Secure SSL, Fast SSL

Citrix NetScaler and Thales nShield work together to protect encryption keys and accelerate SSL traffic
With growing use of cloud-based, virtual, and multi-tenant services, customers want to utilize virtual and multi-tenant appliances such as NetScaler VPX and SDX with enhanced SSL key management. Thales nShield manages large numbers of SSL keys within a FIPS 140-2 Level 3 certified environment. The combined Citrix and Thales solution optimizes SSL traffic and securely manages the critical cryptographic keys to minimize the exposure of sensitive data within the IT infrastructure.

**SSL is Corporate**

The Secure Sockets Layer (SSL)\(^1\) cryptographic protocol is widely used to provide secure communications over the Internet. Because it is relatively simple to implement and enjoys broad industry support, SSL is used extensively for protecting confidential data, for web-based retail and banking applications, and for collaboration tools such as electronic mail, instant messaging, and voice-over-IP (VoIP).

As eCommerce continues to grow, and as governments and standards bodies impose more regulatory requirements for security and privacy, SSL traffic now accounts for a significant share of overall Internet traffic. Today, almost half of the world’s websites are SSL enabled.

<table>
<thead>
<tr>
<th>Percent of Internet traffic using SSL:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Fixed Access</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>North America</td>
</tr>
<tr>
<td>Europe</td>
</tr>
<tr>
<td>Asia Pacific</td>
</tr>
</tbody>
</table>

Percent of aggregate Internet traffic during peak periods. Source: Sandvine Global Internet Phenomena Report, 1H 2014.

Percent of websites SSL-enabled: 45%

Percent of Alexa’s top 1 million websites enabled for SSL/TLS. Source: Julien Vehent blog post at jve.linuxwall.info

Table 1: SSL traffic now accounts for a significant share of overall Internet traffic

SSL is no longer just for “consumer” Internet applications. It is playing a growing and critical role protecting corporate data. Enterprises are increasingly relying on SSL to protect traffic to and from:

- Software as a Service (SaaS) applications
- Cloud-based storage and backup services
- Cloud application hosting services
- New corporate applications deployed on public, private and hybrid cloud infrastructures

\(^1\) Much “SSL traffic” today actually uses the newer Transport Layer Security (TLS) protocol, but for simplicity we will use “SSL” here rather than SSL/TLS.
Vendors and enterprises are also turning to SSL because it is a relatively standard way to encrypt traffic to an increasing number of mobile workers and mobile devices such as laptops, smartphones, tablets and phablets. For example, XenApp® and XenDesktop®, Citrix®’s application and desktop virtualization solutions, use SSL connections to give users secure and remote access from anywhere on any device.

Because of these trends, SSL is increasingly being used to protect business-to-business and intra-business traffic. One recent analysis found that in key parts of the world 30% or more of applications observed on corporate networks were capable of using SSL.

**Percent of applications SSL enabled:**

<table>
<thead>
<tr>
<th>Region</th>
<th>SSL Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas and Canada</td>
<td>32%</td>
</tr>
<tr>
<td>Europe</td>
<td>30%</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>32%</td>
</tr>
</tbody>
</table>

Table 2: In key parts of the world almost one-third of applications on corporate networks are SSL-enabled

**Requirements for SSL: Secure Key Management and Fast Performance**

Because SSL is increasingly being used for business applications, enterprises have had to come to grips with both security and performance issues related to SSL.

Security is obviously a critical question when SSL traffic is being used to carry intellectual property, financial information, personal data of customers and employees, and other company confidential information.

Managing SSL encryption keys is a critical security issue that many organizations overlook. As described in National Institute of Standards and Technology (NIST) Special Publication 800-57: “Keys are analogous to the combination of a safe. If a safe combination is known to an adversary, the strongest safe provides no security against penetration.”

Key management not only encompasses how keys are protected from direct attack, but also operational issues such as the backup of keys and their recovery in the event of system failures or disasters, and compliance issues related to ensuring that access to keys by administrators is controlled and monitored.

Increasing SSL traffic can have a serious negative impact on the perceived performance of web-based applications. Not only do systems on each side of the connection need to encrypt and decrypt the traffic, but significant computing resources are required to create a “handshake” and authenticate a certificate. These activities can slow down the browser client, the web server and the network.

---

2 For example, when an end user visits a web page, the browser client creates a TCP socket to the web server and issues a secure session request. The web server returns a certificate. The browser client authenticates the certificate, generates a key, and sends the key to the web server. The web server uses the key to encrypt the content of the page, and sends the content to the browser client. The browser then decrypts the content. Several of these steps may be repeated for each object on the page, including images and scripts.
In short, as SSL traffic grows and carries more confidential information for mission-critical applications, how can organizations protect encryption keys and application performance without vast new investments in hardware and network bandwidth?

Thales nShield Connect and Citrix NetScaler® work together to enhance the security of cryptographic keys and to offload and accelerate SSL processing. The solution involves integrating Thales nShield Connect hardware security module (HSM) with the Citrix NetScaler application delivery controller (ADC). An overview of the integrated solution is shown in Figure 1, and some of the highlights are discussed below.

Figure 1: Thales nShield Connect and Citrix NetScaler work together to provide secure key management and to offload and accelerate SSL processing

**Secure Key Management with Thales nShield Connect**

nShield Connect from Thales e-Security is a high-performance network-attached hardware security module (HSM) that securely manages cryptographic keys in order to minimize the exposure of sensitive data within the IT infrastructure.

Key management involves a variety of functions, including:

- Key generation, to create truly random keys.
- Key registration, to associate keys with users, systems and applications.
- Key storage, to ensure that keys are isolated from other systems that have the potential to be compromised.
- Key distribution, to make keys available quickly when they are needed.
Key backup and recovery, to ensure that keys are available in the event of a local system failure or a disaster such as a data center fire or a hurricane.

Key rotation, revocation and destruction, to ensure that keys can be replaced and destroyed with complete certainty.

nShield Connect performs these functions with a high level of security, performance and operational efficiency. It is a dedicated appliance that isolates cryptographic processes and keys so they cannot be accessed if applications and servers are compromised.

Security features and capabilities include:

- A highly secure hardware system with a custom built chassis to guard against physical attack, and with tamper response mechanisms (i.e., mechanisms that wipe out keys and “critical security parameters” if the cover is opened or if physical probing is detected).
- Monitoring of environmental conditions, including the integrity of the chassis, power supplies and temperature, to detect potential attack.
- Identity-based authentication mechanisms, so user actions can be recorded and audited.
- Strong separation of duties, to ensure that no single individual has excessive access to keys or system features.

Performance and operational advantages include:

- Protection and management of private keys and acceleration of RSA offload operations.
- Backup techniques that avoid the need to archive keys in dedicated hardware or backup HSMs.
- The ability to combine multiple units for load-balancing, resilience and failover.
- Support for remote operations and backup in lights-out data centers, so centralized staff can manage keys globally without local assistance.

Together these features provide for maximum protection of keys, improved performance, and lower operating costs.

**Offload and accelerate SSL processing with Citrix NetScaler**

NetScaler is the world’s most advanced Application Delivery Controller (ADC) for mobile and web applications. It has several features that help offload and accelerate SSL processing, as well as accelerating other types of traffic.

Key capabilities of NetScaler include:

- Server and database load balancing, to distribute traffic to multiple servers in order to achieve optimal resource utilization, maximize throughput, and minimize response times.
- SSL offload and acceleration, to speed up the handling of the encryption and authentication requirements of SSL web traffic.
- SSL VPN, to terminate SSL VPN connections without using the resources of a web server.
- TCP offload, to reduce traffic by consolidating multiple requests from multiple clients into a single TCP socket to the back-end servers.
• Compression, to reduce the volume of web traffic.
• Application firewall, to scan network traffic and protect against DDOS attacks and a broad range of web-based threats.
• Clustering, for fast, simple scalability.

Figure 2: NetScaler provides key features that enhance availability, performance and security for Web-based applications

Citrix NetScaler is available as high-performance hardware appliances, as flexible software-based virtual appliances, and as appliances with advanced virtualization to support multiple NetScaler instances in a multi-tenant environment.

Conclusion: Taming SSL for Corporate Use
SaaS applications, cloud hosting and mobile computing are increasing the importance of SSL traffic as a business issue in an enterprise. Enterprises can no longer afford to take SSL security and performance for granted because:

• More confidential information is being carried in SSL traffic, so data breaches caused by deficient key management practices could cost millions of dollars in breach notification costs, regulatory fines, and stolen intellectual property
• More mission-critical applications are being deployed with SSL, so performance problems can have a direct impact on employee productivity and customer satisfaction

Thales e-Security and Citrix help Enterprises meet those challenges with a solution that integrates nShield Connect and NetScaler. This solution provides a very high level of security for encryption keys, simplifies and centralizes key management, and improves application performance by offloading key management tasks and SSL termination from web servers.

About Citrix
Citrix (NASDAQ:CTXS) is a leader in mobile workspaces, providing virtualization, mobility management, networking and cloud services to enable new ways to work better. Citrix solutions power business mobility through secure, personal workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. This year Citrix is celebrating 25 years of innovation, making IT simpler and people more productive. With annual revenue in 2013 of $2.9 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.

About Thales
Thales e-Security is a leading global provider of data encryption and cybersecurity solutions to the financial services, high technology, manufacturing, government and technology sectors. With a 40-year track record of protecting corporate and government information, Thales solutions are used by four of the five largest energy and aerospace companies, 22 NATO countries, and secure more than 80 percent of worldwide payment transactions. Thales e-Security has offices in Australia, France, Hong Kong, Norway, United States and the United Kingdom. www.thales-esecurity.com

Copyright © 2014 Citrix Systems, Inc. All rights reserved. Citrix, XenApp, XenDesktop and NetScaler are trademarks of Citrix Systems, Inc. and/or one of its subsidiaries, and may be registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies.