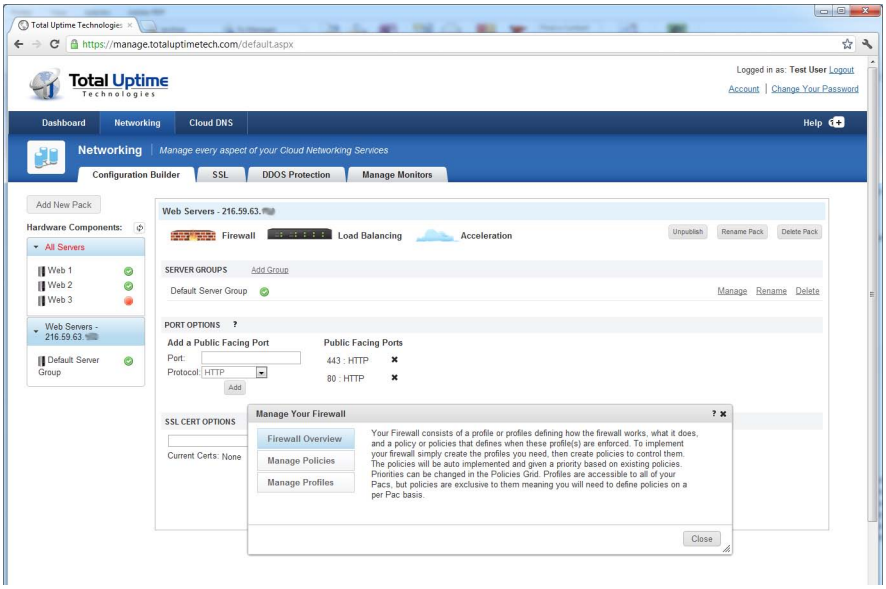
Total Uptime Technologies

CLOUD IPS/FIREWALL

Global Protection and Prevention at the Edge of the Internet

The Total Uptime Cloud IPS/Firewall protects Web applications at the very edge of the Internet as opposed to inside the datacenter. Our solution shields an organization's network from the growing number of application-layer attacks and prevents the loss of valuable corporate and customer data. In addition to proven attack defenses, the Cloud IPS/Firewall also aids in compliance with information security regulations, such as PCI-DSS.



Fastest IPS/Firewall Available

We deliver the industry's highest performing web application security solution, capable of protecting public facing IT environments without degrading throughput or application response times. The Total Uptime Cloud IPS/Firewall delivers multi-ten gigabit security performance that meets the needs of any enterprise or service provider installation.

Automatic Learning Engine

In addition to delivering out-of-the-box protection against all web-based threats, Cloud IPS/Firewall provides the ability to tailor security policies for any application, including those

Key Features

- Malicious traffic and threats are thwarted at the source, not at your datacenter
- Layer 7 Application, Web 2.0, DDoS, SynFlood, BotNet and zero day threat protection
- 640 Gbps capacity at the edge of the Internet
- Augments and enhances current internal firewalls
- Global platform with each node operating with 20 Gbps of IPS and Firewall capacity
- Aggressive SLAs

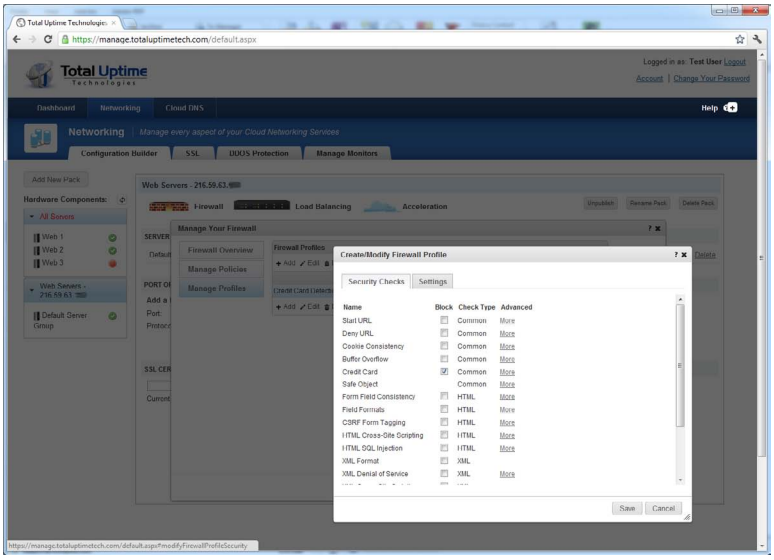
using client-side javascript. The Cloud IPS/Firewall's Learning Engine can automatically learn the behavior of an application and generate human-readable policy recommendations. The security manager can then selectively apply recommendations to strengthen a security policy and to enable permissible application behavior usage demands that customers place on your web operations in real-time. This flexible capacity model enables greater cost-efficiency in operation, reduces the overall costs of managing your website, and improves site performance. Your end users receive the consistent, high quality web experience they need, resulting in higher customer loyalty rates, lower operational costs and enhanced brand equity.

Defend your Web applications

With over 70 percent of successful Internet attacks now exploiting application vulnerabilities, take some time to learn more about our global Cloud IPS/Firewall.

Rapid Implementation

Simply layer Cloud IPS/Firewall on top of your existing public-facing infrastructure for instant protection. Total Uptime Cloud IPS/Firewall will quickly provide the protection you need.



Positive Security Model: Delivers Zero Day Protection

The application security technology of the Cloud/IPS Firewall is based on a positive security model that ensures correct application behavior. This is derived from HTTP industry standards and best coding practices for HTML and JavaScript. Application behavior deviating from the positive security model is treated as potentially malicious and is blocked by the Cloud IPS/Firewall.

Through its understanding of good application behavior, the positive security model does not require attack signatures or pattern matching techniques to detect and block attacks. It is the only proven approach delivering zero day protection against unpublished exploits. The positive security model:

- Verifies best practices
- Ensures RFC compliance
- Models application behavior
- Enforces security in real-time
- Is *not* signature-based

Deep Stream Inspection

Next-generation security requires much more than simple packet-level inspection. Complete application security requires deep stream inspection technology that reconstructs all bi-directional communications for each user session. Once reconstructed, it inspects all content to ensure correct application behavior, and the validity of user and machine inputs.

Deep stream inspection technology is based on multiple core technologies, including:

- Bi-directional analysis of all application traffic
- Complete header and payload inspection
- Full application parsing
- Semantic extraction of relevant application objects
- Traffic sessionization

Adaptive Learning Engine

In addition to delivering out-of-the-box protection against all Web-based threats, the Cloud IPS/Firewall provides the ability to tailor security policies for any application, including those using client-side JavaScript. The adaptive learning engine can automatically learn the behavior of an application and generate human-readable policy recommendations. The security manager can then selectively apply recommendations to strengthen a security policy and to enable permissible application behavior.

Multi-layer Cloaking

The Total Cloud IPS/Firewall incorporates multi-layer cloaking technology to mitigate a hacker's ability to conduct reconnaissance on a target Web-site. It hides sensitive information about an application environment (e.g., application server, database technology, server operating system, internal domain naming, etc.) making it much more difficult for an attacker to devise an effective attack strategy and exploit known vulnerabilities. By cloaking sensitive or revealing information at multiple communication layers, hackers are denied valuable intelligence about an application infrastructure, thus greatly reducing the risk of attack.

For more info about Total Uptime visit totaluptimetech.com.

sales@totaluptimetech.com
(800) 584-1514