

PORTUS™ Application Protection System (APS) Performance Brief



PORTUS APS Overview

PORTUS is an in-line Network Intrusion Prevention System and firewall, delivering in-depth protection against known and unknown forms of attack. The multi-level defenses includes Protocol Anomaly Detection (PAD), Stateful Signature Analysis (SSA) and other application specific defenses. PAD provides Zero-Hour™ protection, blocking new forms of attack at the gateway in real-time without the need for attack signatures. Stateful Signature Analysis of complete requests blocks known attacks and can not be fooled by packet fragmentation. Application specific defenses validate requests blocking invalid, out of sequence and unauthorized commands. PORTUS is capable of stopping all forms of attack in real-time, preventing them from reaching your protected systems. Both PAD and SSA can be fine tuned to maximize security without producing false alarms.

Viruses and worms found in e-mail are blocked by the combined use of PAD and the selective blocking of executable file attachments. This has proven to be the most effective form of defense and has stopped attacks that have penetrated the combined defenses of stateful packet filters, IDS and virus scanners.

PORTUS has successfully secured large organizations for more than 10 years. During this time no vulnerabilities have ever been reported by CERT, BugTraq, SANS or the FBI's NIPC, a record unequaled by other firewalls. Application level defenses block thousands of attacks that pass undetected through the best of the Stateful Packet Filters. Embedded intrusion prevention eliminates the need for intrusion detection software at the network boundary.

In addition to unequaled security PORTUS also provides content filtering, web caching, workload balancing, a fault-tolerant High Availability option and extensive report generation.

PORTUS provides unequaled scalability to meet the requirements of small, medium, large and ultra-large organizations. It is capable of multi-gigabit per second throughput, making it suitable as an Intranet as well as Internet firewall and NIPS.

While the primary purpose of a firewall is to provide high levels of security, the firewall must also process data as fast as the networks to which it is attached. PORTUS achieves unparalleled performance through the use of advanced technologies that maximize performance. PORTUS runs efficiently on uni-processor systems and takes full advantage of multiple processors when more throughput is required. Dynamic tuning software maximizes communication performance permitting full utilization of high bandwidth long latency networks while reducing systems overhead. PORTUS APS is available on four hardware architectures, 32-bit Intel (IA-32), 64-bit AMD processors, IBM 64-bit Power (PowerPC, Power4, Power5), and 64-bit UltraSPARC.

High performance is achievable using inexpensive Intel processors. PORTUS also supports 64-bit processors that have higher memory and I/O bandwidth. Both being crucial for multi-gigabit throughput. PORTUS supports the dual-core dual-thread POWER5 micro-processors that deliver ultra fast throughput and SSL encryption. POWER5 systems use fault tolerant technology such as dynamic processor deallocation and chipkill memory to provide unequaled hardware reliability.

PORTUS APS delivers unequaled performance and systems throughput without compromising security or systems availability at a competitive price. PORTUS APS is capable of performance levels that exceed those published for other firewalls including stateful packet filters.

Application Throughput

Application throughput is the preferred method for measuring firewall performance. The metric produced is expressed in terms of the business function being performed. For example, application throughput will tell you how many megabits per second the firewall can support for FTP or HTTP or SMTP. The primary workload for the majority of firewalls is HTTP. Expressing a firewall's HTTP throughput in MB per second is equivalent to the most widely accepted method for comparing Web Server throughput.

The PORTUS benchmark numbers were made with all PORTUS functions activated. For example, FTP measurements were made while the proxy was performing all of its security checking including protocol anomaly detection and validation of user permissions for every FTP sub-command. The commands were also checked for conformance with published standards. All commands were logged in the syslog. All monitors were active looking for SYN flood attacks, IP address spoofing. Nothing was turned off to make the system run faster. No other network activity was present to interfere with the benchmark. This is important to know when comparing benchmarks. For example, a stateful packet filter may not perform any stateful checking for some applications or have NAT disabled, nor would it be performing NIPS or IDS functions done by PORTUS.

The throughput is expressed in Megabits per second. The systems were moderately tuned by increasing the default buffer size for the proxies from 4 KB to 16 KB. The HTTP workload was similar to the SPEC Web workload, in terms of average URL size. The average file size used for FTP performance measurements was 1 MB. The numbers published are conservative, and have been exceeded at customer sites by as much as 25%.

Multi-gigabit throughput requires more than fast processors. The entire system must be well balanced with high speed memory and a high speed I/O subsystem. All measurements were made using a sufficient number of network adapters to keep the link utilization below 80%. All measurements showing throughput greater than 100 Mbps used one or more pairs of Gigabit Network Interface cards. The performance of some models has been extrapolated from measured values using published relative performance numbers of each machine as well as published SPEC WEB99 numbers.

While the numbers shown below are achievable in a controlled environment there is no guarantee that they can be reproduced in a production environment, where there are many other variables beyond our control.

In this analysis firewall throughput is reported separately for FTP and HTTP traffic. If you need to estimate the throughput for a mixed FTP and HTTP workload you calculate a weighted average using the relative workload for each application.

Hardware Configuration & Customization

The PORTUS APS delivers unequalled levels of system throughput. Since PORTUS supports three hardware architectures you can pick the system and OS that best fits your organization's requirements. Performance is limited by the bandwidth of the hardware and not by the software.

A relatively inexpensive server with a single Intel Pentium Xeon processor can sustain more than 1400 Megabit/second throughput for FTP and 1250 Mbps for HTTP. This exceeds the throughput of an OC24 link (1.244 Gbps) which is equivalent to 672 T1 links (15.44 Mbps). The dual processor Xeon system can sustain more than 2,700 Mbps, enough to saturate a OC48 link (2.48 Gbps).

The dual processor Xeon system also handles up to 548 Mbps throughput for SSL traffic when running in SSL Offload mode. Although not shown PORTUS also runs very well on systems running Pentium 4 and AMD processors.

The Power5 systems demonstrate extraordinary levels of throughput. These systems have exceptional I/O throughput permitting system configurations that can sustain throughput in excess of 12 gigabits/second, enough to saturate five OC48 (2.48 Gbps) optical links. The Power5 systems support 1 and 10 gigabit Ethernet adapters. This level of throughput requires either four 10 gigabit Ethernet adapters or 24 gigabit Ethernet adapters all running on dedicated busses.

PORTUS APS Throughput Performance for FTP

Product	No. Proc	GHz	Processor Type	Mbps
PORTUS-x346	1	3.6	Pentium Xeon	1,420
PORTUS-x346	2	3.6	Pentium Xeon	2,740
PORTUS-p615	1	1.45	Power4+	770
PORTUS-p615	2	1.45	Power4+	1,200
PORTUS-p5-520	2	1.65	Power5	3,200
PORTUS-p5-550	2	1.65	Power5	3,200
PORTUS-p5-550	4	1.65	Power5	6,400
PORTUS-p5-670	2	1.65	Power5	3,690
PORTUS-p5-670	4	1.90	Power5	7,000
PORTUS-p5-670	8	1.90	Power5	13,300

The PORTUS-AP machines were configured with two to twelve Gigabit Ethernet adapters. The gigabit Ethernet adapters employ TCP Offload Engines to enhance system throughput.

The FTP proxy performs complete access control at the FTP sub command level and records all commands and file transfer information. User authentication is active using the integrated authentication server.

PORTUS-APS Throughput Performance for HTTP

Model	No. Proc	GHz	Arch	Ops/ Sec	Mbps	SSL
PORTUS-x346	1	3.6	Xeon	7,500	1,250	No
PORTUS-x346	2	3.6	Xeon	20,160	2,400	No
PORTUS-sfv20z	2	2.4	Opteron	15,552	1,920	No
PORTUS-sfv20z	4	2.4	Opteron	31,104	3,840	No
PORTUS-p5-520	2	1.65	Power5	22,680	2,800	No
PORTUS-p5-550	2	1.65	Power5	22,680	2,800	No
PORTUS-p5-550	4	1.65	Power5	46,200	5,700	No
PORTUS-p5-570	2	1.65	Power5	25,920	3,200	No
PORTUS-p5-570	4	1.90	Power5	49,896	6,160	No
PORTUS-p5-570	8	1.90	Power5	94,835	11,708	No

The HTTP performance numbers were generated using the reverse HTTP proxy Webgate Plus. Webgate Plus provides transparent access to a Web Server residing behind the firewall. Webgate Plus examines all HTTP commands and permits valid requests while blocking invalid requests. It performs complete HTTP access logging, NAT, workload balancing. The hardware configurations shown above employ multiple gigabit Ethernet Adapters with TCP Offload Engines that enhance system throughput. Power5 performance numbers were extrapolated from Power4+ numbers using the relative performance numbers (rperf) published by IBM.

PORTUS-AP Throughput Performance for HTTPS

Model	No. Proc	Ghz	Arch	Ops/Sec	Mbps	SSL
PORTUS-HS20	2	3.0	Xeon	3,567	428	Yes
PORTUS-x346	2	3.6	Xeon DP	6,558	787	Yes
PORTUS-sfv40z	4	2.4	Opteron	12,736	1,525	Yes
PORTUS-p5-550	4	1.65	Power5	13,640	1,640	Yes
PORTUS-p5-570	4	1.90	Power5	14,338	1,717	Yes

The HTTPS performance numbers show system throughput when Webgate Plus uses SSL to encode/decode HTTP traffic between the proxy and the client. This is known as SSL Offload as it offloads the SSL processing from busy web servers.

PORTUS Advantages

The PORTUS proxies offer a higher level of security than the best of the Stateful Packet Filters. Unlike Stateful Packet Filters PORTUS assembles packets into complete messages before examining the data for application specific attacks. This architectural advantage makes PORTUS immune to attacks that have penetrated SPF filters. The application specific proxies offer the best possible protection by tailoring its inspection to the application. In addition the advanced Application Program Interface (API) allows local customization to provide fine grained application specific controls for any application.

The PORTUS architecture also allows for unequalled error detection and isolation protecting itself from hardware and software errors. The PORTUS proxies run without root privilege in chrooted directories with three levels of error detection, reporting and recovery. In this environment errors can be isolated to a single transaction, thereby improving security and availability. Unlike firewalls that run in kernel mode hardware and software failures can not propagate from one thread to the next causing catastrophic failures that can disrupt service or allow unauthorized network penetration.

For more information contact Freemont Avenue Software.

Freemont Avenue Software, Inc.
1830 S. Kirkwood Suite 205
Houston, TX 77077

tel: 281-759-3274
FAX: 281-759-8558

www.lsl.com
portus@lsl.com