P-Series Appliance

Feature Highlights and Quick Start Guide

Feature Highlights

P1		P10	
Interfaces	Two Line-Rate GbE Sensing Ports Two Line-Rate GbE Mirroring Ports SFP Pluggable Module [1]	Interfaces	Two Line-Rate 10 GbE Sensing Ports XPAK Pluggable Module [2]
Inspection Throughput	2 Gbps from 64 Byte to 9,000+ Byte Frames per System	Inspection Throughput	20 Gbps from 64 Byte to 9,000+ Byte Frames per System
Inspection Rate	1,488,096 pps per Port	Inspection Rate	14,880,952 pps per Port
Latency	16 Microseconds	Latency	16 Microseconds
Rule Capacity	1,000 per System	Rule Capacity	650 per System
Number of Flows	2,000,000 per System	Number of Flows	8,000,000 per System
Capture Rate	1,000,000 pps per System	Capture Rate	1,000,000 pps per System
Full Header, Payload Inspection	IPv4 & IPv6	Full Header, Payload Inspection	IPv4
Power	Auto-switching 100-240 VAC	Power	Auto-switching 100-240 VAC
Management	2 10/100Base-T Management Ports 1 RJ-45 Console Port	Management	2 10/100Base-T Management Ports 1 RJ-45 Console Port
Height	1 Rack Unit	Height	1 Rack Unit

Note 1: The P1 appliance uses only Force10 Networks-approved 1G Small-form Factor Pluggable (SFP) laser modules, providing support for SR, LR, ER, and ZR optical interfaces.

Note 2: The P10 appliance uses only Force10 Networks-approved 10G XPAK laser modules.

SFP and XPAK modules must comply with 21 CFR 1040 Class 1 requirements.

Installation Instructions

The following instructions can be used for both the P1 and P10 appliances. During installation, the only noticeable difference between the P1 and P10 appliances is that the P10 has two XPAK ports, while the P1 has four SFP ports.

Attaching the P-Series Appliance to a Rack

Installation Notes: The P-Series appliance is shipped with universal front-mounting brackets (rack ears) attached.

1. Ensure that there is adequate clearance surrounding the rack to permit access and airflow.
2. Secure the appliance in the rack by inserting screws through the connecting ears on each side of the appliance and into the rack post (see Figure 1).

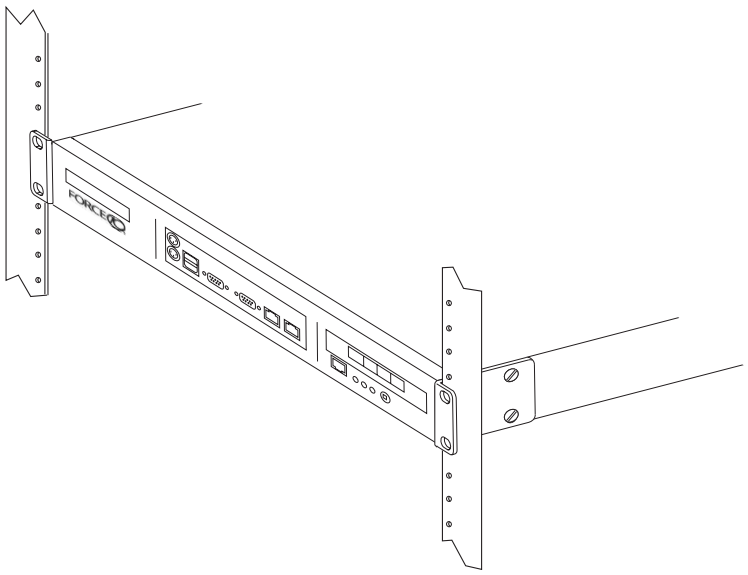

Figure 1 Front-mounting the P-Series Appliance

Making the Electrical Connections

Installation Notes: If you are mounting the P-Series appliance in a rack, Force10 recommends that you do so (as described above) before making the electrical connections.

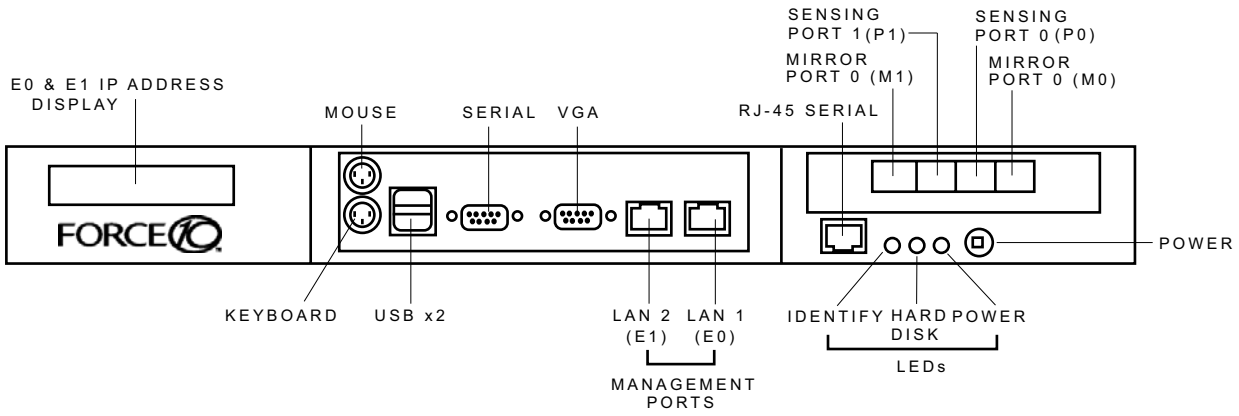

Figure 2 P-Series P1 Appliance (Front View)

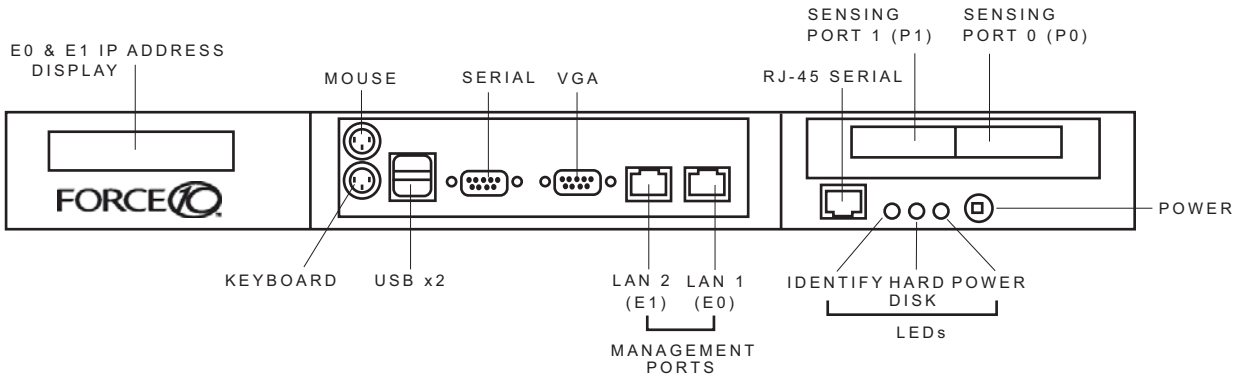

Figure 3 P-Series P10 Appliance (Front View)

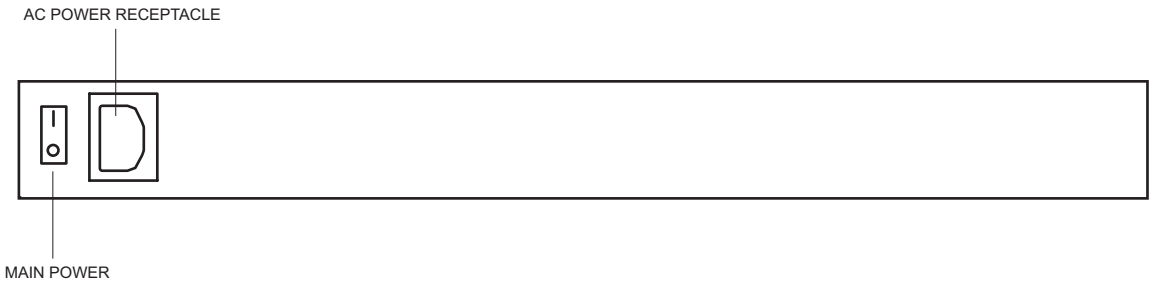

Figure 4 P-Series P1 & P10 Appliances (Rear View)

Label	Description
(LCD screen)	The LCD screen displays the IP address of the appliance next to either “e0:” or “e1:”, which represent LAN ports 1 and 2, respectively.
M1, M0 (on the P1)	These two ports are mirror ports through which copied matched traffic is routed. They accept the 1G small form-factor pluggable modules (SFP).
P1, P0 (on the P1)	These two ports are sensing ports through which traffic is routed. They accept the 1G small form-factor pluggable modules (SFP).
Port 1, Port 0 (on the P10)	These two ports are sensing ports through which traffic is routed. They accept 10G XPAK modules.
(unlabeled RJ-45 serial port next to IDENTIFY)	This port is not used.
IDENTIFY	This LED is not used.
HDD	This LED is blue when the hard disk is accessed.
PWR	This LED is green when the power is on.
(Power Button)	This button turns the appliance on and off. Press and hold the button to turn off the appliance.
(Laser Warning) 	This label in the bottom right corner of the appliance indicates that the appliance is a Class 1 laser product that emits invisible laser radiation. This product complies with CDRH 21 CFR 1040.

Installation Notes: Connections to the sensing, mirroring, and LAN ports require straight-through CAT5 cables.

Step	Task
1	Connect the power cable, a keyboard, mouse, and monitor to the appliance.
2	Connect either LAN 1 port or LAN 2 port on the appliance to the local area network where DHCP is available. If a DHCP server is not available, an IP address can be assigned manually. See "Booting and Configuration" on page 5.
3	For the P1 appliance, install SFPs in the sensing ports (labeled P0 and P1 — see Figure 2) and, optionally, in the mirroring ports (labeled M0 and M1). For the P10 appliance, install XPAKs in the ports labeled Port 1 and Port 0 (see Figure 3). For details, see the separate SFP and XPAK instructions that come with those devices.
4	Connect the sensing ports to the devices from which the appliance will receive traffic: • Traffic originating from the device connected to port 0 will have Channel 0’s rules applied to it. • Traffic originating from the device connected to port 1 will have Channel 1’s rules applied to it.

Step	Task
5	Connect the mirroring ports to the devices that will receive mirrored traffic (P1 only): • Mirror Port 0 mirrors matched traffic from Channel 0. • Mirror Port 1 mirrors matched traffic from Channel 1.
6	Connect the power cable to an AC power source, and switch on the main power on the back of the appliance.
7	Press the power button on the front of the appliance to turn on the device.

Booting and Configuration

During booting, you are prompted to select one of two operating systems: Linux or FreeBSD.

- The Linux option represents Fedora Core 3.
- The FreeBSD option represents FreeBSD version 6.0.

If no choice is made, after a few seconds the Linux option is automatically selected. Once the appliance is booted, perform the following configuration steps:

Step	Task
1	Log in as root with the password **plogin**.
2	Change the password, if desired, with the command **passwd**.
3	If DHCP is not available, use the **system-config-network** command to assign an IP address manually.
4	If desired, modify the host name and/or network configuration using the command **system-config-network**. Other **system-config-*** scripts are available to configure most other system options.

Security Check

The P-Series appliances are remotely accessible only via Secure Shell Daemon (SSHD). However, inspect the configuration, and make sure it meets the security policy requirements of your network before deploying the appliance in a production environment.

Default Behavior

All packets will be forwarded between the appliance ports by default until firmware and the device drivers are loaded. When this is complete, the DPI generates interrupts to the host processor and offers the captured packets in the same way as a standard network interface card in promiscuous mode.

Getting Started

To begin inspecting and filtering traffic you must:

1. Select firmware and specify dynamic rules
2. Select capture/forward policies
3. Generate traffic across the appliance

Complete the following steps:

Selecting Firmware

Step	Task
1	As root, enter the command **mtp** from the Unix command line to invoke a graphical user interface (GUI). • Runtime statistics are displayed upon executing this command.
2	Enter the command **m** from the GUI command line. • From this GUI you can manage dynamic rules, capture/forward policies, and firmware.
3	Select **Manage Firmware** from the Rule Management GUI, and select “null” firmware for the appliance you are using.[3] • See the *P-Series Installation and Operation Guide* for a description of the firmware naming convention. • The firmware *null.null.v143.xc3s5000-4fg900-2* is for the P1 • The firmware *null.null.v143.xc2vp70-6ff1704* is for the P10.
4	Select **Done** and confirm your selection. • This starts the drivers and loads the firmware into the FPGA.

Editing Dynamic Rules

Step	Task
5	Select **Edit Rules** from the Rule Management GUI.
6	Uncomment the rule **alert on c0 icmp any any -> any any (msg:"@icmp";)** by removing the # symbol before the rule. • Visual Editor (*vi*) commands are described in Appendix A of the *P-Series Installation and Operation Guide*.
7	Enter the command **:q!** to exit the *vi* editor, and confirm your changes.

Setting Capture/Forward Policies

Step	Task
8	Select **Manage Rules** from the Rule Management GUI.
9	Select the capture/forward policy *divert* for the rule **alert on c0 icmp any any -> any any (msg:"@icmp";)**.
10	Select **Done** and confirm your selections.
11	Select **Exit** from the Rule Management GUI.

Generating Traffic

Step	Task
12	Run a packet sniffer such as tcpdump on the network interface associated with the appliance.
13	Generate some ICMP traffic to be exchanged between endpoints. • *Endpoints* are two network nodes on opposite sides of the appliance such that traffic between those nodes passes through the appliance. • For example, enter **ping** *destaddress*, where *destaddress* is the IP address of the endpoint on the opposite end of the appliance.
14	If you are using tcpdump, enter the command **tcpdump -i eth2 -n** from the Unix command line. • This prints to standard output all of the packets captured by the DPI (assuming the appliance registers as *eth2*). • If the appliance is operating correctly, you will see the ICMP packets after a few seconds, when the receive buffer is full.

Note 3: The sample firmware and rules files are testing examples only. Force 10 recommends not employing the sample firmware for production IDS/IPS use.

Note 4: Commands **0**, **1**, **2, 3, 4**, and **5** are for Force 10 engineering use only. If a command **1** through **5** is entered by mistake, enter **0** to return to the runtime statistics screen.

Technical Support

Information on operating the appliance can be accessed through manual pages (man pages). The command **man meta** displays the man pages on the command line interface; and **man mtp** displays them on the *Ncurses* interface. Man pages for the compiler can be accessed through **man mtp-compiler**.

- For information on Snort or creating Snort rules visit www.snort.org.
- For detailed information on the P-Series appliances see the *P-Series Installation and Operation Guide* that came with your appliance.