

---



# Premier Services Program (PSP) Tools: Security Overview

---

Software Version 3.0

Extreme Networks, Inc.  
3585 Monroe Street  
Santa Clara, California 95051  
(888) 257-3000  
(408) 579-2800  
<http://www.extremenetworks.com>

Published: May 2008  
Part Number: 120350-00 Rev. 02



Alpine, Alpine 3804, Alpine 3802, Altitude, BlackDiamond, BlackDiamond 6808, BlackDiamond 6816, EPICenter, Ethernet Everywhere, Extreme Ethernet Everywhere, Extreme Networks, Extreme Turbodrives, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, GlobalPx Content Director, the Go Purple Extreme Solution Partners Logo, SentiAnt, ServiceWatch, Summit, Summit24, Summit48, Summit1i, Summit4, Summit5i, Summit7i, Summit 48i, SummitRPS, SummitGbX, Triumph, vMAN, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Summit logos, the Extreme Turbodrives logo, and the Color Purple, among others, are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and other countries. Other names and marks may be the property of their respective owners.

© 2008 Extreme Networks, Inc. All Rights Reserved.

Specifications are subject to change without notice.

Merit is a registered trademark of Merit Network, Inc. Solaris and Java are trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Avaya is a trademark of Avaya, Inc.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org>).

This product contains copyright material licensed from AdventNet, Inc. (<http://www.adventnet.com>). All rights to such copyright material rest with AdventNet.

Use of Open Source Libraries. The Software uses or links to the third party "open source" library(ies). Please read the "Notice" files included with the Software for identification of these libraries and applicable license agreements.



# Contents

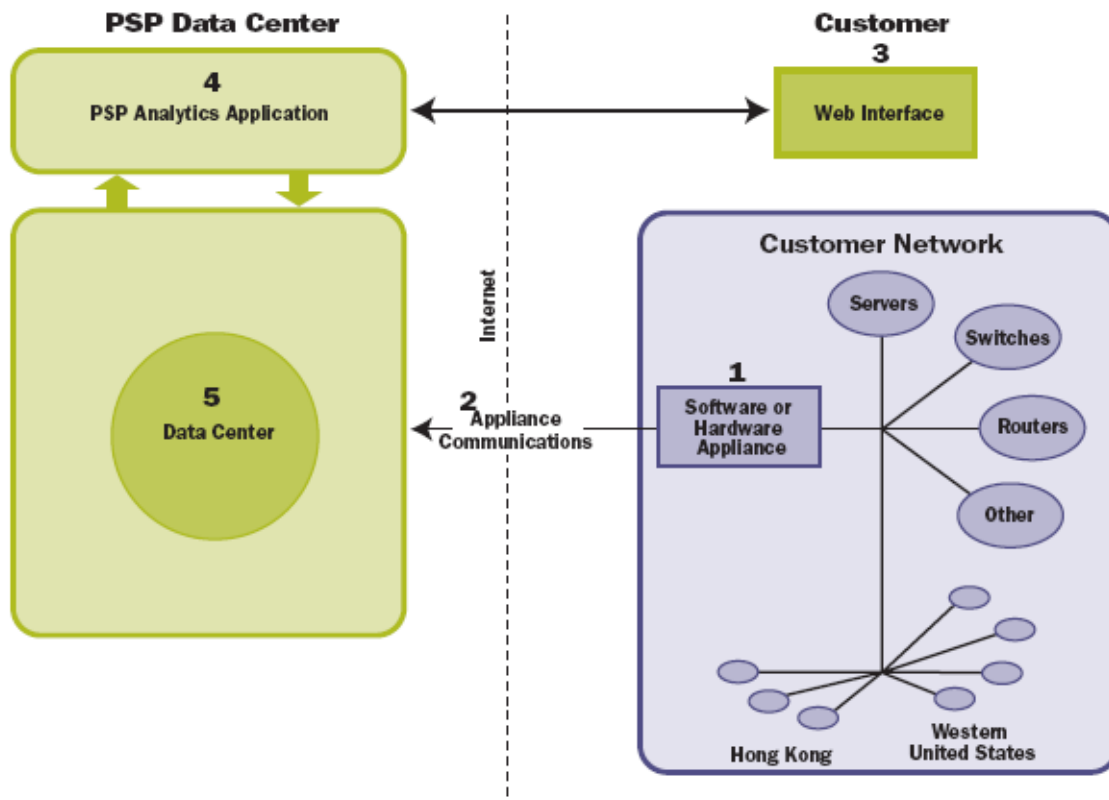
<b>Chapter 1: PSP Security Overview .....</b>	<b>5</b>
PSP Software Appliance and Communications Strategy .....	6
Web Interface Security .....	7
PSP Analytics Application Security .....	7
PSP Data Center Physical Security.....	7



# 1 PSP Security Overview

Extreme Networks – through its Premier Services Program (PSP) – provides an on-demand, hosted solution for network monitoring and analysis of IT infrastructure, including network traffic, routers, switches, storage devices, servers and applications. The PSP software securely collects and transports data from a customer's network devices to the PSP Data Center where it is analyzed and stored. The data is made available to users anytime and anywhere through a hosted web application that provides drill-down analytics, role-specific dashboards, customized reporting and sophisticated alerting.

This document describes the extensive security implemented at all levels of the Premier Services Program's on-demand solution, including security elements within the customer premises, security elements within the PSP Data Center, and communications between those elements.



The document is divided into the following sections:

- PSP Software Appliance and Communications Strategy
- Web Interface Security
- PSP Analytics Application Security
- PSP Data Center Physical Security

# PSP Software Appliance and Communications Strategy

## PSP Software Appliance

**Hardening the software appliance.** The software appliance runs as a service on a Windows server 2000/2003 or XP platform. The appliance software delivered by Extreme Networks contains all the components/services it needs; all non-critical Windows services, aside from basic networking, may be disabled to reduce the attack surface of the appliance server. The customer is responsible for managing the Windows computer hosting the PSP software appliance including patches and updates to the OS.

**Software updates and monitoring.** Extreme Networks continually monitors the health of the appliance to ensure that it is running correctly and is up-to-date. The PSP software running on the customer's Windows computer has an auto-update feature that "pulls" new software versions from the PSP datacenter as they are made available through the software release process.

**Communications between the PSP Software Collector and the PSP Datacenter.** Application communications between the software collector and the Extreme Networks hosted application are secured through Transport Layer Security (TLS). Authentication is performed bi-directionally through RSA 2048-bit X.509 certificates and data is encrypted using 256-bit Advanced Encryption Standard (AES) encryption.

**Communications through Customer's proxy server.** The PSP software appliance can communicate through an HTTP proxy server where the proxy authentication for Internet access is setup to no- or basic-authentication. Communicating through the proxy does not change the security of the communications to the PSP Datacenter described above. Please check the list of verified proxy servers/types in the PSP product documentation.

**No command or control capabilities.** The PSP software collector has no command or control capabilities over any devices in the customer network; it collects read-only performance data.

**Data collection on specified devices only.** The PSP software collector collects data only on those devices that the customer specifies.

**Simple Network Management Protocol (SNMP) data collection.** The PSP software collector collects read-only data utilizing SNMP versions 1, 2c, or 3. SNMP data is collected from the management information bases (MIBs) supported by the customer's devices.

**Flow data collection.** The PSP software collector can be configured by the customer to collect sFlow or NetFlow data only from devices that are explicitly configured to export that data to the software appliance. The PSP software collector is not an in-line device in the communications path, thus it does not alter the reliability or security of network traffic.

**Access controlled through access control lists (ACLs).** As a recommended best practice, the customer should restrict the access of SNMP data by setting the permitted SNMP requestors through ACLs on each device.

## Web Interface Security

Users log in to the PSP tools through a secure web interface. The user has the option to encrypt the data transfer as well for the PSP connection session. The connection between the browser and the web server is secured through industry-standard procedures and protocols, as follows:

**1024-bit authentication and SSL or TLS.** The level of communications encryption is negotiated with the client browser and supports up to 256-bit encryption.

**User ID and password.** Passwords are stored (one-way-encryption) through a secure hash algorithm version 1 (SHA-1) hash so that they cannot be recovered as plain text even with direct database access.

## PSP Analytics Application Security

The PSP application is secured with a combination of internal policies and network security measures.

Internal policies that safeguard the hosted application include the following:

- **Strict rights management.** Rights are restricted to only necessary services and qualified personnel.
- **Limited physical access.** The application servers are within locked cages and safeguarded by card-key access.
- **High Availability.** All the functional components (data and services) have been deployed with full redundancy and failover capability.
- **Database backups and archives.** All data is backed up and archived regularly and securely. The backups include on-line short term disk-based backups for fast recovery as well as tape based backups for longer term and disaster recovery purposes.

Network security measures include the following:

- **Enterprise firewalls.** High-end firewalls with strict policies to secure and maintain data and applications.
- **Network address translation (NAT).** NAT ensures that internal IP addresses are hidden and not routable from the outside.
- **Hardened Applications.** The PSP website has been hardened against malicious attack attempts includes techniques like cross site scripting (XSS) attacks, and SQL/JavaScript injection attacks.

## PSP Data Center Physical Security

The PSP Data Center is located inside a tier 1 telecommunications facility, secured as follows:

- **Solid construction.** The PSP Data Center can withstand high severity level natural or man-made disasters.
- **Highly available and reliable network connectivity.** Redundancy at every level ensures high availability of all the PSP application services.
- **Continuous manned security.** Professional security personnel are present 24x7.
- **Restricted access.** Use of key cards, keypad access, and biometrics, all under video surveillance, ensures that access is restricted to the correct personnel.
- **Fire suppression.** Zoned smoke detection and a fire suppression system protect against fire damage.

- **Redundant power.** Uninterruptible power supply (UPS) batteries and diesel-powered generators ensure against power failure.