2017

Reference Test Report PA-5220 SSL Decryption 2K Key

Proof of Concept

Palo Alto Networks

3/6/2017

Executive Summary

This document will outline a test plan that will serve to confirm that the vendor platform-based threat prevention solution satisfies the requirements of the customer to provide advanced Cybersecurity protection for the firm's network and application infrastructure. Successful completion of this test plan implies that the reviewers are comfortable that the products tested have satisfied the firm's stated acceptance criteria.

1. Overview

The Goal of the POC is to use a snapshot of a customer's traffic profile and show the performance when applied to a PA-5220 platform.

A proof of concept (POC) test is used to ensure that new technologies under consideration will work as expected and related to the technologies or products under test. This document outlines high-level POC requirements.

2. Topology Setup

The NGFW devices to be tested will incorporate, at a minimum, an Application Identification component (Layer 7) and potentially enabling multiple advanced features such as AV, Vulnerability Protection, Wildfire, etc.
The test environment will be setup in the following manner and will apply for all test scenarios defined below:

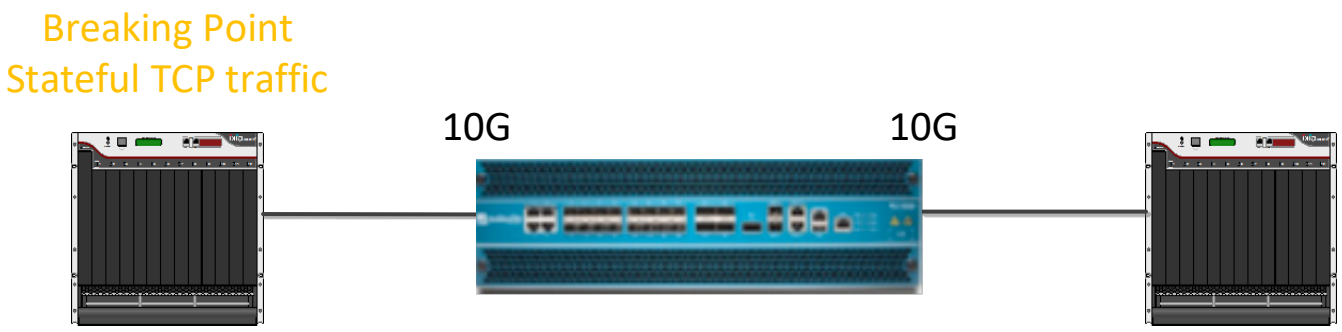


Figure-1 PA-5220 Next Generation Standalone Firewall Network Test Diagram

IP address space will be defined after consultation with the customer. Multiple 10Gbps interfaces may be necessary in order to fully test the firewall.

3. Testing Scenarios

The following table lists test cases that will be executed against the device under test (DUT):
(a description of each test can be found under section 6. Test Scenarios Description)

Area	Test Case	Test Case Description
Application Performance	AP1	Traffic Mix 64KB – Maximum Throughput (L7) – AppID / Threat / SSL Decrypt

4. Topology Configuration

A. Test Equipment

- Hardware: Ixia Breaking Point
- Software: Version 8.13.0 ATI Update: 286052 Strike Date 2016-10-19

B. Firewall

- Hardware: PA-5220 Standalone
- Software: Version 8.0.0
- Palo Alto Networks firewall interfaces are configured in layer3 mode
- Logging is enabled at session end in all tests

C. Traffic Profile

- The content type of HTTP message header is set to “Get (SSL)”.
- TLS v1.2, AES-128-SHA1 cipher is used for SSL Decryption.
- Transaction size (64KB) is used for HTTPS, HTTP, SMTP, and SSH.
- RSA Key with 2048 bit key length is used for SSL Decryption.

Traffic Mix	Percentage	Transaction Size
HTTPS/SSL (TCP/443) • 2048 RSA key size • TLS v1.2, AES-128-SHA1	50%	64k
HTTP (TCP/80)	40%	64k
Enterprise Mix • SMTP (TCP/25) (4%) • SSH (TCP/22) (4%)	8%	64k
DNS (TCP/UDP/53)	2%	255byte

5. Test Results

The Ixia Breaking Point System generates reports for every test case executed. POC will export copies of all relevant test cases executed using the Adobe PDF format.

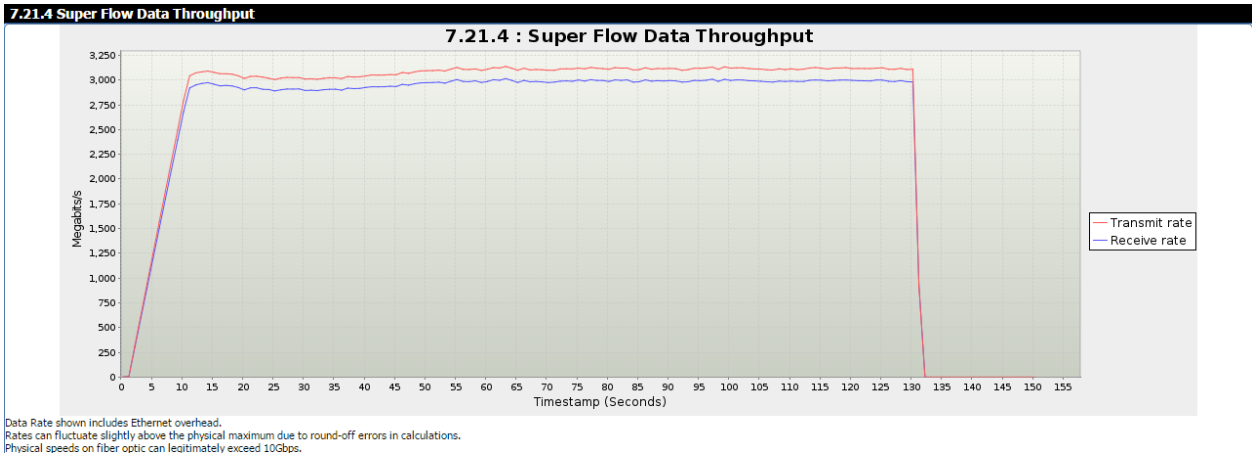
6. Test Scenarios Description

Unless explicitly stated, the firewall will be configured for Application Identification (App-ID) and not just layer4 port based firewalling.

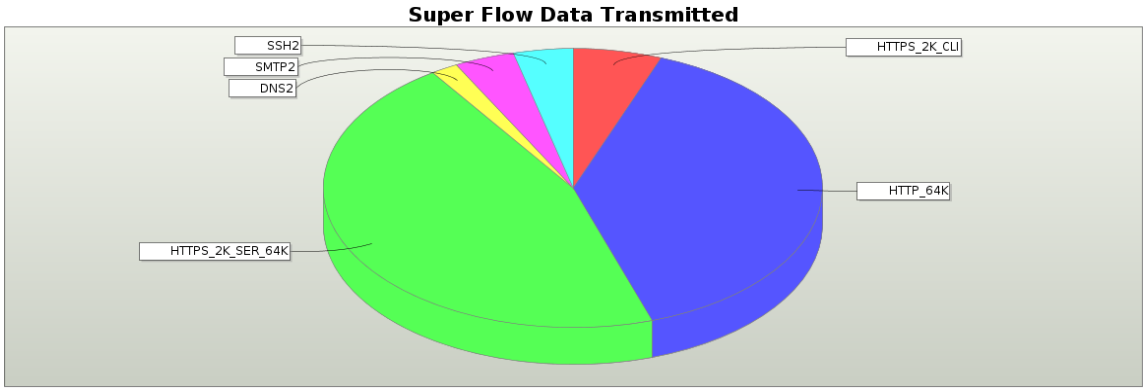
The following details all test scenarios:

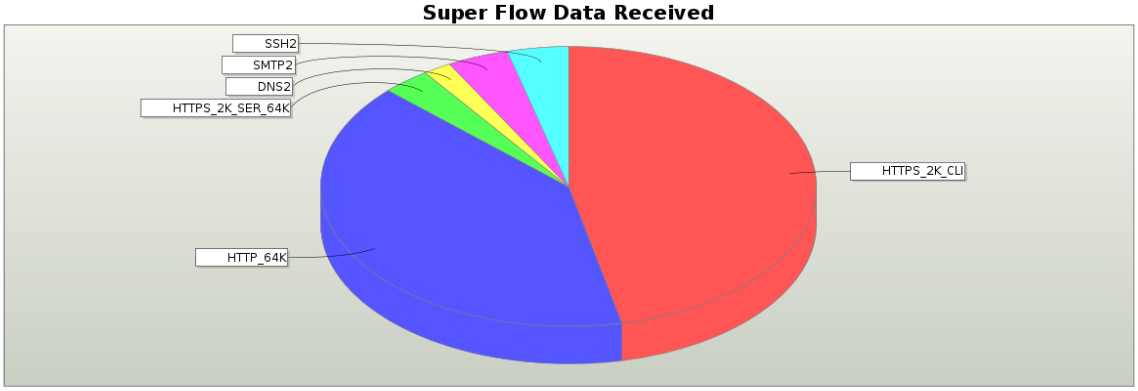
Test Case ID	AP1
Test Description	Traffic Mix 64KB – Maximum Throughput (L7) – AppID / Threat / SSL Decrypt
Purpose	Determine Maximum Throughput with AppID / Threat / SSL Decrypt
Objective	This test case will evaluate the ability of the firewall to establish and maintain maximum throughput using 64KB transaction size with AppID, Threat protection, and SSL Decrypt. The test will use an Application Simulator with an App Profile that has HTTP, HTTPS, SMTP, SSH, and DNS. The Firewall should let the application data through and identify each application. Traffic will run at the highest throughput the Firewall supports with App-ID, AV, Vulnerability, Anti-Spyware, URL Filtering turned on, and no DSRI.
Comments	Able to achieve 3 Gbps of throughput with AppID, Threat protection, and SSL Decrypt.
Metrics	Max Throughput

Overall Throughput at 3 Gbps with 64KB transaction size, AppID, Threat protection, and SSL Decrypt.



Traffic Mix	Percentage	Transaction Size
HTTPS/SSL (TCP/443) • 2048 RSA key size	50%	64k
HTTP (TCP/80)	40%	64k
Enterprise Mix • SMTP (TCP/25) (4%) • SSH (TCP/22) (4%)	8%	64k
DNS (TCP/UDP/53)	2%	255byte





There may be slices in this graph that are too small to be displayed.

Super Flow	Data Transmitted (Bytes)	Data Transmitted (%)	Data Received (Bytes)	Data Received (%)	Delta Received (Tx - Rx) (Bytes)	% Received (%)
HTTPS_2K_CLI	2,680,978,865	5.752%	20,942,399,436	46.539%	-18,261,420,571	781.148
HTTP_64K	18,234,917,960	39.125%	18,234,917,960	40.522%	0	100
HTTPS_2K_SER_64K	21,280,379,141	45.660%	1,412,544,247	3.139%	19,867,834,894	6.638
DNS2	817,534,575	1.754%	817,511,087	1.817%	23,488	99.997
SMTP2	1,798,386,484	3.859%	1,798,342,060	3.996%	44,424	99.998
SSH2	1,794,339,524	3.850%	1,794,339,524	3.987%	0	100

Minimal errors noticed during the test.

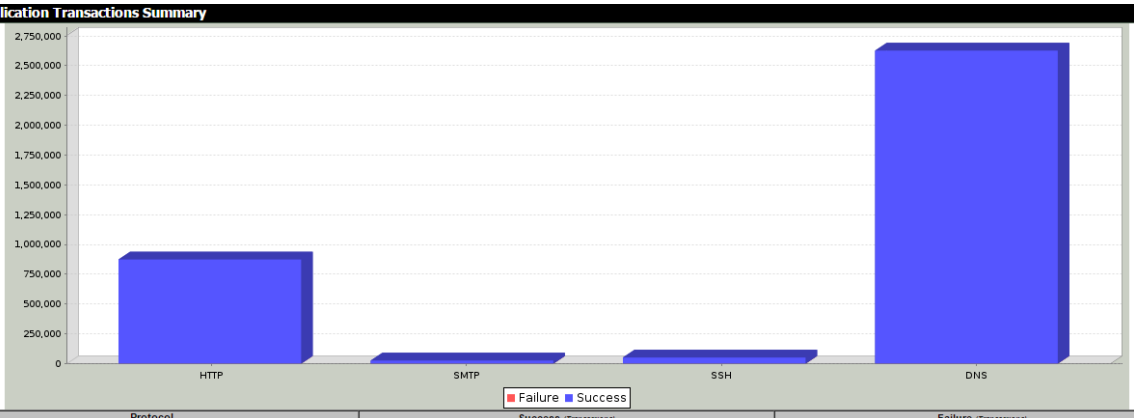
7.7 Application Summary

Measurement	Value
Frames transmitted	81,806,254
Frames received	67,776,680 82.850%
Frame data transmitted	44,643,186,453
Frame data received	43,373,413,994 97.156%
Attempted	3,662,502
Successes	3,662,498 100.000%
Failures due to ramp down	3 0.000%
Failures due to external events	1 0.000%
Failures due to TCP retry limit	0
Failures due to UDP receive timeout	1 0.000%
Failures due to resolve receive timeout	0
Failures due to a premature session close	0
Failures due to a premature Super Flow close	0
General application failures	0
Attempted matches	0
Successful matches	0
Failed matches	0
Conditional Request chunk starts	0
Conditional Request chunk ends	0
Server Response data valid count	0
Server Response data not valid count	0

7.13 TCP Summary

Measurement	Value
Frames transmitted	76,427,737
Frames received	62,401,392 81.648%
Frame data transmitted	43,954,736,286
Frame data received	42,685,199,621 97.112%
Client attempted	635,077
Client established	630,452
Client closed normally	630,450
Client received FIN	630,444
Client closed by sending RST	0
Client received RST	0
Server established	630,452
Server closed normally	630,447
Server received FIN	630,447
Server closed by sending RST	0
Server received RST	0
Unknown/Closed flow received RST	0
Corrupt TCP Options	0
Invalid TCP Header Length	0
Invalid TCP Flag Combination	0
Aggregate open retries	68,698
Aggregate data retries	28
Aggregate close retries	6
Aggregate closed normally	1,260,897
Aggregate closed by sending RST	0

7.6 Application Transactions Summary



Protocol	Success (Transactions)	Failure (Transactions)
HTTP	894,714	0
SMTP	26,174	0
SSH	52,352	0
DNS	2,689,258	1

TLS v1.2 used for SSL Decrypt in BPS

7.15 SSL Summary

Measurement	Value
Encrypted data (bytes)	18,804,398,080
Decrypted data (bytes)	18,804,201,872
Handshakes started	633,230
Handshakes timed out	0
Handshakes finished	633,230
Handshakes finished: SSLv3 Resumed	0
Handshakes finished: SSLv3 NonResumed	0
Handshakes finished: TLSv1 Resumed	0
Handshakes finished: TLSv1 NonResumed	0
Handshakes finished: TLSv1.1 Resumed	0
Handshakes finished: TLSv1.1 NonResumed	0
Handshakes finished: TLSv1.2 Resumed	633,200
Handshakes finished: TLSv1.2 NonResumed	30
Handshakes aborted	0
Handshakes aborted: by client	0
Handshakes aborted: by server	0

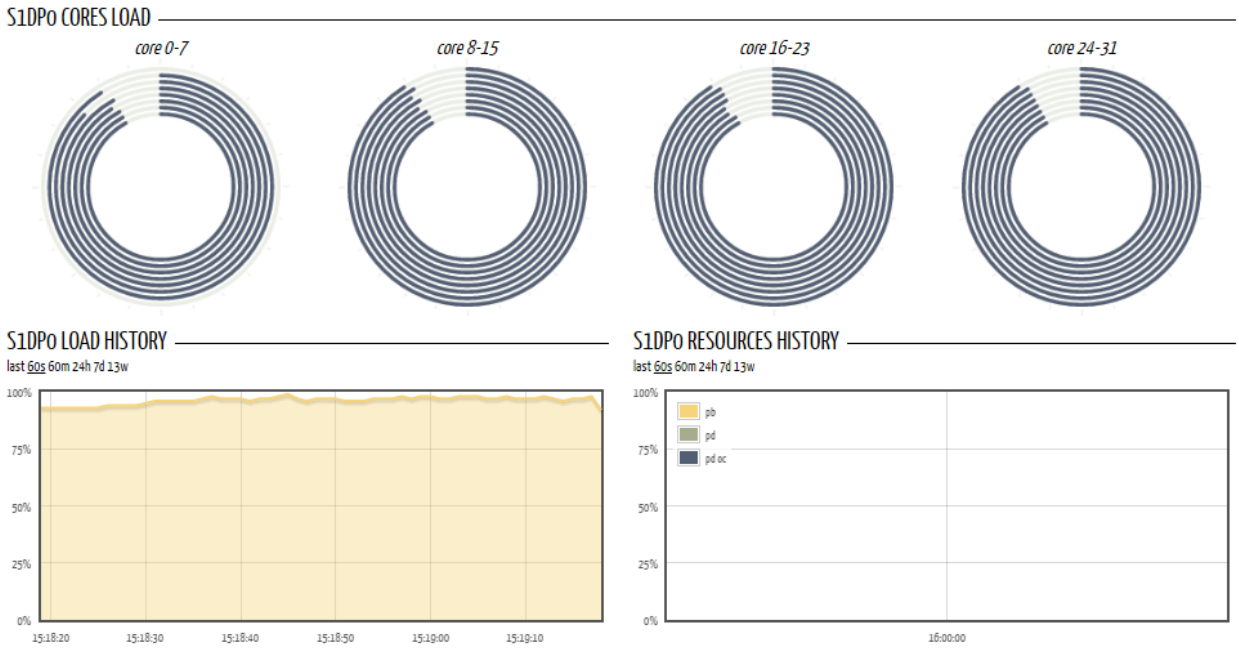
SSL Decrypt Stats – Verifying we are using TLS 1.2 and RSA, AES-128, SHA

```
admin@PA-5220-14> debug dataplane show ssl-decrypt ssl-stats

SSL Protocol Version Stats
TLS1.2                  From Client: 5891348
TLS1.2                  From Server: 5853464

SSL Cipher Suite Stats
TLS_RSA_WITH_AES_128_CBC_SHA        From Client: 5891348
TLS_RSA_WITH_AES_128_CBC_SHA        From Server: 5853464

SSL Session Resume Stats
Not Resumed             From Client: 706
Not Resumed             From Server: 11520
Resumed Locally         From Client: 5877136
Resumed Locally         From Server: 5841944
Resume request to MP    From Client: 13506
Resume request to MP    From Server: 0
Resumed Failed from MP  From Client: 13506
Resumed Failed from MP  From Server: 13506
```

Confirming we are using 2K key

```
admin@PA-5220-14> show system setting ssl-decrypt certificate

Certificates for Global

SSL Decryption CERT

global trusted
ssl-decryption x509 certificate
version 2
cert algorithm 4
valid 170216023356Z -- 180216023356Z
cert pki 1
subject: paloaltonetworks.com
issuer: paloaltonetworks.com
serial number(9)
00 aa 97 9a d0 67 ae 44  b9                    .....g.D .
rsa key size 2048 bits siglen 256 bytes
basic constraints extension CA 1
also serves as untrusted certificate

NO INBOUND CERT
```

Screenshots of CPU during the test. CPU is close to 100%.



Traffic log from the firewall during the test.

Receive Time	Type	From Zone	To Zone	Source	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	Decrypted
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.9	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.7k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.1	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.7k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.9	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.7	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.5	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.5	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.3	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.8	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.7	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.1	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.9	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.5	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.10	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.9	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.5	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.1	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.4	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.10	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.7	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes
03/06 15:18:48	end	Trust-L3	Untrust-L3	100.1.1.4	200.1.1.1	443	web-browsing	allow	Allow ALL TP	tcp-fin	71.4k	yes

Following Decryption Policy used.

			Source			Destination						
	Name	Tags	Zone	Address	User	Zone	Address	URL Category	Service	Action	Type	Decryption Profile
1	decrypt	none	any	any	any	any	any	any	any	decrypt	ssl-forward-proxy	decrypt

		SSL Forward Proxy			SSL Inbound Inspection		SSL Protocol Settings			
Name	Location	Server Certificate Verification	Unsupported Mode Checks	Failure Checks	Unsupported Mode Checks	Failure Checks	Key Exchange Algorithms	Protocol Versions	Encryption Algorithms	Authentication Algorithms
default	Predefined						RSA DHE ECDHE	Min Version: TLSv1.0 Max Version: Max	3DES RC4 AES128-CBC AES256-CBC AES128-GCM AES256-GCM	SHA1 SHA256 SHA384
decrypt							RSA	Min Version: TLSv1.2 Max Version: TLSv1.2	AES128-CBC AES256-CBC AES128-GCM AES256-GCM	SHA1 SHA256 SHA384

Following Security Policy used.

			Source				Destination						
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
Allow ALL APPID	*none*	*universal*	*any*	*any*	*any*	*any*	*any*	*any*	*any*	*any*	*Allow*	*none*	
Allow ALL TP	none	universal	any	any	any	any	any	any	any	any	Allow		
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	

Confirming we are not using DSRI.