White Paper

LoadMaster Application Delivery Controller Security Overview

KEMP TECHNOLOGIES, INC.

SSL Offload/Acceleration, Intrusion Prevention System (IPS) and Denial of Service (DOS)

Overview

Small-to-medium sized businesses (SMB) are increasingly relying upon web-based applications and web-enabled services for running their business. Applications such as CRM, e-commerce transactions and other web-enabled applications are accessed both locally and remotely from outside the business facilities. These web-based applications are vulnerable to attacks from viruses, intrusions, and denial of service (DoS) attacks, as traffic comes into the network through various ports and firewalls without being inspected.

SMBs are facing an extraordinary number of network attacks from internal personnel and external hackers. Security problems such as unauthorized access, firewall breaches and other malicious intrusions are occurring on a daily basis. Compounding these problems is the fact that existing security tools such as firewalls, IDS, VPNs, anti-spam and anti-virus gateways do not have the processing capability, performance and the application-level security intelligence to protect against the growing amount of application-level attacks. SMBs are particularly vulnerable to security threats, and risk major losses of intellectual property, user productivity and potential loss of revenue. With that said, there is an increasing need for security solutions that provide real-time protection from a wide variety of application-level attacks.

When an SMB incurs a DoS attack, their IT resources are deprived of the services. Examples of such an inability of a network service are: e-mail might become unavailable, or there may be a temporary loss of all network connectivity and services, or the datacenter may be forced to temporarily shut down operations. DoS attacks can also wipe out a computer system’s software programs and files.

The need for application-based security protection

- **Web-based Applications are Vulnerable to Attacks** – such as viruses, intrusions, and DoS, as traffic comes into the network through various ports and firewalls without being inspected.
- **Explosive Growth of Attacks** – The amount and seriousness of application vulnerabilities are growing at a dramatic rate, while the cost of these attacks is soaring.
- **Current Security Tools Cannot Block Attacks** – Firewalls, IDS and anti-virus gateways do not have the processing capacity, performance and the application-level security intelligence to guard against application-level attacks, leaving organizations vulnerable.

LoadMaster Security Benefits

- Protects web servers that have no controlled access – including protection from hackers and denial of service attacks
- Protects web servers with controlled access, by limiting access specifically to authorized users
- Provides security protection for Internet, intranet, and extranet environments
- Blocks the most common attacks before they reach servers

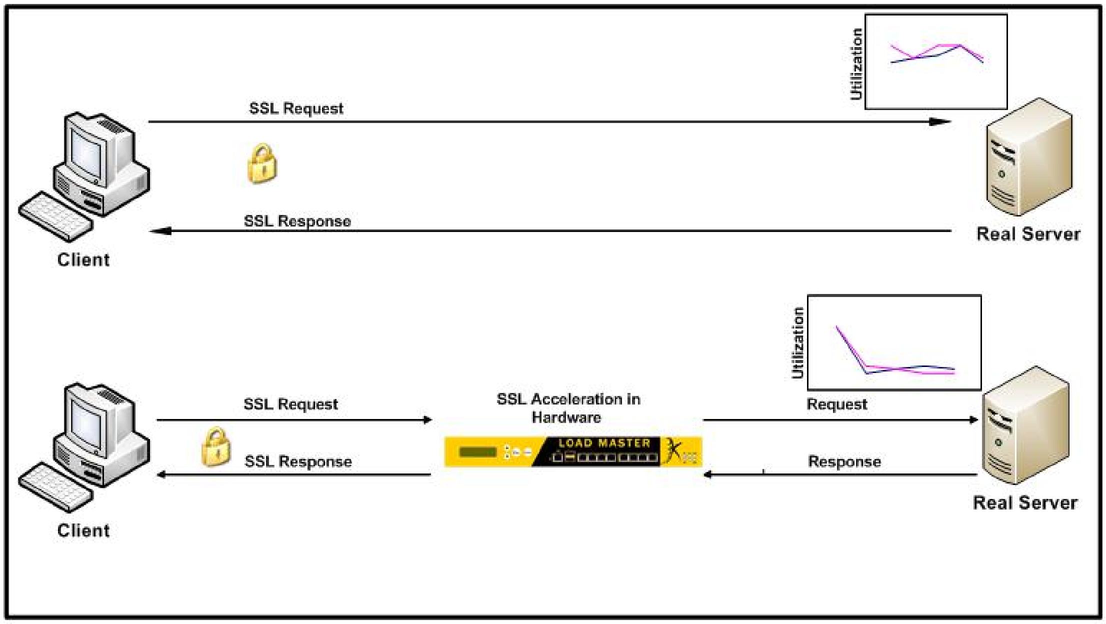
LoadMaster Security Capabilities

- Black List (Access Control List system)
- IP address filtering
- Firewall filtering
- DDOS mitigation
- SYN Flood Protection
- Ping of Death Protection
- ICMP Flood protection
- UDP Flood protection
- SSH/SSL brute force attack protection

LoadMaster SSL Security

All LoadMaster Application Delivery Controllers and Server Load Balancers include hardware-based (ASIC) for Secure Socket Layer (SSL) offload and acceleration. SSL Acceleration performed by LoadMaster provides two benefits:

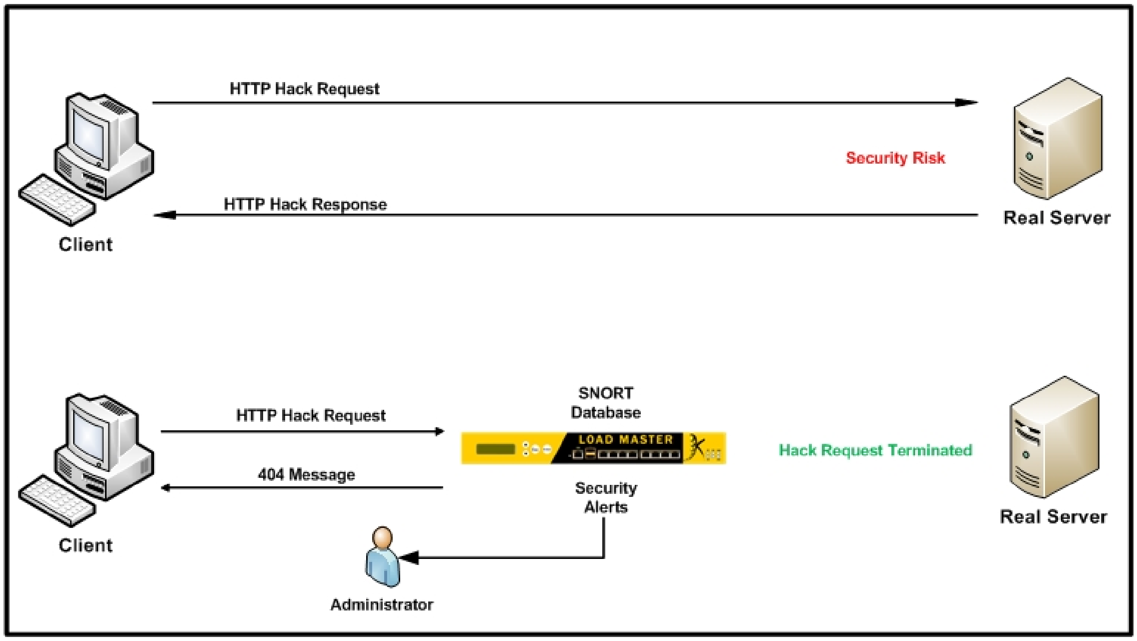
- LoadMaster offloads the SSL workload from the Servers, and performs Layer 7 processing, cookie-based persistence and content switching. ASIC-enabled SSL Acceleration has a separate specialized processor, which handles all SSL functions.
- SSL Acceleration includes support for up to 256 SSL Certificates, supports third-party certificates, automated SSL certificate chaining, and web user interface-based SSL certificate signing request (CSR) generation.



Intrusion Prevention System (IPS)

LoadMaster's Intrusion Prevention System (IPS) is installed in-line, inspecting all traffic before forwarding it onto the network. If the LoadMaster IPS detects malicious activity it terminates the session. By default, intrusion prevention is enabled, and protects all application delivery services. However, administrators can disable the LoadMaster intrusion prevention capabilities. The Intrusion Prevention System protects applications from the following common threats:

- Virus propagation
- Buffer overflows
- Protocol-specific attacks



Network protocol protection

The LoadMaster 3500 contains protocol-specific guards that protect your Servers from attacks targeting SMTP, DNS, and LDAP protocols.

Application-specific attacks

The LoadMaster 3500 protects applications that are particularly vulnerable to external attacks. These applications include IIS, Websphere, Cold Fusion, Exchange, and many others.

Operating system-specific attacks

LoadMaster 3500 contains Microsoft and UNIX-specific detection capabilities that identify malicious activity against these operating systems. The Intrusion Prevention System is updated with the latest threats every hour by Energize Updates.

Avoid the "port 443 blind spot”

With the LoadMaster, you can get complete Application Layer 7 IPS exactly where you need it. As an SSL termination point, the LoadMaster is the outermost point on the network that enables it to see all Layer 7 exploits coming in, and completely avoid the dreaded "port 443 blind spot".

Get the performance you need

The LoadMaster 3500 delivers 2,000 TPS of SSL processing power, so you don't have to sacrifice end-user responsiveness.

Denial of Services

LoadMaster ensures continuous real-time DoS/DDoS and SYN attack protection for web application security. Security events are isolated to ensure continuous uptime even while under attack, while unaffected traffic is allowed through without degrading performance.

- SYN Flood Protection
- Ping of Death Protection
- ICMP Flood protection
- UDP Flood protection

Credit Card Security

LoadMaster Application Delivery Controllers are compliant with PCI-DSS (the credit card data security standard). Companies use LoadMasters every day to process credit card transactions via SSL.

Summary

Small-to-medium sized businesses face unprecedented amounts of network security attacks from internal personnel and external hackers. Security tools such as firewalls, IDS, VPNs, anti-spam and anti-virus gateways are not capable of providing the processing capacity, performance and the application-level security intelligence necessary to protect against the increasing amount of application-level attacks. SMBs are continuously exposed to security hazards that pose a threat to their intellectual property, potential revenue loss and lost productivity.

KEMP Technologies' LoadMaster Application Delivery Controllers and Server Load Balancers help to ensure that online business remains stable even while under attack. The LoadMaster simplifies and centralizes network infrastructure management, and optimizes performance and scalability of IT infrastructure to economically scale server resources and security operations to deliver optimal security management and enforcement.

KEMP products deliver availability, performance, scalability and security to the SMB web infrastructure.