



Version 2.3

Getting Started Guide

Document Version 0.4.006

Product Code: 010-00003-006

SSL Inspector: Getting Started Guide

COPYRIGHT NOTICE

Copyright © 2006-2010 Netronome Systems, Inc.

All Rights Reserved.

No part of this document or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative work by any means including but not limited to by translation, transformation or adaptation without permission from Netronome Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice.

NO WARRANTY

The technical documentation is being delivered to you **AS-IS** and Netronome Systems makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. The documentation may include technical or other inaccuracies or typographical errors. Netronome reserves the right to make changes without prior notice.

LIABILITY

Regardless of the form of any claim or action, Netronome's total liability to any user of this documentation and the SSL Inspector Appliance, for all occurrences combined, for claims, costs, damages or liability based on any cause whatsoever and arising from or in connection with this documentation shall not exceed the purchase price (without interest) paid by such user.

IN NO EVENT SHALL NETRONOME OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE DOCUMENTATION OR THE SSL INSPECTOR APPLIANCE, BE LIABLE FOR ANY LOSS OF DATA, LOSS OF PROFITS OR LOSS OF USE OF THE DOCUMENTATION OR LOSS OF USE OF THE SSL INSPECTOR APPLIANCE OR FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, MULTIPLE OR OTHER DAMAGES, ARISING FROM OR IN CONNECTION WITH THE DOCUMENTATION OR THE USE OF THE SSL INSPECTOR APPLIANCE EVEN IF NETRONOME HAS BEEN MADE AWARE OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL NETRONOME OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE DOCUMENTATION OR THE SSL INSPECTOR APPLIANCE BE LIABLE TO ANYONE FOR ANY CLAIMS, COSTS, DAMAGES OR LIABILITIES CAUSED BY IMPROPER USE OF THE DOCUMENTATION OR THE SSL INSPECTOR APPLIANCE OR USE WHERE ANY PARTY HAS SUBSTITUTED PROCEDURES NOT SPECIFIED BY NETRONOME.

TRADEMARKS

Microsoft, Windows and Internet Explorer are registered trademarks of Microsoft Corporation.

Firefox and the Firefox logo are trademarks of the Mozilla Foundation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

THIRD PARTY ACKNOWLEDGEMENTS

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Contents

1.	Introduction	1
1.1	Components	1
2.	Initial Setup	2
2.1	Network Connection	3
2.2	Power on the SSL Inspector Appliance	3
2.3	Configure the Management Network	5
2.4	Initial Connection to the Web Interface	6
2.5	Forced Password Change	6
2.6	Set Time Zone	7
2.7	Set Time	7
2.8	Verify Network Configuration	8
2.9	Create Internal Re-signing CA Certificate	9
2.10	Install Known Server Keys	11
2.11	Add a Policy	12
2.12	Configure Traffic Diversion Policy	13
2.13	Configure SSL Inspection Policy	13
2.14	Activate Policy	13
2.15	Monitor	14
3.	Licenses	15
3.1	GNU GENERAL PUBLIC LICENSE	15
3.2	OpenSSL License	17
4.	Technical Support	18

List of Figures

Figure 1 - SSL Inspector Appliance Front Panel	2
Figure 2 - Ethernet Data Ports	3
Figure 3 - LCD Display - Booting	4
Figure 4 - DHCP in progress.....	5
Figure 5 - Initial Login.....	6
Figure 6 - Forced Password Change	7
Figure 7 - Set Time Zone	7
Figure 8 - Set Date and Time.....	8
Figure 9 - Management Network Configuration.....	9
Figure 10 - Default Re-signing Certificate	9
Figure 11 - Internal CAs.....	10
Figure 12 - Internal CA Certificate Credentials	11
Figure 13 - Policies	12
Figure 14 - Adding Policy.....	12
Figure 15 - Edit System Policy	13
Figure 16 - System Monitor	14

List of Tables

Table 1 - Component List	1
Table 2 - Front Panel Functions	2
Table 3 - Appliance Information Display.....	5

1. Introduction

1.1 Components

Carefully unpack the Netronome SSL Inspector Appliance and compare the actual contents with Table 1 to ensure that you have received all ordered components. Then follow the instructions in Section 2 to install and set up the appliance.

Part	Description	Quantity
Netronome SSL Inspector Appliance	A single 2U device, rack mountable	1
2 x D-type handles with mounting screws	To be fitted to the appliance as handles	2
2 x Power Cord	One power cord for each redundant supply	2
Administration and Deployment Guide	Document describing functionality and operational details of the SSL Inspector Appliance (on CD)	1
Getting Started Guide	Document providing brief installation and configuration instructions	1
Release Notes	List of fixes and known issues for this release of the product	1
Safety Notice	A single sheet safety notice	1
22" Rack Mounting Slide (if ordered)	General Devices C-300S rack mounting slide	0 or 1
Total Number of Components		9 or 10

Table 1 - Component List

2. Initial Setup

The front panel ports are depicted in Figure 1 and Table 1 below.

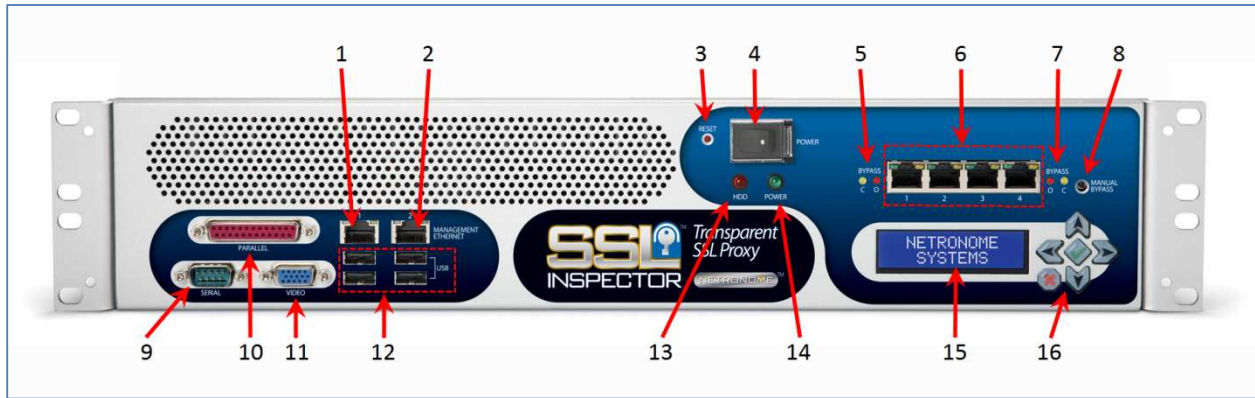


Figure 1 - SSL Inspector Appliance Front Panel

1	Management Ethernet Port	9	Management Serial Port
2	Auxiliary Ethernet Port (reserved)	10	Parallel Port (on some models)
3	System Reset Switch (pinhole)	11	VGA Monitor Port
4	Power Switch	12	USB 2.0 Connectors
5	Link/Activity/ Fail to Wire Status	13	Hard Disk Drive Activity indicator LED
6	Four GigE Data Ports	14	Power LED
7	Link/Activity/Fail to Wire Status	15	Front Panel Display (LCD)
8	Manual Fail to Wire switch (pinhole)	16	Control Keypad

Table 2 - Front Panel Functions

The SSL Inspector Appliance can be configured using one or more of the following methods:

- ❖ **Front panel**
Use the keypad and Liquid Crystal Display (LCD) on the front panel.
- ❖ **Web browser**
Connect the management network cable into the management port (see 1 in Figure 1) on the front panel. The SSL Inspector Appliance’s web interface can be accessed using any of the popular web browsers.
- ❖ **VGA console**
To use this interface, connect a monitor to the front panel VGA monitor port (11) and connect a USB keyboard to one of the front panel USB ports (12).
- ❖ **Serial terminal**

To use this interface, connect a RS-232C serial terminal or terminal emulator to the front panel serial port (9). The terminal emulator should be set to standard VT100 mode. Factory default settings are: 9600 baud, 8 data bits, no parity, 1 stop bit.

❖ **Remote terminal**

The SSL Inspector Appliance command line interface is accessible over the management network using the Secure Shell (SSH) protocol.

The preferred and recommended interface to use is the web interface. This interface provides a complete, simple to navigate, menu driven interface that exposes all management and monitoring functionality.



NOTE: The SSL Inspector Appliance is factory configured to obtain an IP address via DHCP by default. The assigned IP address is displayed on the front panel display (LCD). A different (statically configured) address can be set using the front panel display / keypad. Once the management IP address is known, configuration and management can proceed using the web interface (or in special circumstances the remote console interface).

2.1 Network Connection

Connect the Management Ethernet port (see Table 2) to the management network.

Connect the data network cables according to the mode of operation required. The GigE data network ports are located on the front right side of the appliance (see Figure 1). The ports are numbered 1 to 4 from left to right. When connecting the appliance to the network, one needs to decide how the appliance will be used as the wiring differs between sniffing (also known as IDS) and filtering (also known as IPS) modes. Refer to the Administration and Deployment Guide for a detailed description of these modes.



IMPORTANT: The data ports are GigE **only** and cannot be connected to a 10/100 network



Figure 2 - Ethernet Data Ports

2.2 Power on the SSL Inspector Appliance

Switch on the appliance by toggling the power switch on the front panel (4 in Figure 1). The appliance will:

- ❖ Spin up the hard disk (activity on the Hard Disk Drive Activity indicator LED);
- ❖ Turn on the fans; and

- ❖ Display a message the LCD screen (Figure 3).



Figure 3 - LCD Display - Booting

As soon as the appliance is operational the LCD screen will cycle through a set of status displays. These displays are shown in screens A to I of Table 3.

ID	Screen	Description
A		The SSL Inspector Appliance has three cooling fans installed. The display shows the RPM values for each individual fan and the current power rating.
B		The SSL Inspector Appliance hostname within the configured domain. The factory default setting is localhost.localdomain.
C		The assigned IP address of the SSL Inspector Appliance.
D		The MAC address of the first management Ethernet port.
E		The current CPU utilization for each of the four CPU cores.
F		Average system load for the previous 1, 5 and 15 minutes respectively (not a percentage value).





G		The 'free vs available' system memory ratio as well as the actual free and maximum available memory values.
H		The internal temperature of the SSL Inspector Appliance as well as the temperature of the installed NPU.
I	<p>(a)</p>  <p>(b)</p> 	<p>The port status information for the four SSL Inspector Appliance ports. The possible status values are: Up (port is enabled and connected), LoS (loss-of-signal, network cable may be unplugged), Dis (disabled, or forced down by current failure mode), F2W (fail-to-wire mode) and N/A (not used by current policy). The two sample screens to the left represent:</p> <p>(a) IDS Passive mode (ports 3 and 4 are not used) and</p> <p>(b) IPS fail-to-network mode with port 1 unplugged (failure monitor mirrors link state and forces down port 2) and a SSL Inspector software failure (failure monitor forces ports 3 and 4 to fail-to-wire).</p>

Table 3 - Appliance Information Display

2.3 Configure the Management Network

The management network interface needs to be either statically or dynamically configured to gain access to the SSL Inspector Appliance using the management network.

The factory default setting of the appliance is to use DHCP to configure the management network interface. While configuration using DHCP is in progress, the LCD screen will indicate 'IP address Acquiring...' as shown in Figure 4. The system will continually attempt to acquire an IP address using DHCP until successful or until the interface is statically configured.

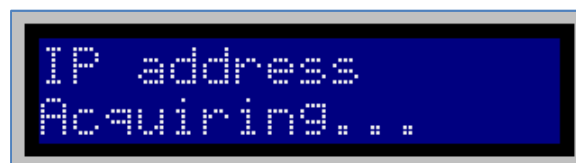


Figure 4 - DHCP in progress



NOTE: If an intrusion was detected all configuration on the front panel will be disabled until the intrusion is cleared using the web interface.

2.4 Initial Connection to the Web Interface

Use a web browser and connect to the SSL Inspector Appliance web interface using the IP address displayed on the LCD screen as the URL. The web browser will display a dialog or message informing you of a problem with the security certificate. This is expected behavior and not an error, and occurs because the current certificate configured on the SSL Inspector Appliance is not known to the web browser. (Please see Section 7 of the *Administration and Deployment Guide* for more information.)

For this session temporarily accept the certificate. Once the SSL Inspector Appliance hostname and IP address have been configured, install the certificate in your browser to avoid the warning dialog or message. The certificate is automatically generated on the SSL Inspector Appliance and uses the hostname or IP address as a credential, so any change in hostname (or IP address, if no hostname was specified) in future will invalidate the current certificate and cause the SSL Inspector Appliance to generate a new certificate.

Once you have accepted the temporary certificate, you will see the login screen as depicted in Figure 5. Log in as user “system” with password “system”.



IMPORTANT: The ‘system’ user is the administrator of the SSL Inspector Appliance and should therefore use a very secure password known only to the administrator of the device.



NOTE: If the “system” user’s password has already been set via another UI, the newly configured password of the user should be used instead of the default password.

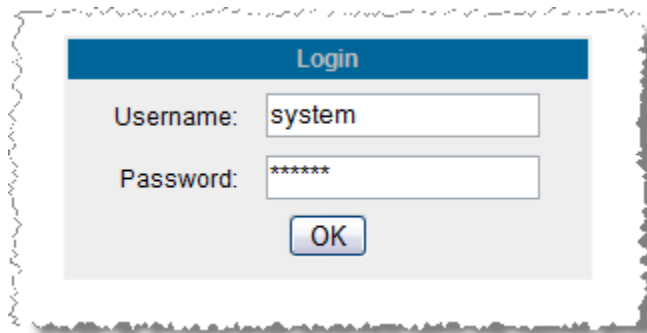


Figure 5 - Initial Login

2.5 Forced Password Change

For security reasons a password change on the system account is enforced immediately after the first login using the default username and password. Please configure a new password for the ‘system’ user.



NOTE: A password must consist of at least 6 characters, and should be made up of a mixture of digits, letters and other printable (and typeable) characters.

home :: session :: password

Changing Password of Admin User system

Parameter	Value
Existing Password	<input type="text"/>
New Password	<input type="text"/>
Confirm Password	<input type="text"/>

Figure 6 - Forced Password Change

2.6 Set Time Zone

Using the web interface, navigate to Platform → Date/Time and then click on the 'Set Time Zone' button. A screen as depicted in Figure 7 is displayed. Changing the time zone requires a reboot of the appliance. Use the drop-down box to select the applicable time zone in which the SSL Inspector Appliance is *deployed*, mark the check box and then click on the 'Save' button.

Set Time Zone

Parameter	Value
Time Zone	US/Eastern <input type="button" value="v"/>

I understand that changing the time zone will reboot the platform.

Figure 7 - Set Time Zone

As certificates used within the SSL Inspector Appliance have expiry dates and times, it is very important to have the correct date and time as well as the correct time zone configured. To automatically keep the time synchronized in future it is recommended to configure a Network Time Protocol (NTP) server and to enable the 'Synchronize Time using NTP' option. Refer to the *Administration and Deployment Guide* for a detailed description.

2.7 Set Time

If use of NTP has been configured as described in section 2.6 then the date and time will be set automatically and the actions described here are not required.

To set the Date and Time of the SSL Inspector Appliance navigate to Platform → Date/Time and then click on the 'Edit Date and Time' button. A screen as depicted in Figure 8 is displayed. Use the dropdown boxes to set the date and time for the appliance and then apply the changes by clicking on the 'Save' button. For convenience the time zone is also displayed.

Action	Description
Editing >>>	7 September 2008 21 : 01 : 34 Time Zone: US/Eastern

Save Cancel

Figure 8 - Set Date and Time

2.8 Verify Network Configuration

By default the SSL Inspector Appliance will configure the management network interface using DHCP. The management network interface can be configured via the web interface, the LCD screen or the command line interface (refer to the *Administration and Deployment Guide*).

To configure the management network interface via the web interface, navigate to the configuration screen shown in Figure 9 via Platform → Management Network and click on the 'Edit' button under 'Configuration'.

The first parameter is the Maximum Transmission Unit (MTU) of the network. For most Ethernet networks this should be set to 1500.

The DHCP configuration option needs to be disabled to manually configure the interface parameters. Once DHCP has been disabled, the IP address, Network Mask and Gateway IP address can be configured. Note that when changing the IP address, the current management session will be terminated when the values are saved.

The hostname for the appliance should typically be a fully qualified name within the local domain. Remember to register the hostname in the Domain Name Server (DNS) if manually configured. Primary and Secondary name server IP addresses can be configured to allow automatic hostname resolution of other devices on the management network.

Management Network

Configuration

Parameter	Value
MAC Address	00:90:FB:13:17:BA
MTU	1500
DHCP	<input checked="" type="checkbox"/> Enable
IP Address	172.16.20.72
Netmask	255.255.252.0
Default Gateway	172.16.20.248
Hostname	qa-sslia-3
Primary Name Server	172.16.20.248
Secondary Name Server	

Figure 9 - Management Network Configuration

2.9 Create Internal Re-signing CA Certificate

The CA certificate to be used for re-signing server certificates must be configured. When the SSL Inspector Appliance is first booted, it automatically creates a unique CA certificate with default fields resembling Figure 10.

home : certificates : internalca

Certificate 102

Subject

Name	Value
commonName	Netronome Default
countryName	US
organizationName	Netronome Systems Customer

Issuer

Name	Value
commonName	Netronome Default
countryName	US
organizationName	Netronome Systems Customer

Details

Field	Value
Certification Authority?	False
Serial Number	1 (0X1)
SHA-1 Fingerprint	5C:62:3B:B6:C1:90:34:2C:90:F0:35:26:03:14:EB:9B:15:4C:54:0D
Valid From	Sep 6 23:23:17 2008 GMT
Valid To	Sep 5 23:23:17 2013 GMT

Figure 10 - Default Re-signing Certificate

Netronome recommends replacing this automatically generated CA certificate with a certificate which identifies your organization, by either importing an existing signed certificate, or by generating a new one with updated information.

To update the information and generate a new CA certificate, navigate to Certificates → Internal Re-signing CAs to reach the screen shown in Figure 11.



Figure 11 - Internal CAs

Clicking on the 'Generate CA Certificate' button opens the screen shown in Figure 12. Enter all the certificate credentials required for the certificate. If the certificate needs to be signed by an external Certification Authority, check the appropriate checkbox to generate a new Certificate Signing Request (CSR). When the 'Save' button is pressed, the certificate will be generated and installed or the CSR will be generated and displayed. If the latter, convey this CSR information to the signing authority – this enables them to issue a signed certificate. Import this signed certificate using the 'Import Signed' button next to the applicable certificate.



NOTE: The default certificate is a self signed certificate.



IMPORTANT: Note that the CSR is only useful if you have a private PKI infrastructure and want your private CA to sign the CA that will be used by the SSL Inspector Appliance. Doing this will ensure that enterprise systems that trust the private CA will also trust the CA used by the SSL Inspector. You should NOT send the CSR to a public certificate issuing authority and request them to sign it.

home :: certificates :: internalca

Generate Internal CA Certificate

Parameter	Value
Common Name	qa-sslia-3
Division/Department/Org. Unit	
Company/Organization -- (required)	Netronome Systems Customer
City/Town/Locality	
Country Code -- (two letter abbrev.)	US
Serial Number	1
Key Size (bits)	1024
Valid For (days)	365 (one year)
Sign With External / Third Party CA	<input type="checkbox"/> Generate Signing Request

Save Cancel

Figure 12 - Internal CA Certificate Credentials

To install a signed certificate and private key, click on the 'Import CA Certificate + Key' button and then paste the PEM formatted certificate and key information into the edit box, or upload the certificate and key as files (encoded as DER, PEM, PKCS#7 or PKCS#12) . Click on the 'Save' button to validate the information – after validation, the system will install the certificate and key.

2.10 Install Known Server Keys

Navigate to Certificates → Known Server Keys and install all known server keys. For each key, first click on the Import button, then paste a PEM formatted key and certificate into the edit box or upload the key and certificate as files (encoded as DER, PEM, PKCS#7 or PKCS#12).

2.11 Add a Policy

Navigate to Policy → Overview. The screen shown in Figure 13 will be displayed.



NOTE: Predefined policies cannot be renamed or deleted. Predefined policies are identified by a double asterisk ‘**’ before and after the name.

All three components of a policy (System, Traffic Diversion and SSL Inspection), are created when a policy specification is added. Each of the three components can be individually viewed or edited. When a policy is deleted, all three components are also deleted.

Activate	Policy Name	Policy Options	Traffic Diversion Rules	SSL Inspection Rules	Rename	Delete
Active >>>	** Bypass (filtering/IPS) Fail to Appliance **	Edit	View	View	Rename	Delete
Activate	** Bypass (filtering/IPS) Fail to Network **	Edit	View	View	Rename	Delete
Activate	** Cut through (sniffing/IDS) INLINE **	Edit	View	View	Rename	Delete
Activate	** Cut through (sniffing/IDS) PASSIVE **	Edit	View	View	Rename	Delete
Activate	** Cut through (filtering/IPS) Fail to Appliance **	Edit	View	View	Rename	Delete
Activate	** Cut through (filtering/IPS) Fail to Network **	Edit	View	View	Rename	Delete

** = Default policy — can be activated or viewed, but not modified.

Note: Policy changes will not affect existing flows.

Figure 13 - Policies

To add a new policy, click on the ‘Add’ button. This will open a screen as shown in Figure 14. Select the mode of operation and give the policy a descriptive name that makes it simple to identify.

Parameter	Value
System Mode	Sniffing / IDS Passive
Policy Name	
Default Rules	<input checked="" type="checkbox"/> Cut through traffic to sites known to be incompatible with SSL **

** Because they use compression, an unsupported cipher-suite, or an unsupported version of SSL/TLS

Figure 14 - Adding Policy

Configure the System Policy by clicking on the 'Edit' button in the System Policy column. The screen shown in Figure 15 will be displayed. Refer to the *Administration and Deployment Guide* for more information on Policy options.

Editing Policy Options

Policy Name: ids_inline_recrypt

General Options

Parameter	Value
System Mode	Sniffing / IDS Inline
SSL Session Log	Enabled
Internal Re-signing CA	Netronome Default / Netronome Systems Customer # 131
Self-Signed Certificate Handling	Accept all self-signed server certificates
Undecryptable SSL Handling	Cut through to attached device
Uncached SSL Session Handling	Cut through to attached device
Known-key Change Handling	Cut through to attached device
Untrusted Cert-chain Handling	Reject (terminate flow)

Plaintext Destination

Parameter	Value
Send to Port(s)	3
Modify Source MAC Address	False
Send on VLAN(s)	-

Failure Mode Options

Mode	Option
Network Failure	Mirror link state between ports 1+2. [code: ids-p2-nf-p2n]
Attached Appliance Failure	Do nothing, except wait for the device to recover from the failure. [code: ids-p2-af-0]
SSL Inspector Software Failure	Enable fail-to-wire and force links down on ports 3+4. [code: ids-p2-sw-f2w+f2a]

Figure 15 - Edit System Policy

2.12 Configure Traffic Diversion Policy

Refer to the *Administration and Deployment Guide* for more information on Traffic Diversion Policy options.

2.13 Configure SSL Inspection Policy

Refer to the *Administration and Deployment Guide* for more information on SSL Inspection Policy options.

2.14 Activate Policy

Any of the available policies can now be activated, but only a single policy can be active at any given time. Navigate to Policy → Overview to obtain a display similar to Figure 13 listing all available policies. Click on the 'Activate' button next to the policy that must be activated. The button will change to indicate that the policy is now active.

2.15 Monitor

The SSL Inspector Appliance is now configured and operational. Navigate to Monitor → Overview to display the system monitor similar to Figure 16. Any errors or problems that are detected in the system will be displayed on this screen.

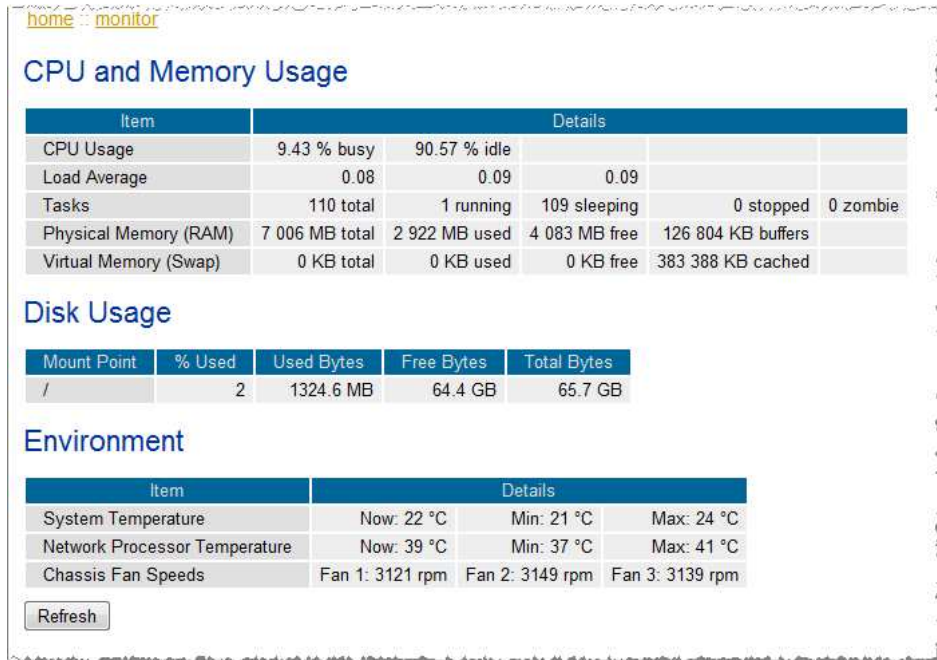


Figure 16 - System Monitor

The configuration described this section is only a very basic system configuration. Please refer to the *Administration and Deployment Guide* for more detailed information.

3. Licenses

3.1 GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".
Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.
1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.
You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.
2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software

Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

3.2 OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

4. Technical Support

To obtain additional information or to provide feedback, please email support@netronome.com or contact the nearest Netronome Systems technical support representative.

Visit <http://support.netronome.com> to download the latest documentation and software, access the knowledge base, or log a support ticket.