November 2002

Cost-Effective, Continuous, Secure Delivery of Business-Critical Web Applications

Advanced web application control that ensures uninterrupted, secure delivery of web applications, while dramatically reducing the cost of operations

NETSCALER

As business-critical applications are deployed on the Internet, IT executives must meet the increasing demands for non-stop application availability and fully secure delivery of these applications, without adversely impacting end-user performance. In addition, steady growth in users must be managed within the confines of reduced capital budgets and staff size.

There are a myriad of point products on the market today that are designed to optimize one or more aspects of web service delivery while attempting to solve some of these challenges for IT managers. Many of these products are designed to protect against specific kinds of Denial of Service (DoS) or intrusion attacks. Others are aimed at improving site capacity or end-user performance in some particular way. The widespread adoption of SSL as the preferred means to ensure data security has elevated the need for point products such as SSL accelerators to handle the encryption/decryption process.

Unfortunately, introducing one or more of these point products into a web infrastructure increases management complexity, degrades application performance and imposes a large drain on ongoing operational budget. In addition, management burden is compounded when other infrastructure optimization capabilities are nullified in the face of encrypted traffic. As a result, companies cannot solve the fundamental problem of ensuring the fully secure delivery of business-critical applications without leaving these applications and infrastructure vulnerable to attack or without degrading end-user response.

Now, for the first time, an affordable application infrastructure solution exists that can secure 100% of application content end-to-end while providing unique application-level protection against attacks and traffic spikes, and reduce the total cost of operations, all without diminishing the end-user experience.

THE CHALLENGE

Today's IT departments face enormous challenges in optimizing their networks to deliver complex web-based applications to a growing base of end users. Web-based interfaces let employees access email, customers use self-service online systems and manufacturers use extranets for online procurement and fulfillment systems. Increasing numbers of online sites routinely accept credit card information over the web. In addition, common-sense business constraints and security-conscious end users mandate that these applications be secure so that communications remain private. But as these applications have become a "business-critical" component to the growth and productivity of companies, the required levels of availability, performance and network scalability have risen even higher deeming existing solutions inadequate and the challenges as yet unmet.

Unfortunately, the ability to scale infrastructure capacity for secure delivery has historically introduced significant management complexity and has been cost prohibitive. As a result, businesses have been forced to trade-off secure delivery for end user responsiveness at a great expense to the business.

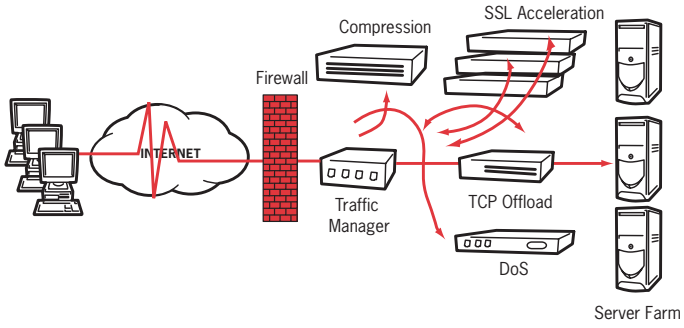

Figure 1: A typical web application infrastructure

Today's typical web application infrastructure (Figure 1, above), features a complex mix of application servers, firewalls, load balancers and point products such as compression and specialty DoS attack protection systems. In addition to the inherent complexity in managing these disparate systems, these products lose much of their value when traffic is made secure, as encryption renders application-level data invisible to these devices.

Today's Solutions Fall Short

IT managers have found that while all of the various point products demonstrate adequate performance independently, when patched together into a network (as shown in Figure 1) a number of problems are incurred:

- Critical optimization functionality is lost when traffic is encrypted
- No combination of products includes this functionality at an affordable cost
- There is an unacceptable escalation in network complexity
- Application-level protection is not possible with secure data transmission

Without a single point product or a combination of products available that will ensure the secure delivery of web applications and provide continuous application availability, site resources and communications remain vulnerable. There are currently several ways that companies are enhancing their infrastructure to include encryption for secure delivery and ensure that data transmissions between clients and servers remain private. The most popular techniques include:

1. Build a VPN infrastructure
2. Enable SSL in the servers
3. Install an SSL acceleration card in each server
4. Deploy an external SSL accelerator

These encryption techniques can be very effective at securing data but come with significant trade-offs, including performance degradation, management complexity, implementation and deployment complexity and costs.

Deploying a VPN Infrastructure

VPNs offer extremely secure links. However, VPNs are not useful for web applications used by non-employees or other people who require the VPN client software. VPNs can become a logistical and management burden for IT personnel, and often lead to sub-standard implementations. For example, an employee might receive instructions and software, complete with usernames and passwords, via unsecured methods.

Enabling SSL in the Web Server

It is relatively simple to enable SSL in a server. Unfortunately, when SSL is enabled in software, the CPU load created on the server makes scalability a serious problem (SSL processing can degrade server capacity by over 95%). For this reason, some companies choose to encrypt only the most sensitive portions of web applications, such as those pertaining to the checkout and purchase process. This often backfires because performance drops significantly as soon as the user attempts to make a purchase, leading to frustrated customers, abandoned shopping carts and other problems.

Installing an SSL Accelerator Card in Each Server

For smaller web applications, installing SSL acceleration cards in servers can help. However, in addition to the deployment pain involved in installing a card in each server, scaling applications, servers and their certificates can become problematic and introduce significant management complexity. This solution also disrupts many of the other traffic management, firewalls or IDS systems that the site may have invested in.

Deploying an External SSL Accelerator

An external SSL acceleration appliance is one of the only ways to fully secure communication between the site and the end-user. Unfortunately this method, which can be costly, disrupts many of the other networking functions that are required to scale a site to any significant size, and causes significant performance penalties for users (e.g., due to more HTTP redirects) and longer page downloads. In addition, most external SSL accelerators do not provide end-to-end secure delivery. These systems send clear text from the device to the servers and back, thus not achieving the levels of security required by many market segments such as government, financial services and healthcare.

SSL has been demonstrated as the most effective way to secure delivery of applications. However, the lack of an effective SSL solution has not only slowed the adoption of encrypted delivery for most

business-critical web applications, it has even slowed the adoption of the web as a medium for delivery of business-critical applications to customers, partners and employees.

THE NETSCALER SOLUTION

Now, there is an effective solution that helps enterprises meet the overwhelming demand for cost-effective, continuous, secure delivery of business-critical applications over the web. The NetScaler Request Switch™ 9000 iON Series is an advanced web application control system that offers all of the essential elements required to meet this challenge.

- 100% secure delivery of all application requests
- Continuous application availability in the face of attacks and legitimate surges
- Significant reduction in cost of operations
- All while maintaining end user responsiveness

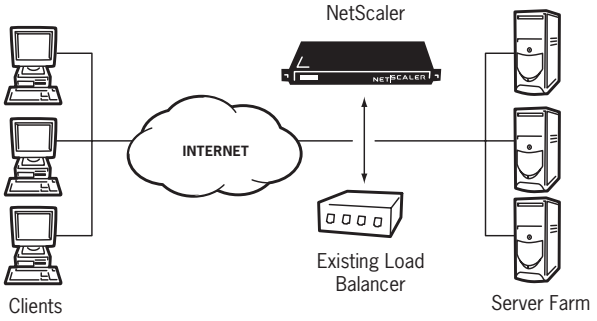

Figure 2: The benefits provided by NetScaler's web application control system

Uniquely complements your existing infrastructure by integrating unlimited SSL capacity, application-level protection and infrastructure optimization into a single solution for the secure delivery of business-critical web applications.

The NetScaler Request Switch 9000 iON Series is the first and only system that enables enterprises, e-businesses and service providers to optimize their networks for the continuous, secure delivery of all business-critical web applications. NetScaler's products apply its patented Request Switching™ technology to address and overcome the inefficiencies of existing infrastructure products and Internet protocols, offering application protection and enabling secure delivery without compromise.

Fully Secure Delivery of Web Applications

The NetScaler Request Switch 9000 iON Series ensures that 100% of web application content can be secured from end-to-end without degradation in end user responsiveness. Other products that only accelerate SSL key generation (the primary burden for SSL encryption) perform at 600 to 800 transactions per second (TPS). While this represents a significant increase in capacity over a typical server (which performs at approximately 100 TPS), it is not nearly enough horsepower to encrypt 100% of the traffic for an entire site. Moreover, the throughput required for bulk encryption of all data being transmitted poses an even greater limitation.

A single system within the Request Switch 9000 iON Series can complete up to 4,400 SSL TPS and deliver encryption throughput of up to 450 Mbps, generally enough to secure all applications for a particular site. For those sites requiring more secure throughput, unlimited NetScaler systems can be clustered to achieve wire-speed encryption throughput and tens of thousands of transactions per second, ***essentially removing SSL capacity as an inhibiting factor in providing secure application delivery***. Therefore, enterprises, e-businesses and service providers no longer need to accept slower performance, increased network complexity or higher costs to achieve 100% secure application delivery.

Complete Protection for Continuous Application Availability

Continuous application availability begins with a complete application protection solution. After a firewall inspects traffic, it permits all legitimate traffic to be passed on to the web server. If this traffic is HTTP based, it is sent through port 80. Unfortunately, over 80% of DoS attacks occur over port 80. Because these types of attacks appear as legitimate traffic they remain undetected by a traditional firewall. Even truly legitimate surges in traffic can threaten the availability of a site. Existing DoS protection solutions either drop requests after reaching server connection limits, or redirect application requests to other servers – consuming expensive back-up capacity.

NetScaler is able to prevent certain attacks from reaching the server and regulate others such that every legitimate transaction is completed without imposing a performance penalty to the user or a capacity penalty to the provider. As 80% of these attacks occur over port 80, NetScaler provides the perfect complement to firewalls and other security infrastructure.

NetScaler provides wire-speed protection against DoS attacks as well as protection against application-level DoS and worm attacks through features such as:

Surge Protection

NetScaler insulates sites from sudden spikes in traffic by decoupling browser connections from the server and queuing the requests in the NetScaler system before sending them on to the server. The queue dynamically regulates site traffic and prevents servers from overloading, whether from a busy online holiday shopping season or following a major news event. NetScaler protects against surges in layer-4 connections as well as layer-7 application requests.

Application Level Flood (App DDoS) Attack Protection

One effective way to rob a server of its resources is to flood a legitimate connection with GET requests. These requests, arriving at a rapid rate, originate from drone clients and can quickly overload a server. When this type of flood happens, NetScaler identifies and de-prioritizes suspected drone clients, and actively elevates the priority of legitimate traffic, preserving capacity for genuine users. The Request Switch 9000 iON Series is unique in its ability to continue service delivery to legitimate users at the maximum capacity of the infrastructure. All other attack protection products are limited in their ability to prevent such attacks, as they provide only the means to shut off traffic when an attack happens, or worse, consume the resources in serving the attack requests. This significantly degrades the user experience and ultimately fulfills the purpose of the attack by denying service to these users. NetScaler on the other hand, de-prioritizes bogus requests and elevates legitimate requests to ensure the continuity of service.

Network Level Flood (Net DDoS) Attack Protection

There are several variants of network level DDoS attacks, those based on the TCP protocol as well as other protocols such as UDP and ICMP. NetScaler provides the industry's best protection against SYN flood attacks, Zombie connection attacks, UDP or ICMP based flood attacks. NetScaler is able to prevent these attacks at full gigabit wire speeds because its solutions are based on the Request Switching technology, which has been purpose-built to process such traffic at maximum efficiency.

Intrusion Filtering to Block Worm Attacks

NetScaler includes an intrusion filter that analyzes HTTP GET and POST requests and filters out any known bad signatures. It makes sense to do this in a NetScaler device as opposed to a firewall, since NetScaler systems are already managing HTTP requests at the application level as part of their request-level traffic management functions. This mechanism can be used by customers to defend against HTTP-based virus attacks such as Nimda and Code Red variants, as well as other exploits such as long URL attacks and CGI open door attacks.

Priority Queuing

When a site is in a surge condition, and clients are contending for access to server resources, NetScaler can prioritize traffic to ensure that the most important traffic is serviced first. This feature allows an overloaded site to continue processing orders without wasting critical resources on low-priority traffic, servicing this traffic at a later time.

Certified Response with SureConnect™

SureConnect ensures application responsiveness even when servers are working at capacity or applications are experiencing processing delays. By providing real-time estimates of Internet response times, interactive priority queuing, and guaranteed content delivery, SureConnect can dramatically improve the real and perceived availability of a site by eliminating the gap between your customer's expectations and their browsing experience.

Distributed Availability

When entire sites become unavailable, NetScaler can direct traffic to a backup site. NetScaler monitors the condition of multiple clusters or sites and ensures continuous application availability in the face of network failures or other disasters.

Reducing Cost of Operations

NetScaler's Request Switch 9000 iON Series maximizes network capacity and reduces the total cost of operations by focusing on major issues including: scaling existing infrastructure capacity and reducing network management complexity and cost.

Scaling Existing Systems Capacity *— NetScaler can double the performance and throughput of caches, servers and firewalls*

- Offload of Transport Protocol Processing: NetScaler enables a server to do what it was built to do: serve content. It has been shown that up to 50% of a server's utilization can be consumed by the processing of TCP connections. By managing this, and using long-lived persistent connections to the server, NetScaler significantly increases server capacity.
- TCP Buffering: NetScaler can dramatically increase the capacity of each server in a connection-limited environment by removing the connection management from servers when slow-speed clients require connections to be held until the data has been transmitted.
- Centralized Logging: NetScaler can eliminate the burden of web logging from servers, and send the log entries to one centralized server. This not only leaves more processing power for the server, it also eliminates the task of consolidating logs from many servers and ensures that time stamps in the logs are consistent.
- Cache Bypass: When a front-end cache is added to a site, all requests must flow through it. However, the cache must evaluate many requests that will never result in a cache hit, adding latency. NetScaler can distinguish between cacheable and non-cacheable requests — sending non-cacheable requests directly to the server, eliminating the load on the cache, and reducing latency for the user.

Scaling Existing Network Capacity *— NetScaler can cut bandwidth costs by up to 50%*

- Reduced Bandwidth Utilization: By compressing text based data such as HTML content and other downloadable gzip compressible files, the bandwidth needs of an application can be reduced by up to 50% for the same web traffic. This reduces monthly bandwidth costs dramatically, and can also extend the life of low capacity WAN links without the need to upgrade.
- Reduced Content Delivery Network (CDN) Charges: It has been conclusively demonstrated that with a NetScaler delivering the content from the origin site to the internet, customers can selectively serve traffic to certain sets of users directly from the origin site and in some cases, completely avoid CDN charges.
- Reduced Load on Routers and Switches: Because NetScaler uses persistent connections to both servers and users and can compress content across these connections, applications transmit significantly fewer packets to and from the internet, thus expanding the capacity of the network infrastructure routers, switches and firewalls to support many more concurrent users.

Reducing Network Management Complexity and Cost

By boosting the efficiency of existing site assets, NetScaler reduces the number of servers and software licenses required to serve the same application to the existing user base and eliminates the need for point products such as SSL accelerators, TCP offload devices or DoS attack protection systems. With NetScaler in place, excess servers can be redeployed or eliminated altogether. In addition, NetScaler expands network capacity by making more efficient use of connections and also by compressing data. NetScaler can significantly reduce bandwidth costs and serve more data through the same network. Furthermore, central web logging considerably streamlines the indispensable web traffic log collection for demographic analysis by eliminating file transfer and sort-merge steps in the process.

End-User Responsiveness

With NetScaler, there is no compromise in performance for availability or secure delivery. NetScaler has carefully woven essential performance functionality into Request Switching technology to ensure that protection and security can be provided at wire speed, while enhancing the end user experience.

Compression

Gzip compression can reduce the size of web application data by up to 80%. This compression feature is usually turned off in servers not only because of the burden it places on the server's CPU, but also because compression doesn't work with all traffic, specifically secure traffic. By letting NetScaler compress the data, the same information can be sent with less data, resulting in much faster page download times (up to 3x-4x faster). In addition, NetScaler can compress secure traffic as well, without affecting performance.

Client Persistence and TCP Accelerator

On a normal web site, with HTTP 1.0 a client may open and close 50 connections just to download one page. When you consider that each connection requires a three-way handshake with TCP parameters established through a slow-start process, one can see the latency inherent in this process. HTTP 1.1 was developed to solve this problem by enabling persistent connections between the client and the server, but enabling HTTP 1.1 produces other less desirable side-effects on server performance such as uneven load distribution, inefficient use of server farm resources, and vulnerability to traffic surges and attacks.

NetScaler's Request Switching decouples the server connection from the client connection, allowing for efficient, separate management of these connections. This eliminates hundreds of connection negotiations per session and greatly improves the end-user experience. In addition, through TCP buffering and other TCP optimizations, NetScaler enables servers to deliver data faster when a client connection is persistent.

CONCLUSION

Plans to transition business-critical applications to the web should not be derailed by concerns over application availability, security, cost of operations, or poor performance. NetScaler's new breed of network infrastructure systems is the first to combine the essential elements of application protection, security and optimization with robust traffic management functionality. The result is that for the first time ever enterprises, e-businesses and service providers can enable continuous secure delivery of business-critical web applications without any compromises, while reducing ongoing operational and bandwidth costs, and simplifying network management.

www.netscaler.com

NETSCALER, INC.
2880 SAN TOMAS EXPWY
SUITE 200
SANTA CLARA
CA 95051
1-800-NETSCALER

NETSCALER

Innovation to Scale the Net