



Features of a comprehensive application security solution

The comprehensive security features of Citrix NetScaler protect against DoS/DDoS, deliver intrusion filtering capabilities for application-level protection, and provide complete, hardware-based encryption to offload CPU-intensive cryptographic functions from the servers.



Introduction

Continuous application availability begins with a comprehensive application protection solution. A common approach to security is to deploy a network firewall and provide a system that stops Internet-based denial-of-service (DoS) attacks and other network-based intrusion attempts. Once the firewall has inspected the traffic, based on administrator configuration, it will permit or deny traffic and forward legitimate traffic to the requested application server. Unfortunately, over 80 percent of application DoS attacks occur on common application ports that pass undetected by traditional firewall solutions. Even truly legitimate surges in traffic can threaten the availability of a server or the entire site, as today's DoS protection solutions either drop requests after reaching a preconfigured limit or redirect application requests to other servers—where they consume expensive backup capacity.

The second piece of the comprehensive application security solution is application content security. For organizations that deliver sensitive, business critical information through public network infrastructures, the threat of this content being intercepted by unauthorized users can be addressed with encryption. However, offering complete end-to-end encryption—encrypting and decrypting content from the application servers—degrades performance.

To overcome these challenges, the comprehensive security features of Citrix® NetScaler® protect against DoS/DDoS, deliver intrusion filtering capabilities for application-level protection, and provide complete, hardware-based encryption to offload CPU-intensive cryptographic functions from the servers.

SYN attack protection

There are several variants of network level DoS/DDoS attacks, like those based on the TCP protocol such as SYN attack. NetScaler is purpose-built to process and protect the traffic that it receives against SYN attacks, and process legitimate traffic at great speed. NetScaler provides the industry's best protection, processing legitimate traffic at maximum efficiency, and providing better performance. For more information about SYN attack protection, see the *NetScaler Application Security Guide* on Citrix.com.

Content filtering

NetScaler includes an intrusion filter that analyzes HTTP GET and POST requests and filters out any known bad signatures. Unlike other offerings, NetScaler is designed to manage client requests at the application level, which provides a defense against HTTP-based virus attacks, such as Nimda and Code Red variants, and other exploits, such as long URL attacks and CGI open door attacks. For more information about content filtering, see the *NetScaler Application Security Guide* on Citrix.com.

Disaster recovery using GSLB

When entire sites become unavailable, NetScaler can direct traffic to a backup site by using global server load balancing (GSLB). NetScaler monitors the condition of multiple clusters or sites and ensures continuous application availability in the face of network failures or other disasters. For more information about GSLB, see the *NetScaler Traffic Management Guide* on Citrix.com.

SSL acceleration

NetScaler provides end-to-end SSL processing and offloads SSL processes from the server. NetScaler intercepts and processes SSL transactions on behalf of the server, and then sends clear text to the servers. NetScaler can also perform server-side encryption to provide end-to-end security. In addition, NetScaler provides a special bridge mode of access for SSL traffic where NetScaler does not offload SSL encryption or decryption and only supports load balancing and connection management features.

NetScaler accelerates SSL processing by using a high-speed SSL accelerator and offloads the SSL handshake, encryption and decryption capability to the SSL acceleration card. NetScaler supports RSA and DH key exchange methods with RSA or DSA authentication. NetScaler accelerates the processing of the cryptographic ciphers, such as RC2, RC4, DES, 3DES and AES.

With the multiprocessor MPX platforms, the NetScaler SSL engine can process up to 50,000 new SSL transactions per second (TPS). With nCore™ technology, NetScaler SSL engine processes 80,000 new SSL transactions per second (TPS). For more information about SSL acceleration, see the *NetScaler Traffic Management Guide* on Citrix.com.

AppExpert rate controls

AppExpert rate controls trigger NetScaler policies based on data rates either to or from a given resource. This prevents overloading the network or particular servers on the network by throttling traffic that exceeds a particular rate. This can be useful for preventing DoS attacks. For more information about AppExpert Rate Controls, see the “Traffic Rate” chapter in the *NetScaler Traffic Management Guide* on Citrix.com.

AppExpert service callouts

In high security zones, it is mandatory to authenticate the user before a resource is accessed by clients. NetScaler AppExpert service callouts externally authenticate the user based on the credentials supplied. AppExpert service callouts can also check incoming requests against an IP Blacklist service. For more information about AppExpert Service Callouts, see the “HTTP Service Callout” chapter in the *NetScaler Traffic Management Guide* on Citrix.com.

Responder

The responder feature functions as an advanced content filter that can be configured to auto-generate responses from NetScaler to the client. Common uses of the responder are to generate redirect responses, user-defined responses and resets. The responder deals only with the request side of NetScaler message processing and can be useful, for example, in redirecting problematic clients to a dummy Web site. The requests processed by the responder never burden the back-end server. For more information about responder, see the *NetScaler Application Security Guide* on Citrix.com.



HTTP rewrite

HTTP rewrite modifies HTTP headers and body text. You can use it to add HTTP headers to an HTTP request or response, make modifications to individual HTTP headers or delete HTTP headers. It also lets you modify the HTTP body in requests and responses.

When NetScaler receives a request or sends a response, it checks for rewrite rules and, if applicable rules exist, it applies them to the request or response before passing it on to the Web server or client computer.

For more information, see the “URL Rewrite” chapter in the *Citrix NetScaler Application Security Guide* on Citrix.com.

Access Gateway

Citrix® Access Gateway™ securely delivers any application with policy-based SmartAccess control. Users can obtain easy-to-use secure access to all of the enterprise applications and data they need to be productive. IT organizations can cost-effectively extend access to applications outside the datacenter while maintaining strict control through SmartAccess application-level policies. IT organizations can cost effectively meet the demands of all workers, deliver flexible working options and implement business continuity while ensuring the highest-level of information security and reducing support calls.

For more information, see the *Citrix Access Gateway Enterprise Edition Administrator's Guide* on Citrix.com.

Application Firewall

Citrix Application Firewall™ uses application level security for filtering content in requests or responses. Application Firewall includes numerous security checks, such as credit card leak prevention, cookie consistency, SQL injection protection, buffer overflow prevention and other HTML security checks, as well as embedded XML firewall. For more information about Application Firewall, see the *Application Firewall Guide* on Citrix.com.

Surge protection

NetScaler insulates servers and sites from sudden spikes in traffic by decoupling browser connections from the server and queuing requests on NetScaler before forwarding. The queue dynamically regulates traffic and prevents servers from being overloaded, 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. For more information about surge protection, see the *NetScaler Application Security Guide* on Citrix.com.

HTTP DoS protection

One effective way to rob a server of its resources is to flood it with legitimate HTTP GET requests. These requests, arriving at a rapid rate, originate from drone clients and, since they are legitimate application requests, the server will treat them as such and will become quickly overwhelmed, causing a DoS condition. When this type of attack happens, NetScaler identifies and prioritizes client requests, setting high priority for legitimate clients and low

priority for suspected drone clients, preserving capacity for genuine users and legitimate requests. NetScaler is unique in its ability to continue service delivery to legitimate users at the maximum capacity of the infrastructure during attack conditions. Most attack protection products are limited in their ability to prevent such attacks, as they provide only the means to shut off or rate limit traffic when an attack happens or, worse, they consume 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, ensures the continuity of service to legitimate users, regardless of whether attacks are occurring or not. For more information about HTTP DoS Protection, see the *NetScaler Application Security Guide* on Citrix.com.

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. For more information about priority queuing, see the *NetScaler Application Security Guide* on Citrix.com.

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 customers' expectations and their browsing experience. For more information about SureConnect, see the *NetScaler Application Optimization Guide* on Citrix.com.

Summary

NetScaler ensures that 100 percent of Web applications and content can be secured from end-to-end without degradation of user performance or responsiveness. A single NetScaler appliance can complete up to 48,000 SSL TPS and deliver encryption throughput of up to 6.5 Gbps per second, which is enough to secure all applications for most Web sites. For those sites requiring more secure throughput, the MPX 17000 offers system throughput at a faster rate. In addition, 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-commerce vendors and content providers no longer need to accept slower performance, increased network complexity or higher costs to achieve 100 percent secure application delivery.

**Worldwide Headquarters**

Citrix Systems, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309, USA
T +1 800 393 1888
T +1 954 267 3000

Americas

Citrix Silicon Valley
4988 Great America Parkway
Santa Clara, CA 95054, USA
T +1 408 790 8000

Europe

Citrix Systems International GmbH
Rheinweg 9
8200 Schaffhausen, Switzerland
T +41 52 635 7700

Asia Pacific

Citrix Systems Hong Kong Ltd.
Suite 3201, 32nd Floor
One International Finance Centre
1 Harbour View Street
Central, Hong Kong
T +852 2100 5000

Citrix Online Division

6500 Hollister Avenue
Goleta, CA 93117, USA
T +1 805 690 6400

www.citrix.com

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) is the leading provider of virtualization, networking and software as a service technologies for more than 230,000 organizations worldwide. Its Citrix Delivery Center, Citrix Cloud Center (C3) and Citrix Online Services product families radically simplify computing for millions of users, delivering applications as an on-demand service to any user, in any location on any device. Citrix customers include the world's largest Internet companies, 99 percent of *Fortune* Global 500 enterprises, and hundreds of thousands of small businesses and prosumers worldwide. Citrix partners with over 10,000 companies worldwide in more than 100 countries. Founded in 1989, annual revenue in 2008 was \$1.6 billion.

©2009 Citrix Systems, Inc. All rights reserved. Citrix®, NetScaler®, nCore™, Citrix Application Firewall™ and Access Gateway™ are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.