Best practices for implementing 2048-bit SSL

www.citrix.com

Executive summary

Secure sockets layer (SSL) technology continues to be essential to the growth of the web. With unabated increases in ecommerce traffic along with transmission of personal information, SSL is no longer just a *nice to have* capability; it is an absolute necessity. The requirement to protect information is further heightened by the universal availability of easy-to-use hacking tools such as Firesheep. This has prompted application owners to adopt an *SSL Everywhere or Always-On SSL* posture, encrypting not only the sensitive components of the application such as the login page, but the entire application *surface area*.

In addition to simply using SSL, the strength of encryption is also critical. Indeed, the security community has reached consensus that any application using SSL should migrate from the *de facto* standard of 1024-bit SSL key strength to 2048-bit (or larger) key sizes. Doubling key size from 1024-bit to 2048-bit offers an exponential increase in strength. From an infrastructure standpoint, however, the SSL processing power required with 2048-bit keys is 5 to 30 times greater than what is required for 1024-bit.

5x
Lower Performance

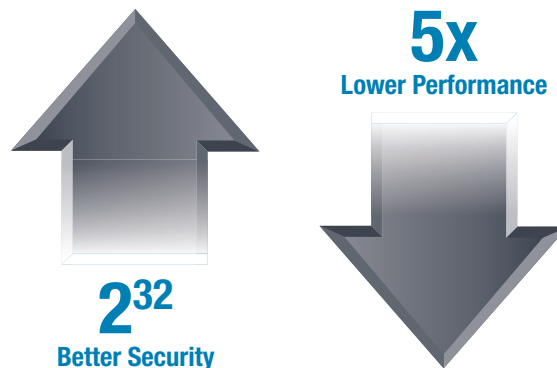2^{32}
Better Security

Figure 1: Impact of 2048-bit keys

To maintain application performance and availability, enterprises must upgrade their application delivery controller (ADC) and SSL infrastructure. Specifically, consideration should be given to selecting an ADC, like Citrix NetScaler, that is performance optimized for 2048-bit keys and that can provide dedicated SSL processing resources per application in a multi-tenant environment. Failure to consider these factors can lead to a degraded end user experience and result in expensive, unplanned infrastructure upgrades to handle the performance impact of 2048-bit keys.

Summary

• SSL usage becoming pervasive

• Industry transitioning to 2048-bit

• 2048-bit lowers performance 5x

2x Faster Performance

2048-bit SSL Transactions Per Sec

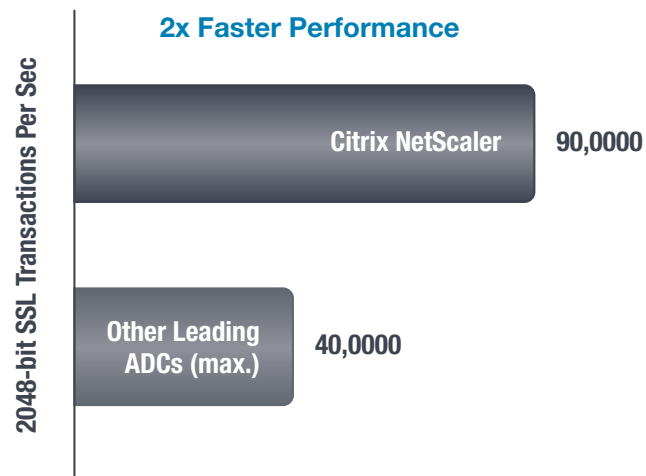| Citrix NetScaler | 90,0000 |
| Other Leading ADCs (max.) | 40,0000 |

Figure 2: Pick an ADC optimized for 2048-bit SSL

SSL everywhere (always-on SSL)

Enterprises increasingly rely upon the web to reach and retain customers. At the same time, readily available hacking tools like Firesheep pose a serious security threat to online operations. To combat these threats, organizations should adopt an SSL Everywhere posture. Simply encrypting login and checkout pages is no longer sufficient. Enterprises must expand the use of SSL to cover the entire user session to better protect themselves and their customers against security threats. For example, Google® Gmail® is now 100% SSL encrypted, and Facebook® offers their users the choice of encrypting every page using SSL.

As more SSL protected applications are put into production and the SSL footprint for each application expands, the aggregate SSL processing requirements of a typical enterprise increase much faster than other aspects of the datacenter infrastructure.

Summary

• Security threats increasing

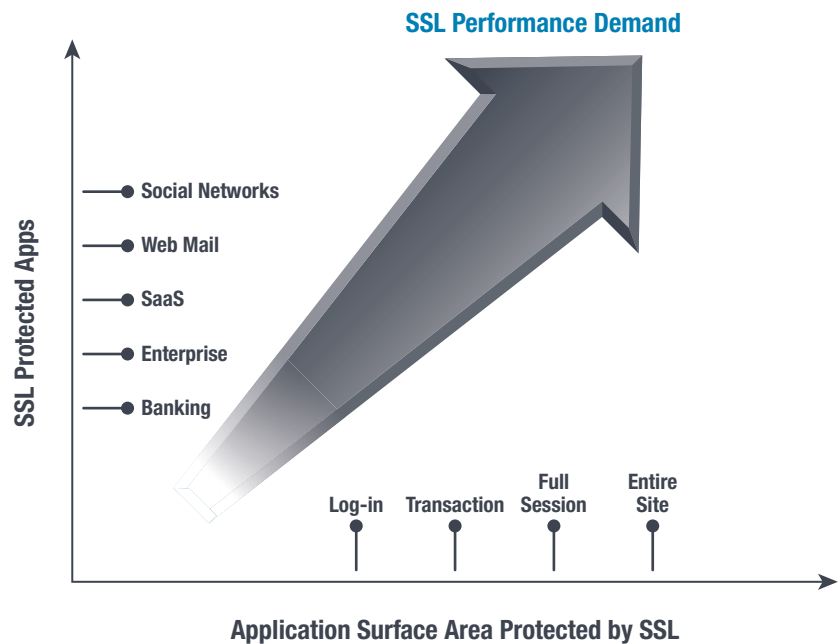• Forcing broader SSL adoption

• Need 2048-bit optimized ADC

Figure 3: Increase in SSL apps and SSL coverage

Advent of stronger SSL

Simply encrypting web application traffic, however, is only half the battle. If the encryption itself is not strong enough to withstand attack, it can be broken.

What an attacker can do with a compromised private key

The business impact of a private key being compromised would be dire. If someone manages to break a 1024-bit key and subsequently derives the corresponding session key used to encrypt and decrypt data, they will then be able to eavesdrop on all communications. For example, with the private key in hand, a hacker can silently observe someone logging in to their bank account or other password protected account, capture the user's credentials, and then masquerade as that user. This would completely compromise the security of the application and leave every user vulnerable. The hacker would have the proverbial *keys to the castle*.

Industry-wide move from 1024-bit to 2048-bit keys

The strength of encryption is directly tied to key size. Key size is expressed in number of bits (e.g., 1024-bit keys). The larger the key size, the more computationally expensive it is for an attacker to use brute force to compromise the public key / private key infrastructure.

Summary

- Encryption is first step
- Key size determines strength
- Smaller keys can be compromised

Less than 10 years ago, 512-bit keys were considered sufficiently secure. When 512-bit keys were cracked in highly publicized demonstrations, IT organizations quickly upgraded to 1024-bit keys. Increasing availability of inexpensive computational resources, however, has now put 1024-bit SSL keys within striking distance of hackers.

With so much at stake, organizations need to consider the threat facing their businesses and operations today. Companies must migrate to 2048-bit keys to ensure the security of their SSL encrypted applications. In fact, the U.S. National Institute of Standards and Technology (NIST), a recognized authority on security practices, has issued a security notification (NIST Special Publication 800-131B) which recommends that organizations deprecate the use of 1024-bit keys between 2011 and 2013. It also explicitly warns against the use of 1024-bit keys beginning in 2014.

Further, leading browser vendors, such as Mozilla®, with Firefox®, and Microsoft®, with Internet Explorer® will soon require websites to use 2048-bit keys to protect browser users. These browser vendors require certificate authorities (CA) to ensure that certificates issued with a key size smaller than 2048-bit will expire before December 31, 2013. For these reasons, all organizations should begin using at least 2048-bit keys to secure their applications and application data, and to ensure that their infrastructure can readily support larger key sizes.

> "From 2011 though 2013, the use of 1024-bit RSA keys to generate a digital signature is deprecated, and is disallowed beginning in 2014."
>
> **NIST Special Publication 800-131B, February 2011**

Maintaining application performance with 2048-bit SSL

While 2048-bit keys deliver greatly increased security, they also require significantly greater processing power than 1024-bit keys. This means—in order to maintain application performance and availability—organizations need to adopt new SSL infrastructure specifically designed for stronger SSL.

Impact of larger key sizes on application and infrastructure performance

In order to select SSL infrastructure that meets the demands of 2048-bit keys, it is important to understand how SSL works, as well as the factors that impact SSL performance. Every SSL session can be broken into two phases: 1) session negotiation and 2) bulk data encryption / decryption.

In the session negotiation or *SSL handshake* phase, the initial connection is established, the cipher suite is negotiated (i.e., what encryption and authentication algorithms will be used), the session ID is assigned and the session keys are generated and exchanged. Once the session is actually established, the bulk data transfer, including encryption and decryption of data, between the client and server happens. Importantly, the bulk data transfer phase is substantially less computationally expensive than the SSL handshake phase.

Summary

- 1024-bit security at risk
- NIST recommends 2048-bit
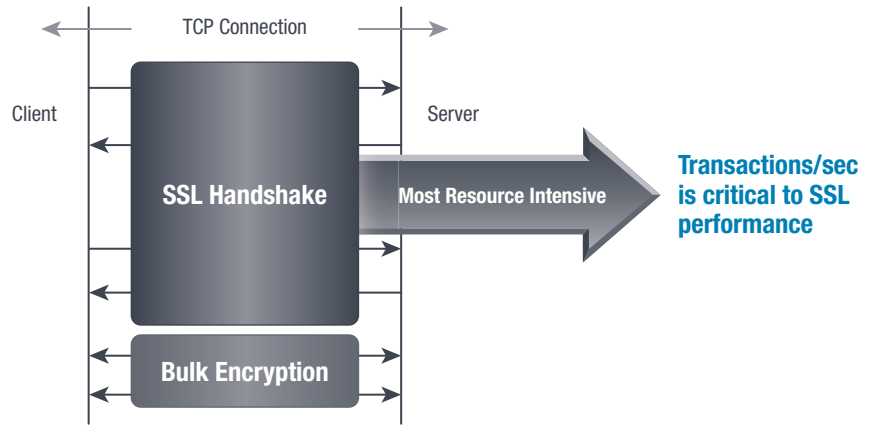- Larger key impacts performance

Figure 4: Anatomy of an SSL session

Understanding the distinction between the SSL negotiation phase and bulk encryption / decryption phase is crucial to fully appreciating how SSL security can impact web application performance, as well as the ability of the data center infrastructure to keep pace with traffic growth. The performance overhead imposed during the SSL session negotiation phase dominates the overall performance dynamics of SSL sessions. For any given application or infrastructure, the number of new SSL sessions that can be supported over a given period of time—commonly measured in SSL transactions per second (TPS)—is a critical metric.

SSL TPS performance is directly impacted by the size of SSL keys. Doubling key strength from 1024-bits to 2048-bits delivers an exponential increase in protection due to the sheer increase in mathematical computations required to break the larger keys. While better security is provided, the computational power required to process 2048-bit certificates is 5 to 30 times greater than what is required for 1024-bit certificates.

Summary

- SSL handshake consumes resources
- Transactions/sec key performance factor
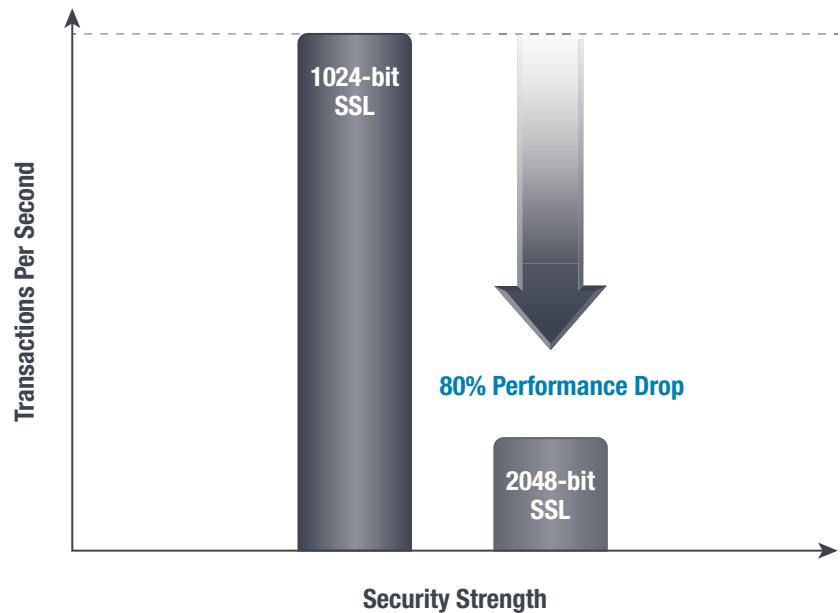- 2048-bit lowers TPS performance 80%

Figure 5: Performance Impact of 2048-bit keys

For example, an ADC appliance that is capable of handling 5,000 TPS for a 1024-bit certificate can only support approximately 1,000 TPS for a 2048-bit certificate. That means a web site operator would have to add 5 times more ADC appliances to provide the same SSL processing capacity the site had for 1024-bit certificates. The bottom line: enterprises need to properly plan for the migration from 1024-bit to 2048-bit certificates or risk significant performance degradation and business impact to their operations.

Specifically, enterprises need to consider that the infrastructure for SSL processing must be able to not only maintain high performance (i.e., no meaningfully induced latency) when negotiating SSL sessions, but must also have sufficient headroom to accommodate expected growth in the number of applications and amount of application traffic. While SSL throughput rates must still be taken into consideration, the most critical metric that needs to be considered for SSL performance is SSL transaction rate (i.e., SSL TPS).

Best practices for planning 2048-bit SSL processing infrastructure

In order to deliver appropriate levels of SSL TPS, *best practices* for building a scalable and efficient SSL network infrastructure must be understood. Unfortunately, off-the-shelf servers are inefficient for handling computationally intensive SSL tasks at high speed. While a newer generation of CPUs may provide native support for popular encryption algorithms (e.g., AES), these benefits are largely negated by the compute overhead first imposed during the session negotiation phase. Even if a server were able to support the SSL processing load, doing so would likely consume the available CPU and memory resources, impacting the server's ability to perform its primary role of running the application.

To address this issue, manufacturers have developed specialized SSL processors that are highly efficient in performing both the repetitive and computationally intensive tasks involved in SSL processing. These specialized processors are integrated into ADCs which are deployed in front of web and application servers and act as a proxy in the communication between a client and server. Offloading SSL processing to an ADC frees servers to perform their intended functions and offers a logical point of consolidation for SSL processing in the datacenter.

Another advantage of consolidating SSL processing with an ADC is SSL connection persistence. This is important in ecommerce transactions where the user needs to be connected to the same server until the session or transaction is complete. In SSL v3, a new SSL Session ID is used to establish client / server connection persistence. This Session ID is changed every two minutes in certain newer browsers. ADCs can be used to offload this frequent Session ID renegotiation and properly interpret the data to ensure connection persistence.

Summary

- 2048-bit migration requires planning
- Servers not optimized for SSL
- Use ADC for SSL acceleration

Best practices

Preparing the infrastructure for 2048-bit SSL certificates

1. Offload SSL session set-up and bulk data encryption to an ADC that is optimized for 2048-bit SSL processing. High-performance ADCs integrate hardware-based SSL acceleration that is capable of handling far more SSL TPS than a general purpose server. Advanced ADCs can also rewrite client requests and application responses from clear text HTTP to SSL-secured HTTPS on the fly, automatically forcing the entire application to be SSL protected even if the application was not originally designed for SSL.

2. Take inventory of each infrastructure element that is terminating SSL traffic. Make sure that it has the processing capacity to support stronger levels of encryption without adding latency or dropping packets.

3. Complete an audit of SSL certificates currently in use. Those that expire soonest will need to be renewed first, and your certificate authority will likely mandate that the certificate renewal be at 2048-bit key strength.

4. Evaluate current SSL performance requirements of your network and applications. Beyond measuring current traffic capacities, extrapolate historical growth rates for at least an additional three years. The goal is to design the infrastructure to meet both present and future requirements.

5. Do not focus solely on SSL throughput metrics. It is SSL transactions per second (TPS) that matters most for proper infrastructure sizing. Make sure that each component is optimized for 2048-bit keys.

6. Start with evaluation certificates for less mission critical applications to gain familiarity with the technology and understand the new performance demands. Free trial development SSL certificates are available from Symantec (certificate evaluation).

7. Move to 2048-bit certificates first. 4096-bit or greater SSL keys will only be required in exceptional circumstances.

8. For highly sensitive applications, re-encrypt communications between the ADC and the back-end server infrastructure. This provides end-to-end encryption which may be required in some environments. All popular ADC solutions support SSL re-encryption.

9. Measure end-user application performance before, during and after the transition to 2048-bit SSL. Pay particular attention to SSL session negotiation times at various load conditions. There are a number of commercial services that offer detailed performance measurements. However, make sure they have the capability to measure end-to-end performance of SSL-secured HTTPS applications. In addition, many ADCs also offer application performance monitoring tools that can be used to assess overall impact.

Summary

- Prepare infrastructure for 2048-bit
- Measure application performance
- Scale infrastructure as appropriate

Pick the *right* ADC

After deciding to offload SSL processing to an ADC, it is important to choose an ADC optimized to handle 2048-bit SSL traffic at high transaction rates and throughput levels. When evaluating the SSL performance of an ADC, keep in mind that SSL processing capabilities depend largely upon two factors: 1) the capability and capacity of integrated SSL processing hardware, and 2) finely-tuned software optimizations that maximize the performance of the integrated SSL chips or SSL acceleration cards.

Understanding the first factor is typically straightforward. It is recommended that datacenter managers discover it by evaluating a vendor's more recent product offerings. These platforms are likely built with the latest SSL processors designed to handle the larger 2048-bit and 4096-bit key sizes, and will provide much greater performance than older processors designed for 1024-bit keys. The second factor, software optimization, requires a bit more research to identify the *right* ADC.

Many ADC vendors actually use the same SSL processors. Therefore, aside from speed and the number of chips, SSL performance is dependent on how tightly coupled and intelligently the software is designed to extract maximum performance and utilization from those chips. Leading ADC vendors, like Citrix with NetScaler, have developed advanced technologies to optimize SSL performance for 2048-bit keys. These include:

- **Intelligent load balancing of SSL chips** – SSL sessions are load balanced across SSL chips to provide the best processing performance and lowest latency.

- **Multiple queues per SSL chip** – Multiple SSL operations can be queued per chip to optimize utilization of a chip's processing capabilities.

- **SSL resource isolation** – In a multi-tenant ADC deployment, each tenant is assigned dedicated SSL resources, preventing one ADC instance from consuming a disproportionate processing capacity and, thus, degrading the performance of other tenants.

The final consideration is whether to choose a hardware-based ADC or a software-based ADC virtual appliance. A hardware-based ADC with an integrated SSL ASIC processor is best suited for delivering applications with heavy SSL demands. For applications that do not require more than 50 to 100 SSL TPS , a virtual appliance ADC deployed on a modern datacenter class server should be sufficient.

Summary

- Pick the right ADC
- Not all ADCs are created equal
- NetScaler outperforms other ADCs

Citrix NetScaler

90,000 ssl tps

2x Faster Performance
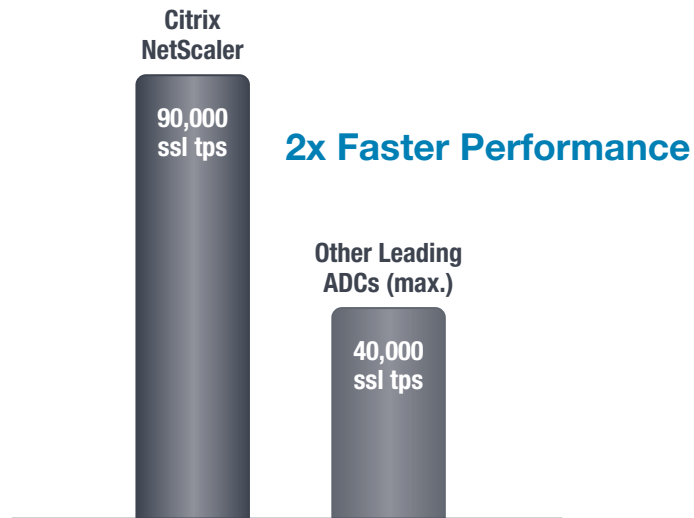
Other Leading ADCs (max.)

40,000 ssl tps

Figure 6: Citrix outperforms other ADCs in 2048-bit SSL performance

Conclusion

All web applications must now be secured by SSL using 2048-bit or longer key lengths. The migration from 1024-bit SSL to 2048-bit SSL delivers an exponential increase in protection. However, there is a cost. The SSL processing power required by 2048-bit keys is 5 to 30 times greater than for 1024-bit keys.

To maintain security and application performance, enterprises must upgrade their SSL infrastructure, particularly their ADCs. Evaluation of ADCs should focus on solutions optimized to process 2048-bit SSL certificates, such as Citrix NetScaler.

Failure to properly upgrade the SSL infrastructure can lead to a degradation of the end user experience, and result in expensive, unplanned infrastructure expenditures to handle the performance impact of 2048-bit keys.

CITRIX®

VeriSign
Secured®
VERIFY ▶

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 6301-10, 63rd Floor
One Island East
18 Westland Road
Island East, Hong Kong, China
T +852 2100 5000

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

www.citrix.com