RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Is the Security Industry Ready for SSL Decryption?

SESSION ID: TECH-R01

John W. Pirc
Chief Technology Officer
NSS Labs Inc.
@jopirc

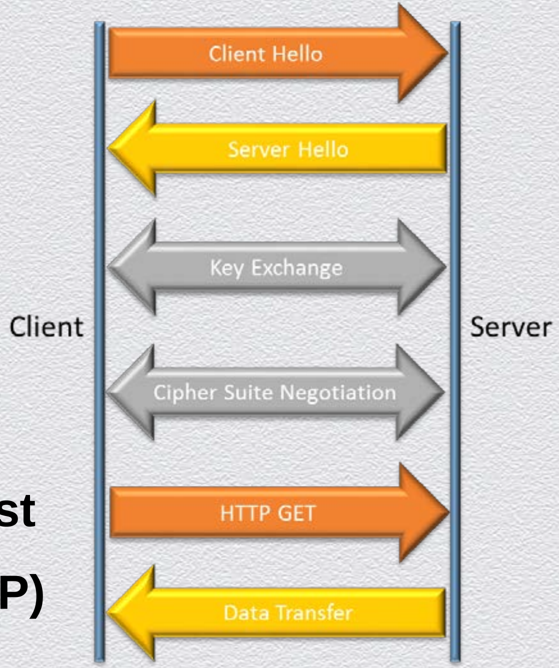
David DeSanto
Director, Product Management
NSS Labs Inc.
@david_desanto

Agenda

- SSL Primer
- What is Driving SSL Everywhere?
- Browsing History to Today
- The Adversary and SSL
- Network Security Product Visibility
- Encryption HW Acceleration
- NGFW / SSL Performance Results
- Recommendations / Key Takeaways

SSL Primer (Thank you Dr. Taher Elgamal)

- Secure Socket Layer / Transport Layer Security (SSL/TLS)
  - Netscape Communications:
    - 1994 SSL v.1 (Never released publicly)
    - 1995 SSL v.2 (Contained security flaws)
    - 1996 SSL v.3 (Complete re-write)
  - **SSL increases latency ~4x BEFORE HTTP Request**
  - **SSL is by port (443/HTTPS, 993/IMAP and 995/POP)**
  - **TLS is by protocol (Skype)**



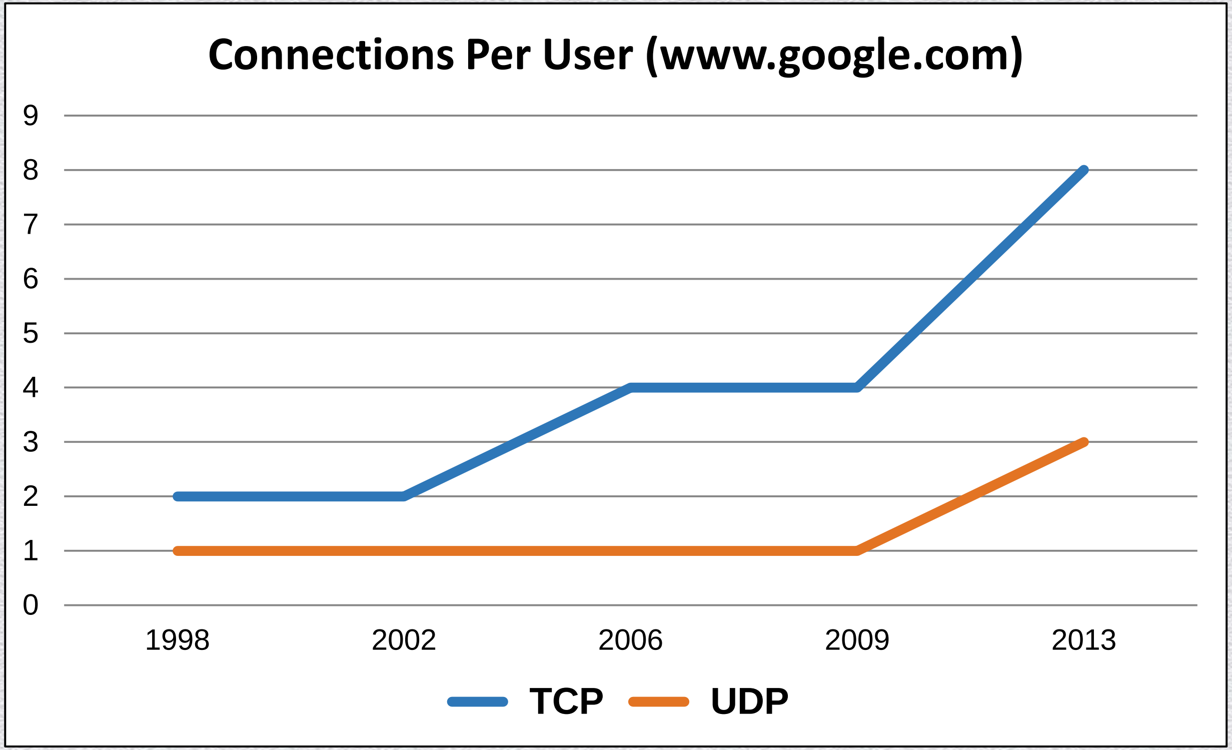
What is Driving SSL Everywhere

- The NSA ;-)
- Regulatory Compliance / Best Practices
- CA/B Forum move to distribute 2048-bit key length starting 1/1/14
- Search Engines, Social Media, Online Banking, Commerce…
- On average ~25% - ~35% of network traffic is SSL/TLS
- Recent study conducted with 200,000 websites: 91.2% using 2048-bit

Browsing History to Today

- HTTP 1.0
  - Single HTTP transaction per TCP connection
- HTTP 1.1
  - Persistent connections (a.k.a. keep-alive)
  - HTTP pipelining allowing for multiple HTTP transactions per TCP connection
- SPDY
  - Goal to reduce page load time by prioritizing and multiplexing transfers over one single connection
  - Active Push/Pull concept between client (browser) and server (application)

Browsing History to Today

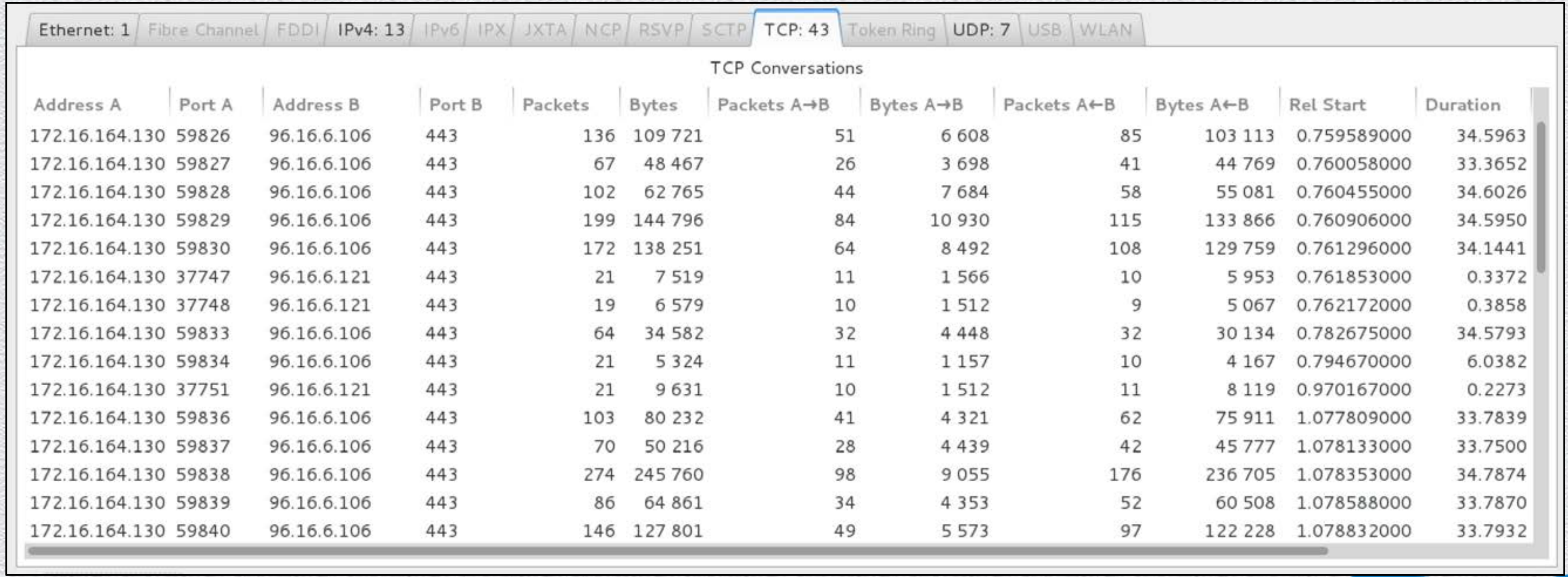


Browsing History to Today

Alexa Top Sites	TCP Conns/User	Encryption
google.com	8	✔
facebook.com	43	✔
youtube.com	23	
yahoo.com	31	✔
baidu.com	15	
wikipedia.org	12	
qq.com	161	
taobao.com	75	
live.com	22	✔
twitter.com	26	✔
linkedin.com	38	✔

Browsing History to Today

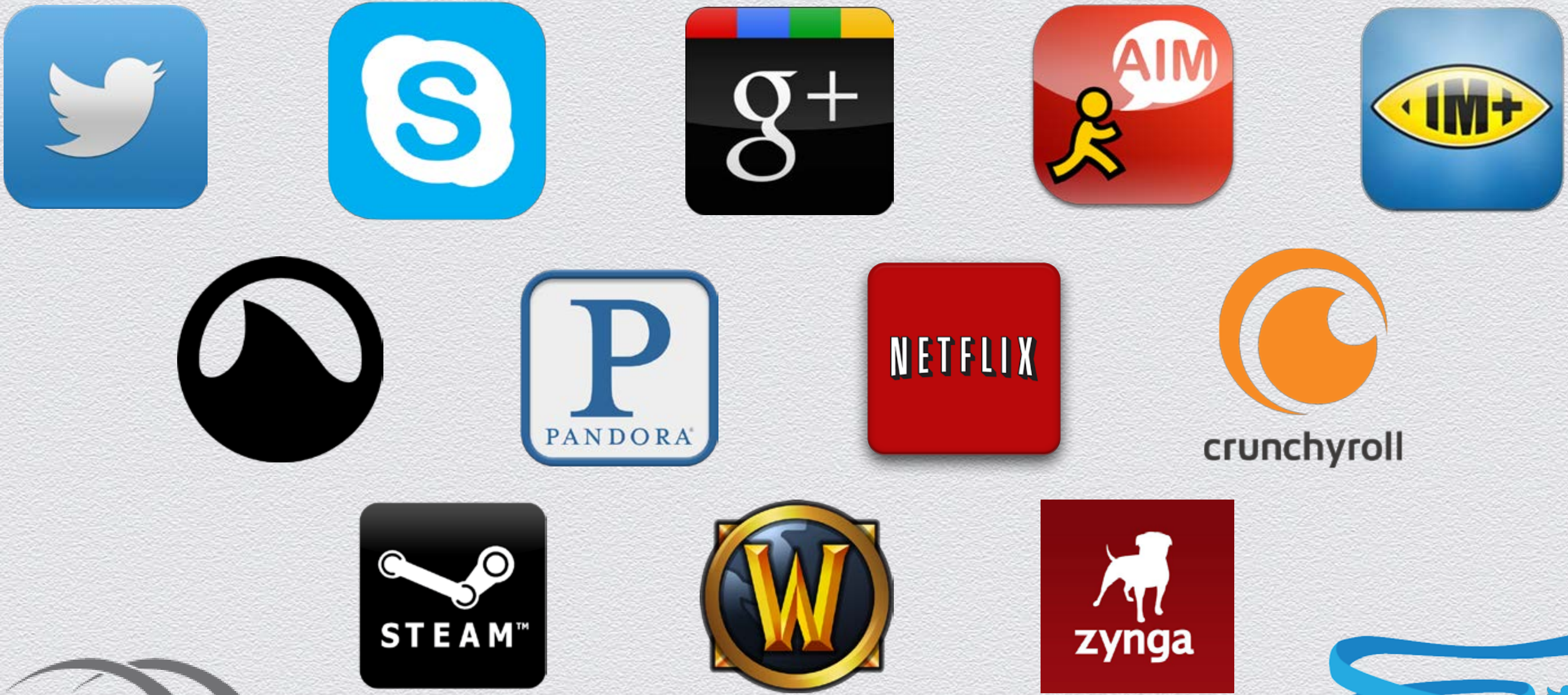
Facebook TCP Connections



TCP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration
172.16.164.130	59826	96.16.6.106	443	136	109 721	51	6 608	85	103 113	0.759589000	34.5963
172.16.164.130	59827	96.16.6.106	443	67	48 467	26	3 698	41	44 769	0.760058000	33.3652
172.16.164.130	59828	96.16.6.106	443	102	62 765	44	7 684	58	55 081	0.760455000	34.6026
172.16.164.130	59829	96.16.6.106	443	199	144 796	84	10 930	115	133 866	0.760906000	34.5950
172.16.164.130	59830	96.16.6.106	443	172	138 251	64	8 492	108	129 759	0.761296000	34.1441
172.16.164.130	37747	96.16.6.121	443	21	7 519	11	1 566	10	5 953	0.761853000	0.3372
172.16.164.130	37748	96.16.6.121	443	19	6 579	10	1 512	9	5 067	0.762172000	0.3858
172.16.164.130	59833	96.16.6.106	443	64	34 582	32	4 448	32	30 134	0.782675000	34.5793
172.16.164.130	59834	96.16.6.106	443	21	5 324	11	1 157	10	4 167	0.794670000	6.0382
172.16.164.130	37751	96.16.6.121	443	21	9 631	10	1 512	11	8 119	0.970167000	0.2273
172.16.164.130	59836	96.16.6.106	443	103	80 232	41	4 321	62	75 911	1.077809000	33.7839
172.16.164.130	59837	96.16.6.106	443	70	50 216	28	4 439	42	45 777	1.078133000	33.7500
172.16.164.130	59838	96.16.6.106	443	274	245 760	98	9 055	176	236 705	1.078353000	34.7874
172.16.164.130	59839	96.16.6.106	443	86	64 861	34	4 353	52	60 508	1.078588000	33.7870
172.16.164.130	59840	96.16.6.106	443	146	127 801	49	5 573	97	122 228	1.078832000	33.7932

Just Browsing?



Browsing History to Today

- Alexa Top Sites
  - 50% use encryption by default
  - All use multiple connections per user page request (i.e., connections/user)
- Browsing vs. other uses for SSL/TLS
  - Streaming content and "the cloud"
- Mobile
  - Adoption of BYOD
  - Growth of mobile applications

The Adversary and SSL

- Detected and Validated SSL Malware by NSS Labs Inc.
  - Accounts for ~.01% of our overall library in June 2013
  - Statistic was validated with other security research firms
  - Majority of malware using SSL is highly targeted
  - 2% Spike in SSL malware seen in January 2014 (200% increase)
- Latest SSL Malware Examples:

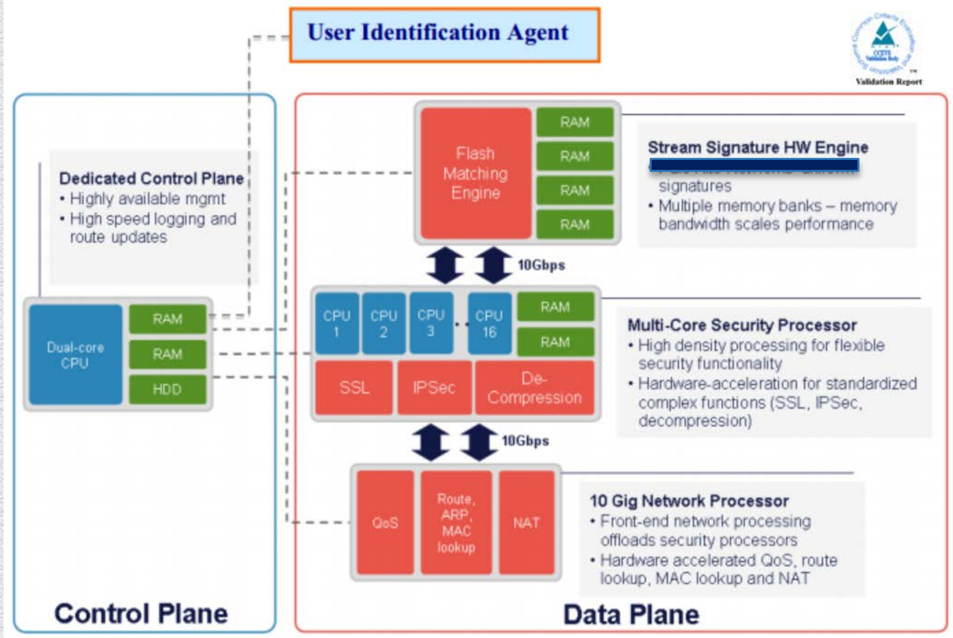
Victim IP	Remote-C&C IP	Sample Name	Port
10.254.4.80	122.55.79.88	86.exe	443
10.254.5.17	98.138.253.109	heap.exe	443
10.254.4.26	223.25.233.248	Nvsmart.exe	443

What Network Security Vendors Claim

- Datasheets
  - SSL support listed
  - Performance not covered
- Regulatory Compliance
  - PCI and its friends
- RFP process

Encryption HW Acceleration (+ I/O intensive inspection)

- Next Generation Firewalls
  - Security Effectiveness
    - Firewall Policy Enforcement
      - State / Session Tracking
    - Application Control
    - User ID / Group ID Aware
    - Intrusion Prevention
    - Resistance to Evasion
  - Performance
  - Stability and Reliability



Dedicated Control Plane
- Highly available mgmt
- High speed logging and route updates

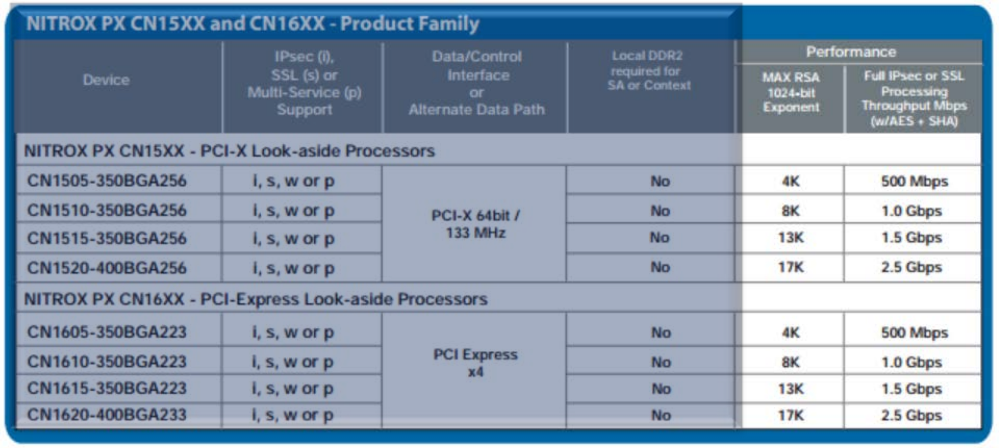
Stream Signature HW Engine
- [redacted] signatures
- Multiple memory banks – memory bandwidth scales performance

Multi-Core Security Processor
- High density processing for flexible security functionality
- Hardware-acceleration for standardized complex functions (SSL, IPSec, decompression)

10 Gig Network Processor
- Front-end network processing offloads security processors
- Hardware accelerated QoS, route lookup, MAC lookup and NAT

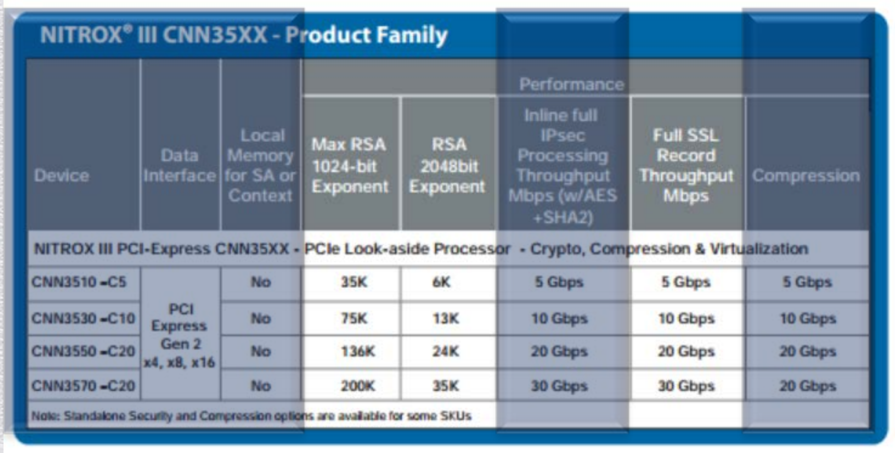
http://www.commoncriteriaportal.org/files/epfiles/[redacted]pdf

Encryption HW Acceleration (+ I/O intensive inspection)



NITROX PX CN15XX and CN16XX - Product Family

Device	IPsec (i), SSL (s) or Multi-Service (p) Support	Data/Control Interface or Alternate Data Path	Local DDR2 required for SA or Context	Performance	
				MAX RSA 1024-bit Exponent	Full IPsec or SSL Processing Throughput Mbps (w/AES + SHA)
NITROX PX CN15XX - PCI-X Look-aside Processors					
CN1505-350BGA256	i, s, w or p	PCI-X 64bit / 133 MHz	No	4K	500 Mbps
CN1510-350BGA256	i, s, w or p		No	8K	1.0 Gbps
CN1515-350BGA256	i, s, w or p		No	13K	1.5 Gbps
CN1520-400BGA256	i, s, w or p		No	17K	2.5 Gbps
NITROX PX CN16XX - PCI-Express Look-aside Processors					
CN1605-350BGA223	i, s, w or p	PCI Express x4	No	4K	500 Mbps
CN1610-350BGA223	i, s, w or p		No	8K	1.0 Gbps
CN1615-350BGA223	i, s, w or p		No	13K	1.5 Gbps
CN1620-400BGA233	i, s, w or p		No	17K	2.5 Gbps



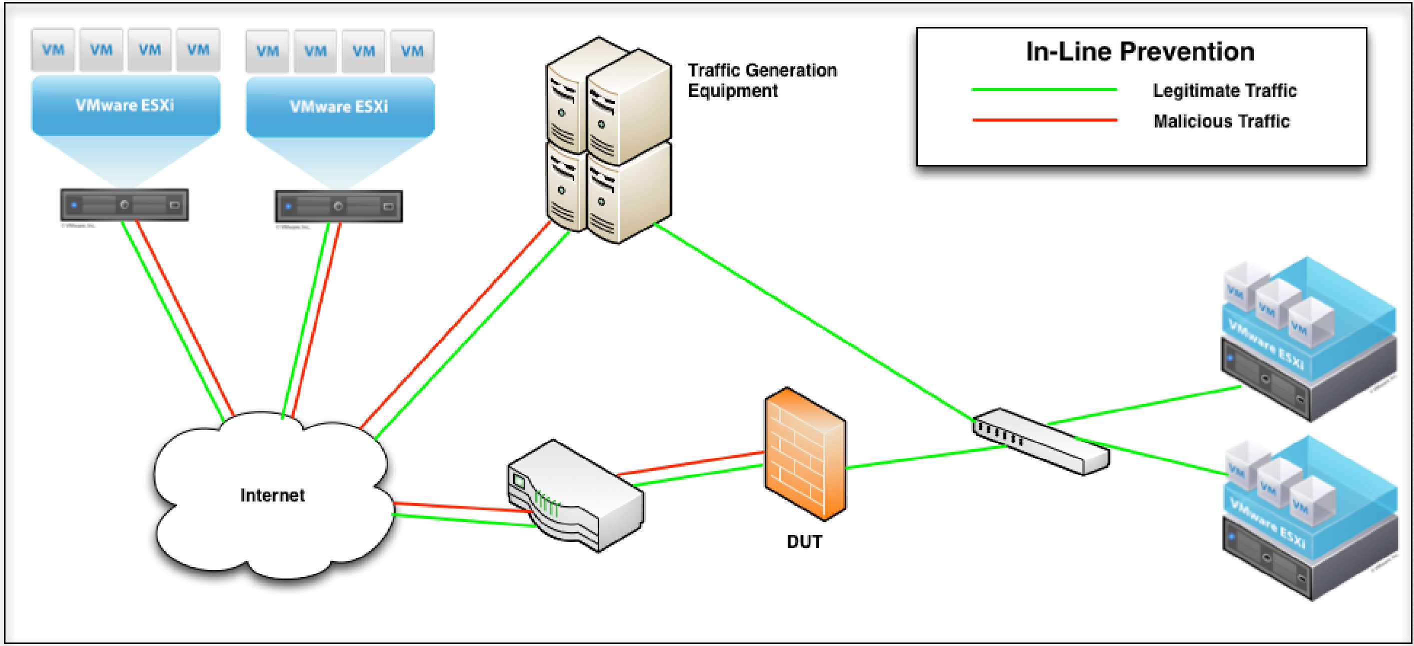
NITROX® III CNN35XX - Product Family

Device	Data Interface	Local Memory for SA or Context	Performance				
			Max RSA 1024-bit Exponent	RSA 2048bit Exponent	Inline full IPsec Processing Throughput Mbps (w/AES +SHA2)	Full SSL Record Throughput Mbps	Compression
NITROX III PCI-Express CNN35XX - PCIe Look-aside Processor - Crypto, Compression & Virtualization							
CNN3510 -C5	PCI Express Gen 2 x4, x8, x16	No	35K	6K	5 Gbps	5 Gbps	5 Gbps
CNN3530 -C10		No	75K	13K	10 Gbps	10 Gbps	10 Gbps
CNN3550 -C20		No	136K	24K	20 Gbps	20 Gbps	20 Gbps
CNN3570 -C20		No	200K	35K	30 Gbps	30 Gbps	20 Gbps

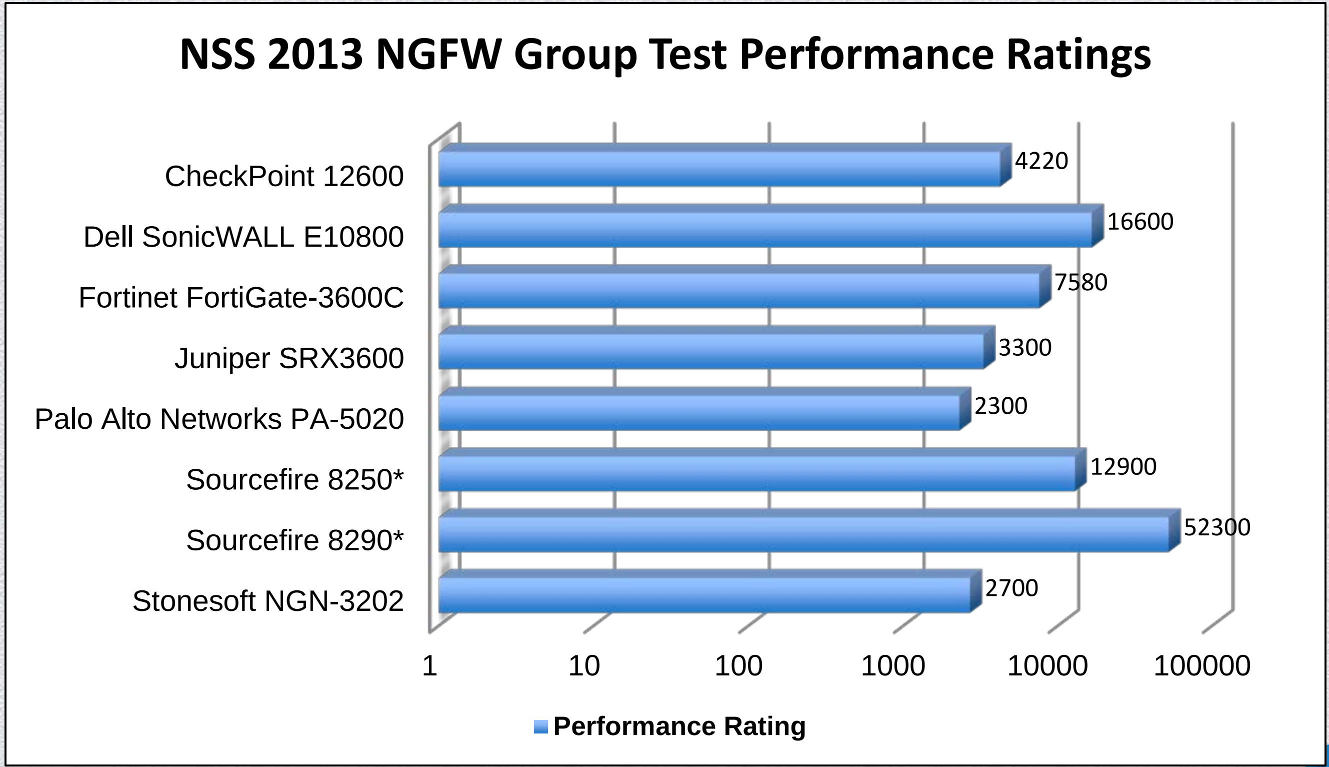
Note: Standalone Security and Compression options are available for some SKUs

NGFW / SSL Performance Results

Test Environment Architecture

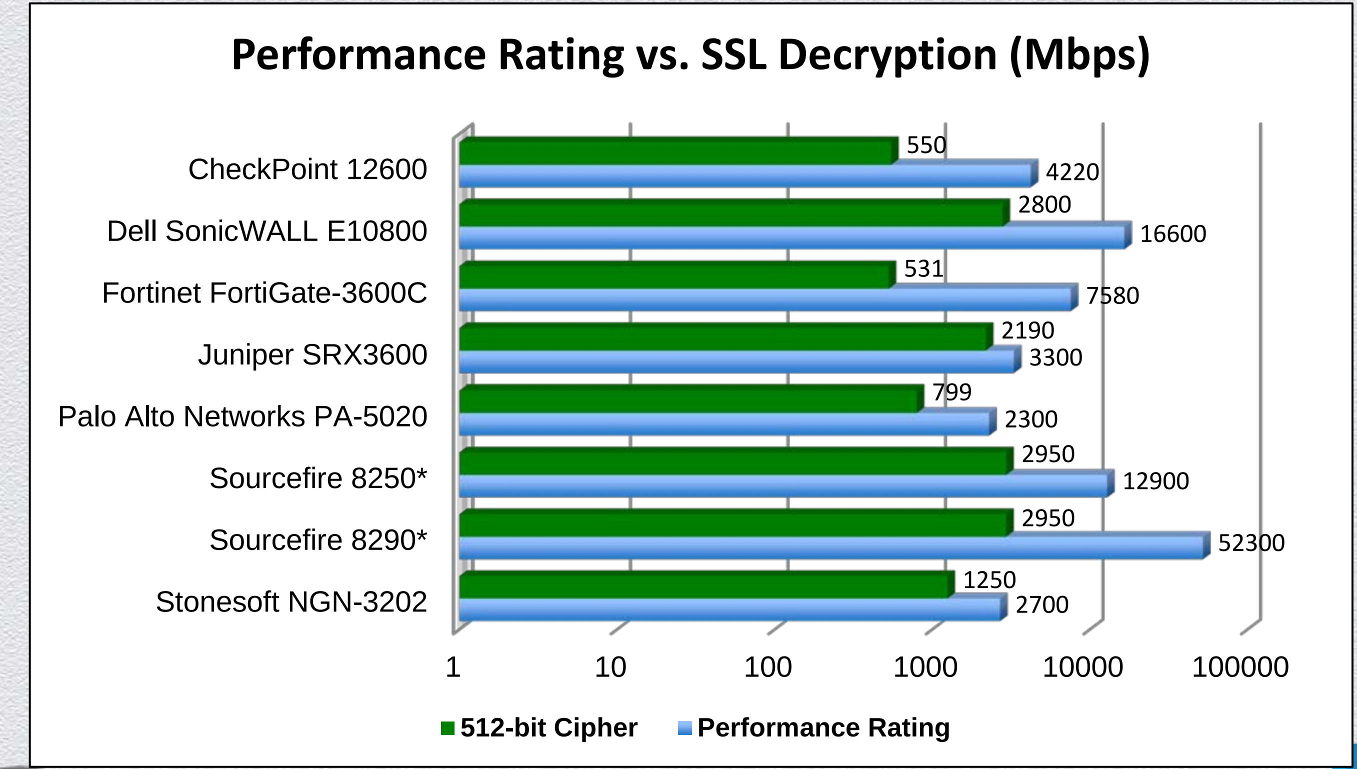


NGFW / SSL Performance Results


NSS 2013 NGFW Group Test Performance Ratings

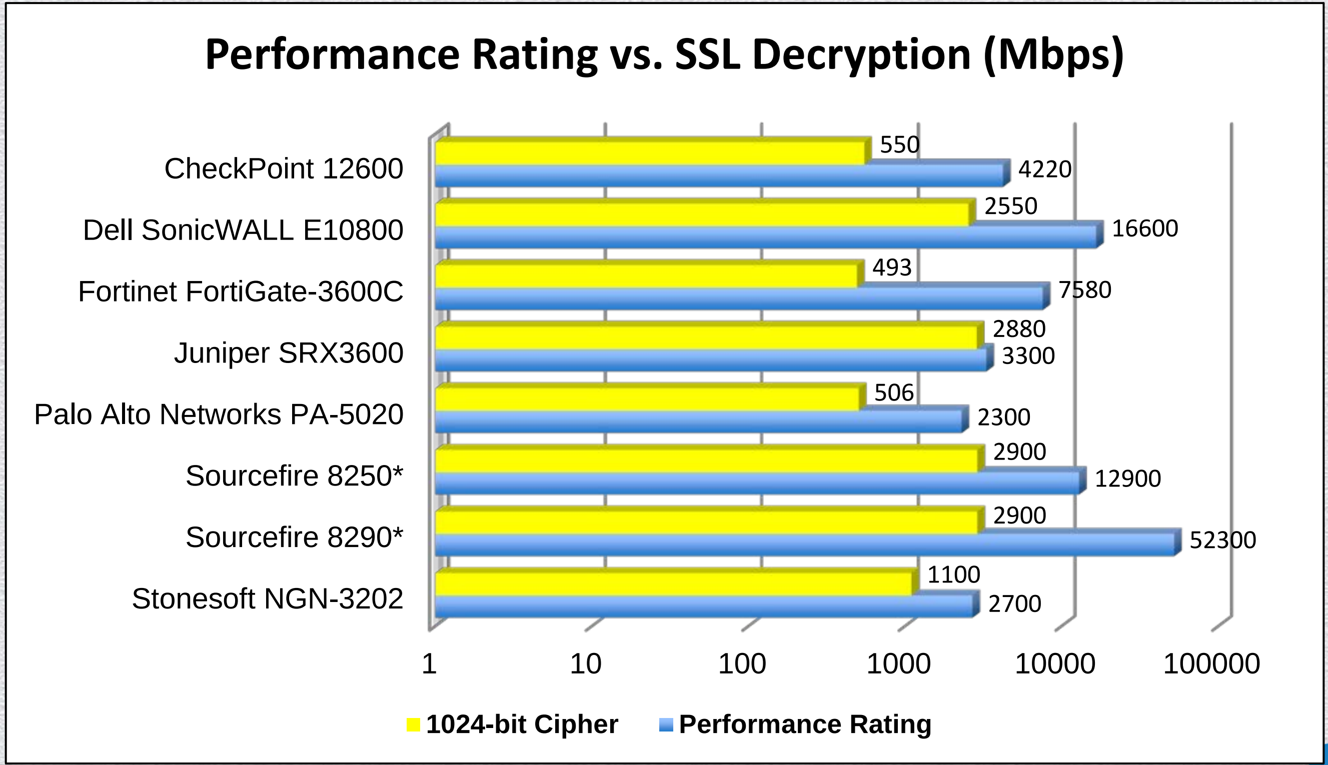
* Used Netronome SSL Offloading

NGFW / SSL Performance Results



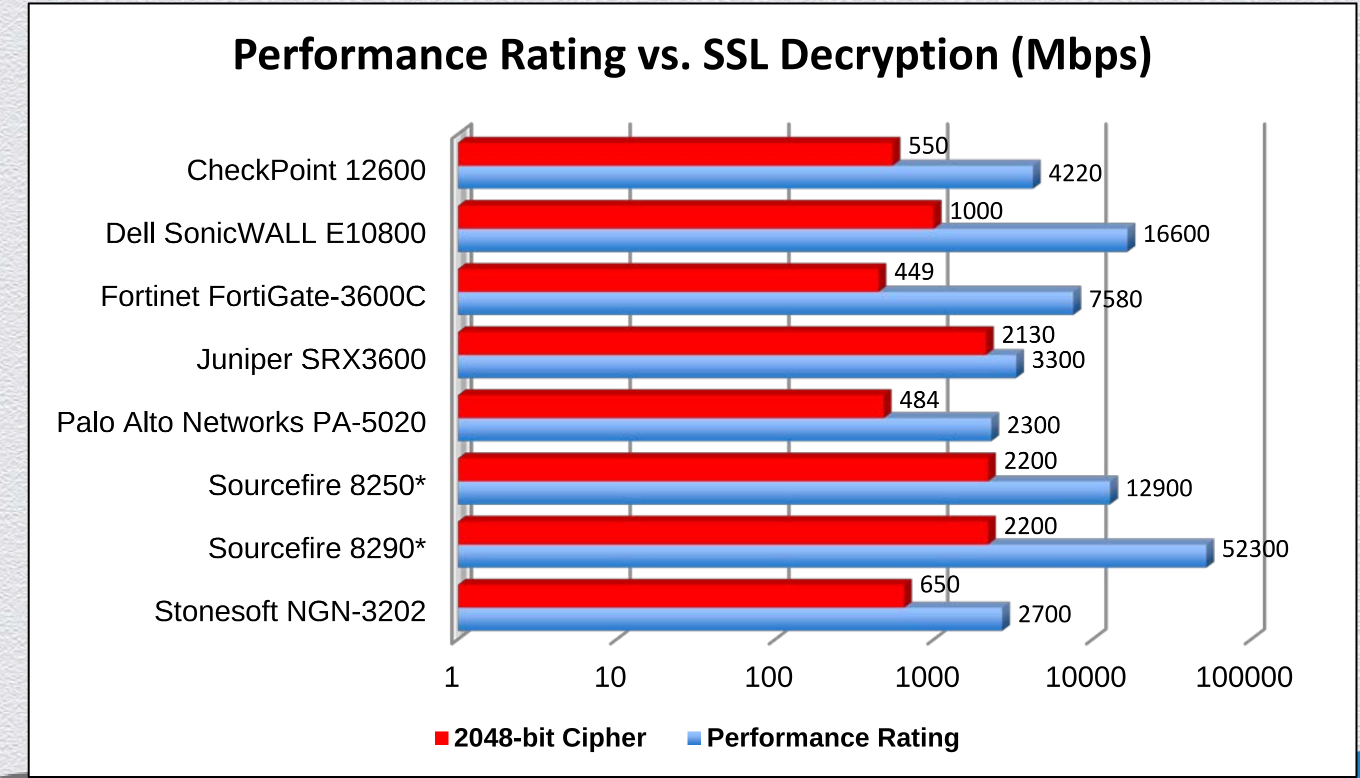
* Used Netronome SSL Offloading

NGFW / SSL Performance Results



* Used Netronome SSL Offloading

NGFW / SSL Performance Results



* Used Netronome SSL Offloading

NGFW / SSL Performance Results

Maximum Throughput Results

		512-bit Cipher		1024-bit Cipher		2048-bit Cipher	
Vendor	**Performance Rating (Mbps)**	**Throughput (Mbps)**	**% Loss**	**Throughput (Mbps)**	**% Loss**	**Throughput (Mbps)**	**% Loss**
Check Point 12600	4,220	550	87%	550	87%	550	87%
Dell SonicWall E10800	16,600	2,800	83%	2,550	85%	1000	94%
Fortinet FortiGate-3600C	7,580	531	93%	493	93%	449	94%
Juniper SRX3600	3,300	2,190	34%	2,880	13%	2,130	35%
Palo Alto Networks PA-5020	2,300	799	65%	506	78%	484	79%
Sourcefire 8250*	12,900	2,950	77%	2,900	78%	2,200	83%
Sourcefire 8290*	52,300	2,950	94%	2,900	94%	2,200	96%
Stonesoft NGN-3202	2,700	1,250	54%	1,100	59%	650	76%

* Used Netronome SSL Offloading

NGFW / SSL Performance Results

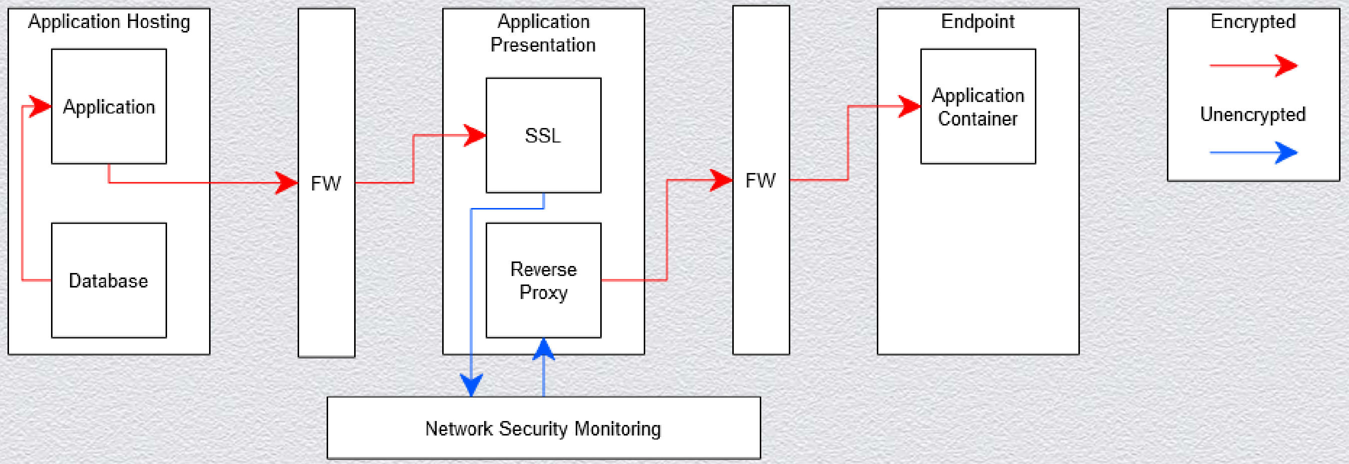
Maximum Connections Per Second Results

		512-bit Cipher		1024-bit Cipher		2048-bit Cipher	
Vendor	Connections/Second Rating	Connections/Sec	% Loss	Connections/Sec	% Loss	Connections/Sec	% Loss
Check Point 12600	53,000	1,500	97.17%	1,500	97.17%	1,500	97.17%
Dell SonicWall E10800	220,000	1,500	93.18%	12,200	94.45%	2600	98.82%
Fortinet FortiGate-3600C	78,000	1,515	98.06%	1,424	98.17%	1,294	98.34%
Juniper SRX3600	39,000	8,400	78.46%	8,400	78.46%	8,000	79.49%
Palo Alto Networks PA-5020	17,119	5,098	70.22%	4,662	72.77%	3,767	78%
Sourcefire 8250*	114,000	18,000	84.21%	17,800	84.39%	6,800	94.04%
Sourcefire 8290*	432,145	1,800	95.83%	17,800	95.88%	6,800	98.43%
Stonesoft NGN-3202	33,000	7,500	77.27%	6,250	81.06%	2,000	93.94%

* Used Netronome SSL Offloading

Recommendation

Conceptual Recommendation



Key Takeaways

- Fundamental difference between SSL and TLS
- Per user connections are on the rise
- The adversary is now using SSL too (200% increase in 6 months)
- Time to protection vs. time to market
- Embedded encryption acceleration (i.e., NGFW) **“should be”** examined carefully
- Offloading of SSL inspection **“may render”** better performance

Thank You