NetScaler 2048-bit SSL Performance

July 2010

Overview

NetScaler 9.2 boosts SSL performance with 2048-bit keys 5X to meet the needs of customers as they transition to 2048-bit key sizes. Extending NetScaler's nCore architecture to better utilize the SSL hardware on device along with other enhancements enable this boost in performance. This paper details the SSL performance on current shipping MPX platforms.

SSL is a core technology to secure transactions on the Internet. The most widespread deployment model uses RSA public key cryptography with 1024-bit keys to negotiate a secure, symmetric session key between the client and server. Current security research has demonstrated the distinct, near term possibility of breaking 1024-bit RSA keys using significant computing resources. The U.S. National Institute of Standards and Technology (NIST) issued Special Publication 800-57 in March 2007 recommending the use of 2048-bit RSA keys starting Jan. 1, 2011. With current technology and research, doubling the key length from 1024-bit to 2048-bit increases the computational complexity of breaking a key by close to a billion times. 2048-bit keys are expected to be secure till 2030.

Following this recommendation and Microsoft Windows security guidelines, Certificate Authorities (CAs) are migrating to 2048-bit SSL certificates for end users. Extended Validation (EV) certificates (in use at major ecommerce and financial sites) are already at 2048-bit strength. Starting the later half of 2010, CAs will enforce this requirement by issuing only 2048-bit certificates.

How 2048-bit keys impact SSL performance

In recent years, the SSL transactions per second (TPS) performance on NetScaler has improved tremendously for 1024-bit keys. For instance, the NetScaler MPX 21500 (released 2010) can perform 220,000 TPS with 1024-bit keys compared with 25,000 TPS on the NetScaler 12000 (released 2007). Doubling the key lengths from 1024-bit to 2048-bit significantly increases the computational requirements and has a major impact on the TPS supported by the device. To support the same TPS with 2048-bit keys, the SSL infrastructure will need a significant upgrade (30x increase in some cases).

nCore architecture delivers exceptional SSL performance

NetScaler 9.1 introduced the nCore architecture to take advantage of multiple processor cores available on the MPX hardware platforms. In NetScaler 9.2, the nCore architecture was extended to the SSL acceleration processors. This includes:

- **Intelligent load balancing of SSL chips**: Each MPX platform contains multiple SSL chips. The nCore architecture allows the packet engines to intelligently load balance the SSL operations among the chips available.

- **Multiple queues per SSL chip**: To better utilize the chip hardware capabilities, multiple SSL operations can be queued per chip.

- **SSL card optimization**: Citrix has worked with Cavium Networks to optimize the performance of SSL hardware to process larger RSA keys (2048-bit and 4096-bit).

SSL Performance with 2048-bit keys

The SSL performance of NetScaler platforms with 2048-bit RSA keys is listed in the table below. All the tests were performed on NS 9.2nc B46.3 nCore. This version shows significant improvement in SSL TPS numbers with 2048-bit keys compared to previous releases.

Platform	**NS9.2 Performance (SSL TPS)**	**NS9.1 Performance (SSL TPS)**
MPX 5500	1000	350
MPX 7500	5,000*	2000
MPX 9500	11,000	2000
MPX 10500	18,000	4500
MPX 12500	22,000	4500
MPX 15500	22,000	4500
MPX 17000	22,000	4500
MPX 17500	22,000	4500
MPX 19500	33,000	6000
MPX 21500	45,000	7000

* Numbers have been rounded / normalized. Raw test data is available in the appendix.

Notes

- All MPX platforms have license imposed TPS and throughput limits that may be lower from the actual numbers achieved in this test. Refer to the official datasheet for supported SSL throughput by platform.

- The rows are grouped (shading) by hardware platform. For instance, the MPX 10500, 12500 and 15,500 share the same platform. Upgrade between the models in a group is possible through NetScaler's Pay-As-You-Grow model.

- The 2048-bit performance improvements are available on the MPX platforms only. The 2048-bit key SSL TPS number is significantly lower than the TPS with 1024-bit key size. For instance, the MPX21500 can do 220,000 1024-bit SSL negotiations per second versus 45,000 with 2048-bit keys. This is expected as doubling the key length exponentially increases the computation required (roughly 4-8 times).

NetScaler 9.2 Security highlights

NS9.2 also contains significant security highlights related to SSL and other security modules in the NetScaler system. These include:

- **OCSP support**: Dynamically check for Certificate revocation by connecting to an OCSP responder. This is in addition to the standard Certificate Revocation List (CRL) mechanism.

- **Subject Name Indicator (SNI) support**: extension to TLS1.1 that allows the modern browsers to indicate the server name to which it is trying to establish a secure channel. This is very useful in Virtual hosting scenarios.

- **Application Firewall CSRF support**: The Application Firewall module added new defense against Cross-Site Request Forgery attacks.

- **AAA Form-based SSO**: The AAA module now supports auto-submission of credentials to backend web applications that use a HTML form to request user credentials.

More information

Follow us on twitter at http://twitter.com/netscaler

NetScaler Product datasheets and other information are available at http://www.citrix.com/netscaler

Join the Citrix NetScaler community at http://community.citrix.com/p/cdn-networks

References

NIST Special Publication 800-57 – Recommendation for Key Management: http://csrc.nist.gov/publications/PubsSPs.html

NIST Special Publication 800-131 – Draft Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes: http://csrc.nist.gov/publications/PubsSPs.html

Verisign - https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=SO6989

Appendix:

Test description

Tests were performed with an internally developed test harness consisting of a client / server setup. Traffic is directed to an SSL VIP that is bound to HTTP servers on the backend (that is, NetScaler – Server communication is in the clear). Two separate tests were run on each platform to benchmark performance. Each test measures a single entry on each row, for instance SSL TPS. You can either maximize the TPS (column 1) or the bulk throughput (column 2).

SSL TPS

This test measures the number of SSL Transactions per Second (TPS). The NetScaler is loaded with a 2048-bit key. The client harness opens a new TCP connection, does a SSL negotiation, sends a single HTTP request and receives the full response. The transaction is terminated using a SSL CLOSE_NOTIFY after end of the response. Cipher suite used is RC4-SHA. The HTTP request and response are 64 bytes long.

SSL Throughput

This test measures the bulk throughput through the NetScaler. The client harness opens as many SSL sessions as necessary to measure the bulk throughput. Once the SSL session is established, the client maintains a persistent connection and sends requests to a 100KB page. Cipher suite used is RC4-SHA. All connections are terminated gracefully at end of test.

RSA key length does not impact the bulk throughput significantly. This testing focused on the SSL TPS performance, so the bulk throughput numbers are not tuned for maximum performance.

I: Raw test data

Platform	**SSL TPS**	**SSL Throughput (mbps)**
NS12000 (9.2cl)	2023	3140
MPX5500	1228	537
MPX7500	11,258	1074
MPX9500	11,258	3281

MPX10500	18,861	5239
MPX12500	22,753	8482
MPX15500	22,687	8516
MPX17000	22,362	7040
MPX17500	22,763	7509
MPX19500	33,885	11327
MPX21500	45,422	11410

II. SSL Performance with 1024-bit keys

Platform	**SSL TPS**	**SSL Throughput (mbps)**
MPX5500	5000	500
MPX7500	10,000	1000
MPX9500	20,000	3000
MPX10500	30,000	5000
MPX12500	60,000	6000
MPX15500	87,000	6500
MPX17000	100,000	6500

MPX17500	110,000	8000
MPX19500	165,000	10,000
MPX21500	220,000	11500

III SSL 2048-bit performance on 9.1 (B104.5)

Platform	**SSL TPS**	**SSL Throughput (mbps)**
NS12000 (classic)	2034	3002
MPX5500	366	536
MPX7500	2045	1099
MPX9500	2029	3321
MPX10500	4667	5367
MPX12500	4565	8412
MPX15500	4557	8374
MPX17000	4658	6976
MPX17500	4698	8168
MPX19500	6357	11969
MPX21500	7390	11682

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® and Citrix Application Firewall™ 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.