.x or 4.x release, you must upgrade the device to 3.0.6 first using the older 'inxcfg' utility.
- When using the older 'inxcfg' utility to upgrade the firmware, please note that the upgrade commands changed slightly between versions. For the version of 'inxcfg' that shipped with the 1.x and 2.x packages, the command is 'copy file flash'. With the version of 'inxcfg' that shipped with the 3.x packages, the command is 'copy to flash'.
- The version of 'inxcfg' is matched to each specific firmware release, so it will be necessary to de-install the old version and install a new version if you upgrade the firmware on a SSL device. The matched version of 'inxcfg' is shipped with each version of firmware, except for versions 4.x and newer, as it has been discontinued.
- It's always a good idea to have a console connection active when installing new firmware version so you can monitor the upgrade process when the device reboots with the new

firmware. The SSL devices will provide feedback on whether or not the upgrade process was successful.

Important notes about SSL Devices:

1. As of firmware release 4.1, the older 'inxcfg' utility has been discontinued and is no longer distributed with the firmware. Use the Console port, Telnet, or the Web GUI to configure and monitor SonicWALL SSL devices.
2. You must use the Console port to first set the device to one-port mode or two-port mode, and to set the device's IP address information.
3. If you are unsure of what command to enter, just type in a '?' or hit the TAB key, and it will respond with what commands it expects at that particular prompt.
4. Negating most commands is done with a 'no _____' (replace underline with command to remove).
5. To erase the running configuration, issue the command 'erase startup-config'; to erase the startup configuration, issue the command 'erase running-config'.
6. SNMP traps will have the 'public' community string attached to them unless you explicitly define the community-string at the end of the trap-host command.
7. When attempting to manually set the speed and duplex on an active Ethernet port, it will sometimes ignore your settings and remain set to 'auto'. The simplest way to resolve this is to set the speed and duplex via the console port menu, and to temporarily disconnect the ports before setting it so they are not active.
8. Remember to use the 'ephrsa' command when creating 'server' objects to activate Ephemeral RSA, which is necessary if 40-bit browsers will be using the 'server' object, or if the certificates used for the 'server' object are either Step-Up or SGC certificates. As of firmware version 3.2, this command is now a default for any server definition created.
9. In two-port mode, you cannot use the HTTPS web management GUI from the 'Server' port side -- only the 'Network' port side. This is the only method of remotely accessing the SSL device from the 'Network' port side.

Useful CLI commands for the SSL Accelerators:

'show device' – this will list device details on the device you are currently logged into

'show startup' – this will list the saved configuration of the SSL

'show running' – this will list the running configuration of the SSL

'show interface' – this will display the settings for each Ethernet interface

'show interface stat cont' – this will list a running table of the statistics for the Ethernet interfaces (hit any key to stop the updating)

'show messages' – this will list the diagnostic and operating message log of SSL device

'clear messages' – this will clear out all entries in the message log of the SSL device

'show netstat' – this will list the current UDP and TCP sessions on the SSL device

'show snmp' – this will list all active SNMP settings of the SSL device

'show ssl' – this will list a summary of all Key Associations, Security Policies, SSL Servers, Certificates, and Certificate Groups currently installed on the SSL device

'show ssl errors' – this will list any SSL session errors encountered

'show ssl server' – this will list full details on all server objects

'show ssl statistics cont' - this will list a running table of the statistics for the SSL sessions in progress (hit any key to stop the updating)

'show ssl session-stats' – this will display a table of all cumulative SSL connection statistics on the SSL device for each defined server object

'show flows' – this will display all current TCP/UDP connections on the SSL device

'show version' – this will display the current firmware versions installed on the SSL init

'show diagnostic-report' – this will display *everything* (for tech support use)

'show date' – this will display the current date, time, and timezone for the SSL device

'Show sntp' – this will display details about the NTP servers, their update success/failure count, the stratum level of the NTP server, and the NTP interval currently in use

'show terminal' – best used from Console port; will show you all terminal settings including baud rate

'show sessions' – this will display all active management sessions on the SSL device

'write flash' – this will save all changes from running-config into startup-config

Sample configuration of an SSL Accelerator:

Below is a sample/test configuration of a SonicWALL SSL-R device named “weeble” running in ‘one-port’ mode, with two servers defined:

```
#
# SonicWALL SSL Device Configuration File
#
# Written:      Mon Jan 20 14:11:29 2003 PST
# Inxcfg:      version 4.1 build 200212021602
# Device Type: SSL-R
# Device Id:   S/N 08867c
# Device OS:   MaxOS version 4.1.0 build 200212021602 by reading

### Mode ###

mode one-port

### Interfaces ###

interface network
  auto
end
interface server
  auto
end

### Device ###

ip address 192.168.200.25 netmask 255.255.255.0
hostname weeble
timezone "PST8DST"

### Password ###

password idle-timeout 15

### SNTP ###

sntp interval 28800
sntp server 192.43.244.18

### Static Routes ###

ip route 0.0.0.0 0.0.0.0 192.168.200.1 metric 1

### RIP ###

no rip

### DNS ###

ip name-server 4.2.2.2
no ip domain-name

### Telnet ###

telnet enable

### Web Management ###

web-mgmt port 80
web-mgmt enable
```

Quickstart Guide for SSL Offloaders Running Firmware 4.1

```

### SNMP Subsystem ###

snmp enable
snmp contact "Dave Parry"
snmp location "Lab"
snmp default community "sn00py"
snmp trap-type enterprise cpu-utilization hysteresis 75 90
snmp trap-type enterprise ssl-tps hysteresis 170 190
snmp trap-type enterprise ssl-total-connections hysteresis 600 800
snmp trap-type generic
snmp trap-type enterprise config-changed

### SSL Subsystem ###

ssl
  cert _webManagement_ create
  binhex 526
  =3082020a30820173a003020102020100300d06092a864886f70d010104050030
  =4b311430120603550403130b31302e35302e31362e393131333031060355040a
  =132a53656c662d5369676e65642053534c2041646d696e697374726174696f6e
  =204365727469666963617465301e170d3030303130313038303030305a170d30
  =39313232393038303030305a304b311430120603550403130b31302e35302e31
  =362e393131333031060355040a132a53656c662d5369676e65642053534c2041
  =646d696e697374726174696f6e20436572746966696361746530819f300d0609
  =2a864886f70d010101050003818d0030818902818100c74c5d170e73571a9283
  =eb5165a3fca61ace47c68f7ea38d89665ba7754602d5294f5c448b4f5d48803f
  =d0a54f812f37c684111f0de42b9faef9e0715b048e91085fd2247ae4505dda7c
  =3e6e13f84203ac6590290792122d02b6b84a4be41bb03c2e4f414dd8b548a4f9
  =a8703054c3d00ff5cfe427552be7ee8cb89b54cd5c610203010001300d06092a
  =864886f70d0101040500038181009ff711f330cedc38d7babe0f4aaac8caf6c6a
  =8daf7985f294092060908f3392374ac5e855a86e05a7f1752a2d703a7464c338
  =773a6d0c31f846e310654989d5269ee1b147e38610f37a893b3b6e11638f53de
  =8135b3fe9741db9abeb3449cfce8dd944e89cd3ec20c0060ccfcd1f773b5f4d2
  =bbb0c08046292ccf0b7ef833ca8e
  end
  secpolicy verystrong create
  crypto DES-CBC3-MD5
  crypto DES-CBC3-SHA
  crypto ARC4-MD5
  crypto ARC4-SHA
  end
  server _webManagement_ create
  ip address 127.0.0.1
  localport 40443
  remoteport 80
  key _webManagement_
  cert _webManagement_
  secpolicy strong
  sslv2 enable
  sslv3 enable
  tlsv1 enable
  session-cache size 20480
  session-cache timeout 300
  session-cache enable
  no transparent
  no clientauth enable
  clientauth verifydepth 1
  clientauth error cert-other-error fail
  clientauth error cert-not-provided fail
  clientauth error cert-has-expired fail
  clientauth error cert-not-yet-valid fail
  clientauth error cert-has-invalid-ca fail
  clientauth error cert-has-signature-failure fail
  clientauth error cert-revoked fail
  sharedcipher error failhtml
  ephemeral error failhtml
  certgroup clientauth defaultCA
  no httpheader client-cert
  no httpheader server-cert
  no httpheader session

```

Quickstart Guide for SSL Offloaders Running Firmware 4.1

```
no httpheader pre-filter
httpheader prefix "SSL"
ephrsa
keepalive frequency 5
keepalive maxfailure 3
no keepalive enable
end
server test create
  ip address 10.5.12.200
  localport 40443
  remoteport 80
  key default-1024
  cert default-1024
  secpolicy default
  sslv2 enable
  sslv3 enable
  tlsv1 enable
  session-cache size 20480
  session-cache timeout 300
  session-cache enable
  no clientauth enable
  clientauth verifydepth 1
  clientauth error cert-other-error fail
  clientauth error cert-not-provided fail
  clientauth error cert-has-expired fail
  clientauth error cert-not-yet-valid fail
  clientauth error cert-has-invalid-ca fail
  clientauth error cert-has-signature-failure fail
  clientauth error cert-revoked fail
  sharedcipher error failhtml
  ephemeral error failhtml
  no httpheader client-cert
  no httpheader server-cert
  no httpheader session
  no httpheader pre-filter
  httpheader prefix "SSL"
  ephrsa
  keepalive frequency 5
  keepalive maxfailure 3
  no keepalive enable
end
end
```