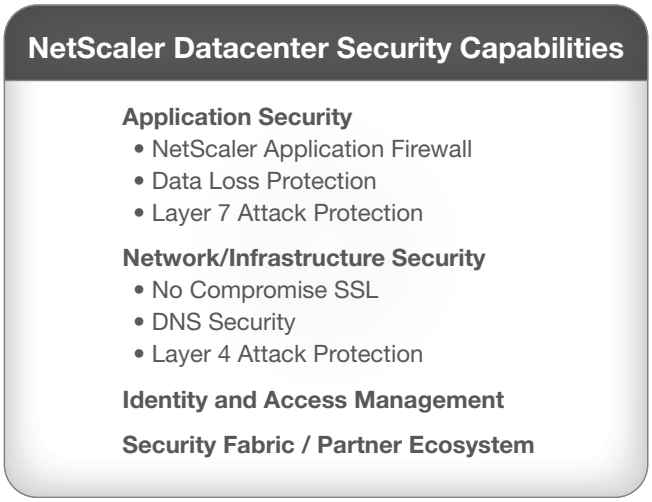
Citrix NetScaler—A foundation for next-generation datacenter security

CITRIX®

Introduction

The need for robust datacenter security has never been greater. Traditional challenges and concerns—including extensive regulatory requirements, the rise of targeted attacks, and the continuing erosion of perimeter-centric security models—are now being joined by the need to account for highly dynamic enterprise cloud architectures and flat networks with fewer, natural 'choke points.' Add the ever-present budgetary pressures to do more with less, and it becomes clear that the foundation for stronger security must be built using existing datacenter infrastructure.

Citrix NetScaler, the best application delivery controller (ADC) for building enterprise cloud networks, is precisely such a solution. Already a strategic component in thousands of enterprise datacenters, NetScaler delivers an extensive portfolio of essential datacenter security capabilities. Moreover, it minimizes the need for enterprises to invest in a large number of expensive, standalone security solutions. NetScaler not only provides critically important application security, network/infrastructure security, and identity and access management, but also supports a rich ecosystem of partner products to cover adjacent security domains.



The net result is a strong foundation for next-generation datacenter security that is also cost effective.

NetScaler for Application Security

Security practitioners are justifiably investing substantial time, effort, and money on application-layer security. After all, attacks against vulnerable application-layer services, faulty business logic, and valuable data have proven quite fruitful. Accordingly, NetScaler incorporates numerous app-layer protections, including a full-featured application firewall, data loss protection, and countermeasures for thwarting denial-of-service (DoS) and other Layer 7 attacks.

NetScaler Application Firewall

Traditional network firewalls lack the visibility and control required to protect against the more than 70 percent of Internet attacks that target application-layer vulnerabilities. This is the rationale behind the NetScaler Application Firewall, a comprehensive ICSA-certified web application security solution that blocks known and unknown attacks against web and web services applications. Employing a hybrid security model and analyzing all bi-directional traffic, including SSL-encrypted communications, Application Firewall counteracts a broad range of security threats without requiring any modifications to applications.

Hybrid security model. A combination of both positive and negative security models provides the most complete protection against all modes of attack. To defeat new, unpublished exploits, a positive-model policy engine that understands permissible user-app interactions automatically blocks all traffic falling outside this scope. Complementing this, a negative model engine uses attack signatures to guard against known threats to applications.

XML protection. In addition to blocking common threats that can be adapted for attacking XML-based apps (e.g., cross-site scripting, command injection, etc.), Application Firewall incorporates a rich set of XML-specific protections. These include: schema validation to thoroughly verify SOAP messages and XML payloads, the ability to block XML attachments containing malicious executables, defense against XPath injection techniques for gaining unauthorized access, and the ability to thwart related DoS attacks (e.g., excessive recursion).

Advanced protection for dynamic elements. Augmenting the default protection profile, an advanced profile provides essential security for applications that process user-specific content Multiple, session-aware protections secure dynamic application elements such as cookies, form fields, and session-specific URLs, thereby thwarting attacks that target the trust relationship between client and server (e.g., cross-site request forgery). Application dynamism is handled by the positive security engine, and secured without explicitly defining each dynamic element in the policy. Because only exceptions need to be learned, configuration is easier and change management is simplified.

Tailored security policies. An advanced learning engine automatically determines the expected behavior of enterprise web applications and generates human-readable policy recommendations. Administrators can then tailor the security policy to the unique requirements of each application, and avoid potential false-positive events.

Ensured compliance. Application Firewall enables enterprises to achieve compliance with data security mandates—such as the Payment Card Industry Data Security Standard, which explicitly encourages the use of web app firewalls for public-facing applications that handle credit card information. Detailed reports can be generated to document all protections defined in the firewall policy that pertain to PCI mandates.

Zero-compromise performance. The industry's highest performing web application security solution delivers up to 12 Gbps of comprehensive protection without degrading application response times. In addition, NetScaler improves

application performance through advanced acceleration technologies (e.g., content caching) and server offload capabilities (e.g., TCP connection management, SSL encryption/decryption, and data compression).

Fully integrated architecture. More than simply deployed on the NetScaler platform, Application Firewall is tightly integrated with it. Object and policy level sharing simplify administration, while system-level process sharing ensures high performance by avoiding the need for multi-pass packet processing.

Data Loss Protection

Unexpected leakage of sensitive data in application server responses results from a successful attack against the application, a flaw in the application's design, or misuse by an authorized user. A prudent step for enterprises to take, and an essential part of a defense-in-depth security strategy, is to actively guard against such leakage. NetScaler facilitates this requirement with a straightforward, easy-to-use data loss protection capability.

Safe Object data checks, an integral feature of the NetScaler Application Firewall, provide administrator-configurable protection for sensitive business information, such as social security numbers, order codes, and country/region-specific telephone numbers. An administrator-defined regular expression or custom plug-in tells the application firewall the format of this information and defines the rules to be used to protect against leakage. If a string in a user request matches a safe object definition, the application firewall can then take appropriate action, including

- Block the response
- Mask the protected information
- Remove the protected information from the response before sending it to the user

Different actions can be specified for each individual Safe Object rule.

NetScaler also provides Credit Card check to prevent inadvertent leakage of credit card numbers. Inspection of header information and payload data provides the thoroughness needed to avoid false negatives, while algorithmic string matching delivers the high-accuracy detection needed to avoid false positives. If a credit card number is discovered, and the administrator has not allowed credit cards numbers to be sent for the app in question, then the response can be blocked in its entirety, or the firewall can be set to mask all but the last 4 digits of the number (e.g., xxxx-xxxx-xxxx-5678).

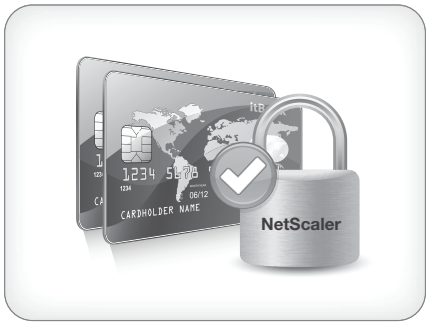


Figure 1: NetScaler protects against the leakage of confidential customer information.

The net result is another powerful feature set IT security teams can use not only to monitor for misuse events and successful attacks, but also to substantially limit their impact.

Additional Layer 7 Attack Protection

NetScaler includes several additional mechanisms that provide application-layer attack protection.

HTTP protocol validations. Enforcing RFC compliance and best practices for HTTP use is a highly effective way that NetScaler eliminates an entire swathe of attacks based on malformed requests and illegal HTTP protocol behavior. Additional custom checks can also be added to the security policy by taking advantage of integrated content filtering, custom response actions, and bi-directional HTTP re-write capabilities. Potential use cases expand to include: preventing users from accessing specified parts of a web site unless they are connecting from authorized locations; defending against HTTP-based threats (e.g., Nimda, Code Red), and removing information from server responses that could be used to perpetrate an attack.

Figure 2: Citrix NetScaler secures web applications.

HTTP DoS protection. An innovative method is used to mitigate HTTP GET floods. When an attack condition is detected (based on a configurable threshold for queued requests), a tunable percentage of clients is sent a low-impact computational challenge. This challenge is designed such that legitimate clients can easily respond to it properly, but 'dumb' DoS drones cannot. This enables NetScaler to distinguish bogus requests from requests sent by legitimate application users. Adaptive timeouts and other mechanisms can also be employed to defend against other types of DoS threats, such as SlowRead and SlowPost attacks.

Rate limiting (and more). One approach for thwarting DoS attacks is to keep network and servers from overloading by throttling or redirecting traffic that exceeds a specified limit. To that end, AppExpert rate controls trigger NetScaler policies based on connection, request, or data rates either to or from a given resource (i.e., virtual server, domain, or URL). Closely related capabilities include:

- Surge protection for dampening the impact of traffic spikes on servers
- Priority queuing to ensure that critical resources are served ahead of non-critical resources during periods of high demand

NetScaler for Network and Infrastructure Security

NetScaler also incorporates several network and infrastructure-oriented security capabilities. Most notable among these are extensive support for SSL-based encryption, DNS security, and Layer 4 attack protection.

No-Compromise SSL

Whether it's to ensure app delivery policies are fully applied to encrypted traffic and/or to offload back-end server infrastructure, ADCs must include the ability to process SSL-based traffic. Simply having basic functionality in this area is no longer sufficient, however, as two factors are driving SSL processing requirements to the point of over stressing infrastructure resources.

First, enterprises are increasingly adopting an *SSL Everywhere* posture. Typically pursued to pacify customer concerns and counteract hacking tools such as Firesheep, this is where encryption is used not only for the sensitive parts of an app, such as a login page, but for the entire application surface area. The result is a dramatically growing SSL footprint.

The second issue involves the deprecation of 1024-bit encryption keys in favor of 2048-bit (and larger) keys. Consistent with guidance issued by the U.S. National Institute of Standards and Technology (NIST), this transition is also being driven by leading browser vendors' plans to not support websites using certificates with keys weaker than 2048 bits beyond December 31, 2013. The impact in this case is an exponential increase in strength of encryption, but at a cost of least 5 times greater processing demands.

NetScaler appliances address both of these trends. By incorporating dedicated SSL acceleration hardware with support for both 2048 and 4096 bit keys, NetScaler delivers essential encryption capabilities that avoid the need to make tradeoffs between having stronger security and maintaining a high-performance user experience.

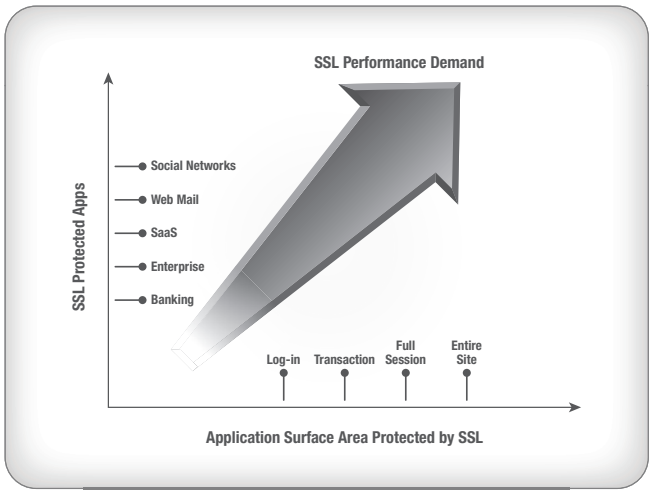


Figure 3: SSL everywhere increases security and performance requirements.

Another related feature is policy-based encryption. With this capability, administrators can configure NetScaler to automatically encrypt portions of legacy web apps that were originally designed to not use encryption, but now warrant it.

For those organizations requiring a high-level of cryptographic assurance, NetScaler is also available in FIPS 140-2, Level 2 compliant models.

DNS Security

DNS is an essential infrastructure service for the modern datacenter. In the absence of a robust, secure DNS implementation, the availability and accessibility of key services and applications is put in jeopardy.

In addition to providing high-scale load balancing of an organization's internal DNS servers when operating in DNS proxy mode, NetScaler can also be configured to operate as an authoritative DNS (ADNS) server to directly handle name and IP resolution requests.

In either deployment scenario, NetScaler delivers a robust, secure implementation based on the following features:

Hardened design – Designed from the start as a hardened service, NetScaler's implementation of DNS is not based on open source BIND, and, therefore, not subject to the vulnerabilities routinely discovered in BIND.

RFC compliance/enforcement – NetScaler performs full DNS protocol validation and enforcement to automatically block attacks leveraging malformed DNS requests, or other types of DNS misuse.

Native DNS rate limiting – To help prevent DNS flood attacks, policies can be set to rate limit or drop queries based on configured parameters. This control can be implemented based on query type and/or domain name – a feature that enables enterprises and service providers serving multiple domains to establish separate policies for each.

Cache poisoning protection with DNSSEC – Response hi-jacking is a serious class of threats that involves hackers injecting forged records into a DNS server, thereby poisoning its cache. These records then direct users to a hacker-controlled site that serves malicious content or otherwise attempts to harvest valuable account and password information. NetScaler guards against this type of threat with two powerful protections:

- Built-in support for DNSSEC that can be implemented for both ADNS and proxy DNS configurations. NetScaler enables response signing so that resolving clients can subsequently validate authenticity and integrity of the response. This standards-based approach eliminates the introduction of forged records into an otherwise vulnerable DNS cache.
- Randomizing DNS transaction IDs and source port information makes it difficult for a hacker to insert the necessary information into a request and corrupt DNS records.

Layer 4 Attack Protection

NetScaler protects against network-layer DoS attacks by ensuring that back-end resources are not allocated until a legitimate client connection has been established and a valid request has been received.

For example, NetScaler's defense against TCP-based SYN floods is based primarily on allocating resources only after a three-way TCP handshake between the client and NetScaler appliance has been fully completed, and secondarily on having a performance-optimized, security-enhanced implementation of SYN cookies.

In addition, a hardware platform and operating system architecture capable of processing millions of SYN packets per second provides assurance that NetScaler itself does not succumb to such attacks.

Other network-layer security protections include: (a) layer 3 and 4 access control lists (ACLs) that can allow necessary application traffic while blocking everything else, (b) the rate limiting, surge protection, and priority queuing capabilities discussed previously, and (c) a high performance, standards-compliant TCP/IP stack that has been enhanced to:

- Automatically drop malformed traffic that could pose a threat to back-end resources.
- Prevent disclosure of connection and host-based information (e.g., server addresses and ports) that could prove useful to hackers intent on perpetrating an attack.
- Automatically thwart a multitude of DoS threats, including ICMP flood, pipeline, teardrop, land, fraggle, small/zero window, and zombie connection attacks.

AAA for Application Delivery

Although having robust network, infrastructure, and application layer coverage is essential to achieving effective datacenter security, it is simply not enough. Another dimension IT security teams need to account for is the user layer. NetScaler delivers an extensive set of AAA functionality:

- **A**uthentication capabilities for validating user identities.
- **A**uthorization for verifying and enforcing which specific resources each user is allowed to access.
- **A**uditing capabilities to keep a detailed record of each user's activities (i.e., for troubleshooting, reporting, and compliance purposes).

The strength of the NetScaler AAA solution is not only its broad capabilities, such as support for password changes and a wide variety of authentication mechanisms (e.g., local, RADIUS, LDAP, TACACS, certificates, NTLM/Kerberos, and SAML/SAML2). More importantly, NetScaler centralizes and consolidates these services across applications. Rather than implementing, enforcing, and managing these controls individually for every application, administrators can take care of everything in one place. Advantages of this approach include the ability to:

- **Improve server performance** – Server load can be reduced and application performance improved as back-end resources are freed from having to perform AAA tasks.

- **Add security to legacy apps** – Critical security functionality can be added to legacy apps lacking native AAA capabilities. Modern apps also benefit from a greater array of choices—such as having the ability to incorporate stronger authentication or more granular logging without modifying the application.
- **Deliver a consistent user experience** – The user experience can be homogenized by standardizing authentication mechanisms, parameters (e.g., timeouts), and policies (e.g., for handling failed attempts) across sets of applications.
- **Enable single sign-on (SSO)** – Users need only log in once, as NetScaler transparently logs them in to all of the resources within a given domain.
- **Enhance security** – Numerous opportunities exist to strengthen security, including: enabling multi-factor or secondary authentication mechanisms; implementing secure logout (i.e., where authentication cookies automatically timeout); and enforcing consistent policies across different sets of users and/or resources.
- **Simplify security design** – Having just one place (rather than 10's or 100's of them) to implement and manage AAA services significantly streamlines administration and reduces the potential for errors that lead to gaps in an organization's defenses.

Establishing a Security Fabric with NetScaler Partner Products

NetScaler's value as a datacenter security solution is strengthened by a rich ecosystem of partner products. Key examples include:

- **Reporting and analytics** – A standards-based technology, NetScaler AppFlow extends the TCP-level information already captured by IPFIX—the IETF standard for NetFlow—to include per flow application-layer data records. Completely non-intrusive, AppFlow eliminates the need for proprietary taps, software agents, or additional devices by leveraging an organization's existing NetScaler infrastructure to provide insight into who is using which resources, when, and to what extent. Splunk, a Citrix Ready Partner, consumes AppFlow data in its *Splunk for NetScaler with AppFlow* solution to enable analysis and reporting of security related details such as: SSL VPN and application firewall events, policy violations, and resources under attack.
- **Security information and event management (SIEM)** – NetScaler App Firewall also supports the Common Event Format (CEF) and syslog for data output to third-party solutions. One common use case is the processing of NetScaler event and log information by leading SIEM platforms (e.g., HP ArcSight and RSA enVision) for operational security and compliance management purposes.
- **Vulnerability management** – HailStorm and ClickToSecure from Citrix Ready Partner Cenzic provide dynamic, black-box testing of web sites to generate vulnerability information. In this instance, the partnership has led to simplified import of Cenzic scan results into the NetScaler Application Firewall for configuring rules to protect against threats that target vulnerabilities discovered in applications and services.

A handful of other representative partners and their technologies include: RSA (Adaptive Authentication), Qualys (vulnerability management), Sourcefire (IPS and real-time network awareness), TrendMicro (AV and web security), and Venafi (key/certificate management). The bottom line is that these, and a host of other available partner solutions, enable enterprises to build on the foundation provided by NetScaler to establish a complete datacenter security fabric.

Conclusion

Ongoing budget constraints and a mounting requirement for increasingly robust datacenter security have created a scenario where enterprises need to do more for less. Citrix NetScaler, the best application delivery controller for building enterprise cloud networks, is a perfect fit for this situation. Combining an extensive portfolio of application, network, and user—layer security capabilities with a rich ecosystem of interoperable partner products, NetScaler enables today's enterprises to leverage their existing infrastructure to establish and extend upon a robust, cost-effective foundation for next-generation datacenter security.

Citrix Partner

Corporate Headquarters
Fort Lauderdale, FL, USA

Silicon Valley Headquarters
Santa Clara, CA, USA

EMEA Headquarters
Schaffhausen, Switzerland

India Development Center
Bangalore, India

Online Division Headquarters
Santa Barbara, CA, USA

Pacific Headquarters
Hong Kong, China

Latin America Headquarters
Coral Gables, FL, USA

UK Development Center
Chalfont, United Kingdom

About Citrix

Citrix Systems, Inc. (NASDAQ:CTXS) transforms how businesses and IT work and people collaborate in the cloud era. With market-leading cloud, collaboration, networking and virtualization technologies, Citrix powers mobile workstyles and cloud services, making complex enterprise IT simpler and more accessible for 260,000 organizations. Citrix products touch 75 percent of Internet users each day and it partners with more than 10,000 companies in 100 countries. Annual revenue in 2011 was $2.21 billion. Learn more at www.citrix.com.

©2012 Citrix Systems, Inc. All rights reserved. Citrix® and NetScaler® are trademarks or registered 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.