2017

Internet Traffic Blend Report PA-5220

Proof of Concept

Palo Alto Networks

4/5/2017

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:

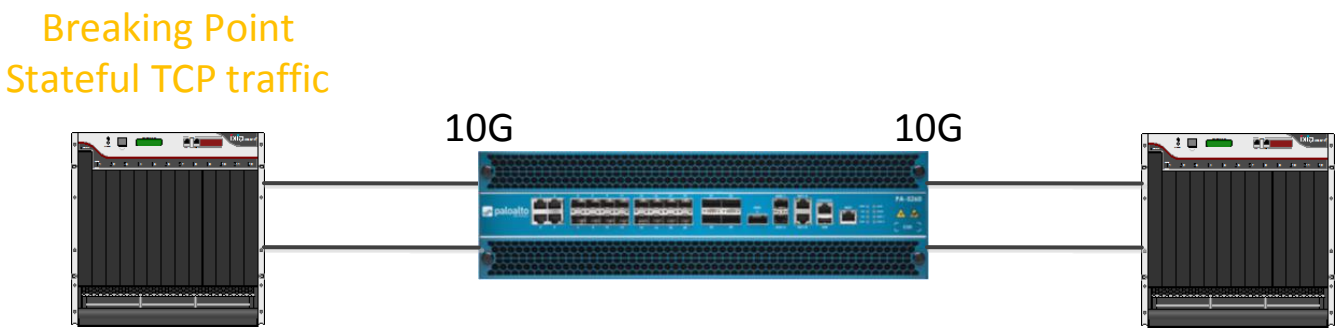


Figure-1 PA-5220 Next Generation Standalone Firewall Network Test Diagram

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	Internet Traffic Mix – Maximum Throughput (L7) – AppID / Threat Prevention

4. Topology Configuration

A. Test Equipment

- Hardware: Ixia Breaking Point
- Software: Version 8.13.0 ATI Update: 302252 Strike Date 2017-03-24

B. Firewall

- Hardware: PA-5220 Standalone
- Software: Version 8.0.1
- Palo Alto Networks firewall interfaces are configured in layer3 mode
- Logging is enabled at session start and session end in all tests

C. Traffic Profile

- The following Internet Traffic Mix was used for performance testing.

Internet Traffic Blend

Protocol	Content	Action	Per Cent
HTTP	Amazon Home Page	HTTP GET -> 676K	16%
	Yahoo Home Page	HTTP GET -> 292K	16%
	Facebook Home Page	HTTP GET -> 271K	16%
	Google Home Page	HTTP GET -> 41K	17%
	Google Mail	HTTP GET of Gmail index.html file, 21K	2%
	HTTP Post	100K PDF File	1%
SMTP	SMTP 17K	MIME Message with PDF attachment	7%
	SMTP 100K	MIME Message with Word attachment	6%
HTTPS	HTTPS 10K	HTTPS GET of 10K file	5%
	HTTPS 100K	HTTPS GET of 100K file	5%
Other	DNS	DNS Query	6%
	POP3	Message size: 256-512 bytes	1%
	Telnet	Login; cd /disk/images; ls	1%
	FTP	FTP GET, 1MB file	1%

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

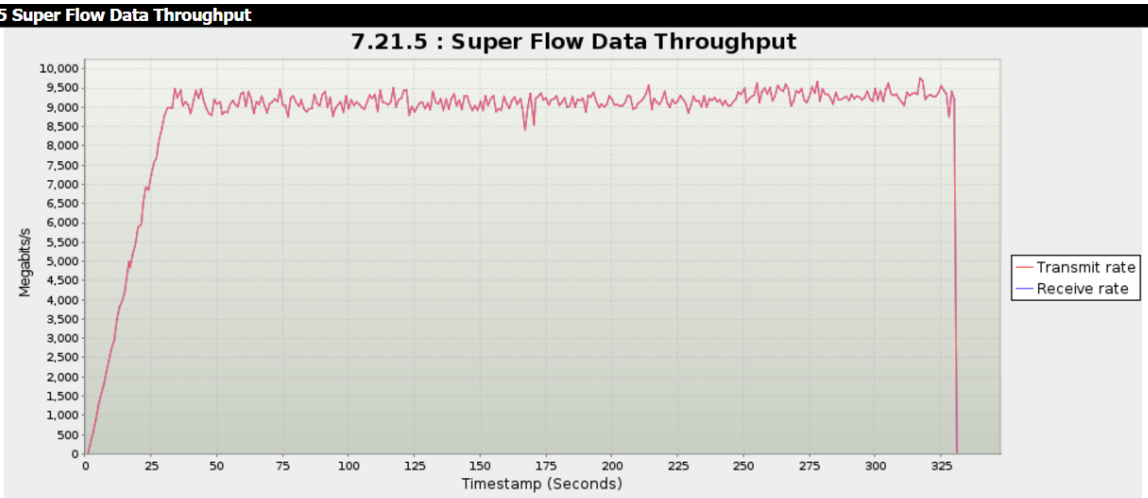
Unless explicitly stated, the firewall will be configured for Application Identification (App-ID) and not just layer4 port based firewalling.

The following details all test scenarios:

Test Case ID	AP1
Test Description	Internet Traffic Mix – Maximum Throughput (L7) – AppID / Threat Prevention
Purpose	Determine Maximum Throughput (L7) with AppID & Threat Prevention
Objective	This test case will evaluate the ability of the firewall to establish and maintain maximum throughput using Internet traffic mix with AppID and Threat Prevention enabled. Traffic will run at the highest throughput the Firewall supports with App-ID, Anti-Virus, Anti-Spyware, Vulnerability Protection, URL Filtering, File Blocking, and Wildfire turned on, and no DSRI.
Comments	Able to achieve 9 Gbps of throughput with AppID and Threat Prevention.
Metrics	Max Throughput

Overall Throughput ~ 9 Gbps with AppID and Threat Prevention.

7.21.5 Super Flow Data Throughput



Data Rate shown includes Ethernet overhead.
Rates can fluctuate slightly above the physical maximum due to round-off errors in calculations.
Physical speeds on fiber optic can legitimately exceed 10Gbps.

Traffic mix percentage

Super Flow	Iterations *(Iteration)*	Iterations *(%)*
Telnet Login	15,247	1.010%
SMTP 17K MIME Message with PDF	106,792	7.074%
HTTP Post 100K PDF File	15,140	1.003%
Facebook Home Page 271K	244,786	16.215%
Google Home Page HTTP GET - 41K	258,710	17.138%
Yahoo Home Page HTTP GET - 292K	243,552	16.133%
FTP GET 1MB file	14,921	0.988%
POP3 Message size: 256-512 bytes	15,213	1.008%
BreakingPoint DNS	92,072	6.099%
HTTPS 10K GET of 10K file	75,415	4.996%
Google Mail HTTP GET 21K	30,234	2.003%
SMTP 100K MIME Message with PDF	78,267	5.185%
HTTPS 100K GET of 100K file	76,304	5.055%
Amazon Home Page HTTP GET - 676K	242,952	16.094%

Minimal errors noticed during the test.

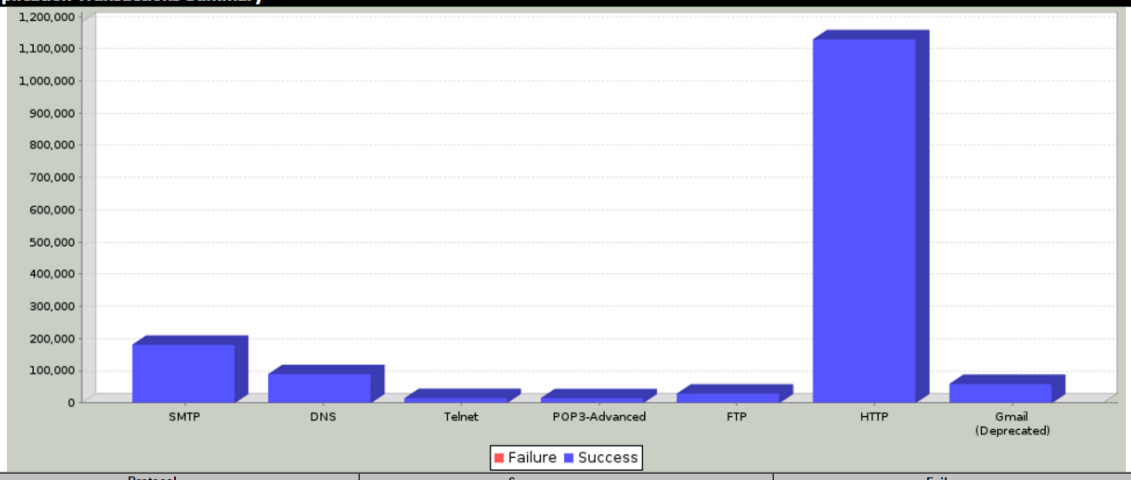
7.7 Application Summary

Measurement	Value
Frames transmitted	276,153,330
Frames received	276,153,277 *100.000%*
Frame data transmitted	348,625,337,921
Frame data received	348,625,294,225 *100.000%*
Attempted	1,554,760
Successes	1,554,757 *100.000%*
Failures due to ramp down	3 *0.000%*
Failures due to external events	0
Failures due to TCP retry limit	0
Failures due to UDP receive timeout	0
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	15,213
Successful matches	15,213
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

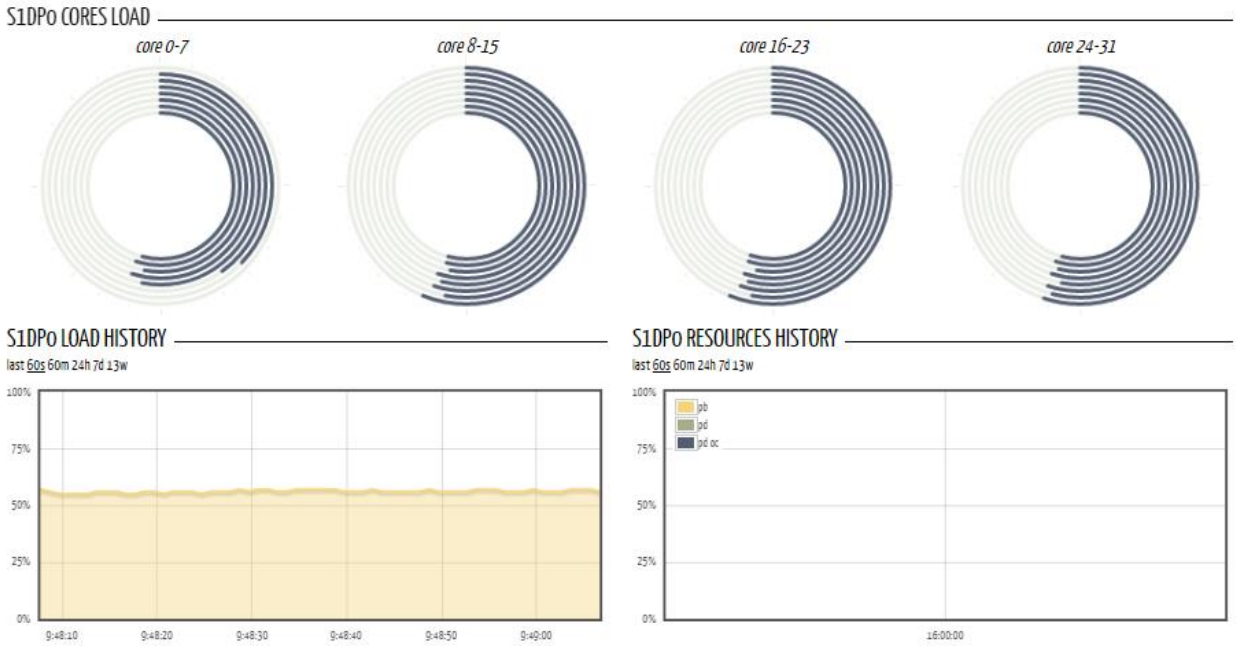
Measurement	Value
Frames transmitted	275,969,186
Frames received	275,969,141 *100.000%*
Frame data transmitted	348,601,767,489
Frame data received	348,601,724,605 *100.000%*
Client attempted	1,432,454
Client established	1,432,454
Client closed normally	1,432,451
Client received FIN	1,432,452
Client closed by sending RST	0
Client received RST	0
Server established	1,432,454
Server closed normally	1,432,451
Server received FIN	1,432,452
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	0
Aggregate data retries	21
Aggregate close retries	2
Aggregate closed normally	2,864,902
Aggregate closed by sending RST	0

7.6 Application Transactions Summary



Protocol	Success *(Transactions)*	Failure *(Transactions)*
SMTP	185,057	0
DNS	92,072	0
Telnet	15,247	0
POP3-Advanced	15,212	0
FTP	29,842	0
HTTP	1,156,859	0
Gmail (Deprecated)	60,468	0

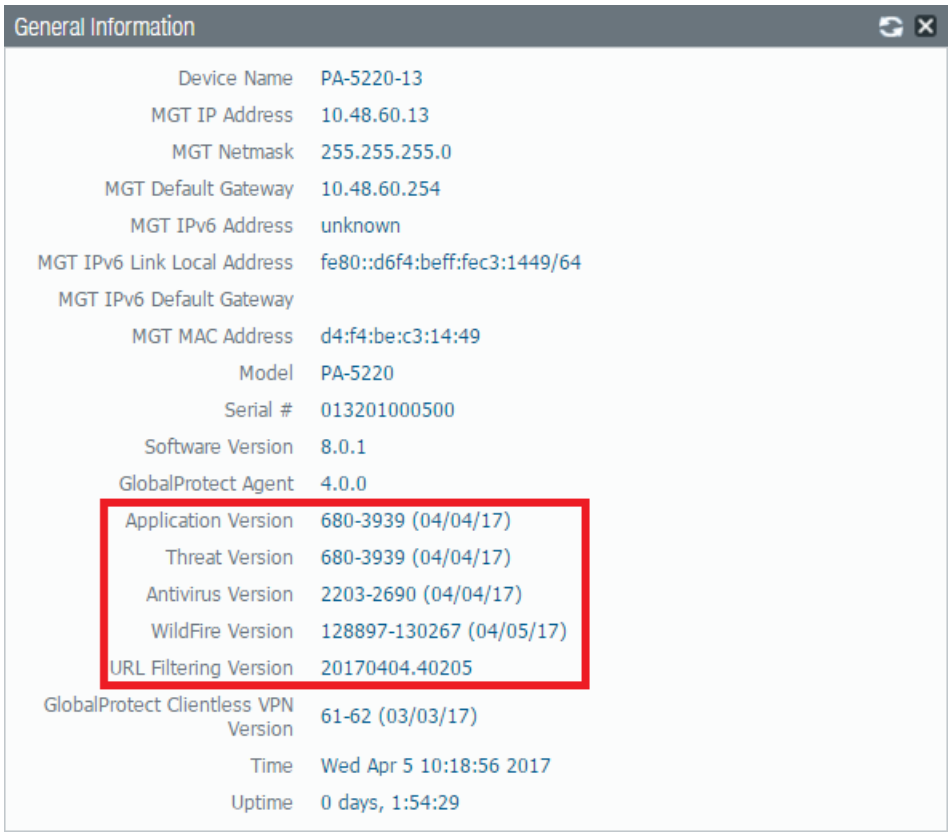
Screenshot of DP CPU during the test. CPU ~ 54%



Traffic log from the firewall during the test.

Receive Time	Type	From Zone	To Zone	Source	Destination	NAT Applied	NAT Source IP	From Port	To Port	Application	Action	Rule	Session End Reason	Bytes	Ingress I/F	Egress I/F
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.38	200.1.1.46	yes	200.1.1.254	10090	80	web-browsing	allow	rule37	tcp-fin	641.0k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.44	200.1.1.42	yes	200.1.1.254	64166	80	facebook-base	allow	rule43	tcp-fin	269.7k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.36	201.1.1.46	yes	200.1.1.254	25018	80	web-browsing	allow	rule85	tcp-fin	641.0k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.39	200.1.1.11	yes	201.1.1.254	41804	80	web-browsing	allow	rule38	tcp-fin	295.0k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.25	200.1.1.4	yes	201.1.1.254	30319	25	smtp	allow	rule24	tcp-fin	111.4k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.45	200.1.1.27	yes	201.1.1.254	53420	25	smtp	allow	rule44	tcp-fin	18.9k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.9	200.1.1.36	yes	201.1.1.254	2252	80	web-browsing	allow	rule8	tcp-fin	641.0k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.40	201.1.1.6	yes	200.1.1.254	27097	80	google-base	allow	rule89	tcp-fin	40.0k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.40	201.1.1.18	yes	200.1.1.254	59502	25	smtp	allow	rule89	tcp-fin	18.9k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.25	200.1.1.6	yes	201.1.1.254	9778	80	facebook-base	allow	rule24	tcp-fin	269.7k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.15	201.1.1.30	yes	201.1.1.254	14524	25	smtp	allow	rule64	tcp-fin	18.9k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.6	200.1.1.6	yes	200.1.1.254	28428	80	web-browsing	allow	rule5	tcp-fin	295.0k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.10	200.1.1.2	yes	200.1.1.254	60453	80	facebook-base	allow	rule9	tcp-fin	269.7k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.49	200.1.1.38	yes	201.1.1.254	5340	25	smtp	allow	rule48	tcp-fin	18.9k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.5	201.1.1.43	yes	201.1.1.254	3040	80	web-browsing	allow	rule54	tcp-fin	641.0k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.25	201.1.1.35	yes	201.1.1.254	63584	25	smtp	allow	rule74	tcp-fin	18.9k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.45	201.1.1.43	yes	201.1.1.254	45388	25	smtp	allow	rule94	tcp-fin	111.4k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	101.1.1.10	201.1.1.44	yes	200.1.1.254	18823	80	facebook-base	allow	rule59	tcp-fin	269.7k	ethernet1/7	ethernet1/8
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.28	200.1.1.32	yes	200.1.1.254	30194	80	web-browsing	allow	rule27	tcp-fin	295.0k	ethernet1/5	ethernet1/6
04/05 09:49:16	end	l3-trust	l3-untrust	100.1.1.6	200.1.1.21	yes	200.1.1.254	59923	80	web-browsing	allow	rule5	tcp-fin	641.0k	ethernet1/5	ethernet1/6

5220 Firewall Configuration – Running latest content



General Information

Device Name	PA-5220-13
MGT IP Address	10.48.60.13
MGT Netmask	255.255.255.0
MGT Default Gateway	10.48.60.254
MGT IPv6 Address	unknown
MGT IPv6 Link Local Address	fe80::d6f4:beff:fec3:1449/64
MGT IPv6 Default Gateway	
MGT MAC Address	d4:f4:be:c3:14:49
Model	PA-5220
Serial #	013201000500
Software Version	8.0.1
GlobalProtect Agent	4.0.0
Application Version	680-3939 (04/04/17)
Threat Version	680-3939 (04/04/17)
Antivirus Version	2203-2690 (04/04/17)
WildFire Version	128897-130267 (04/05/17)
URL Filtering Version	20170404.40205
GlobalProtect Clientless VPN Version	61-62 (03/03/17)
Time	Wed Apr 5 10:18:56 2017
Uptime	0 days, 1:54:29

Bypass queue limit for both TCP and UDP are disabled.

```
admin@PA-5220-13> show system setting ctd state

Notify user for APP block      : no
Alternative AHO                : no
Skip CTD                       : no
Parse x-forwarded-for          : no
Strip x-fwd-for                : no
Bloom Filter                   : yes
HTTP Proxy Use Transaction     : yes
Enable Regex Statistics        : no
URL Category Query Timeout     : 5
Bypass when exceeds queue limit for TCP: no
Bypass when exceeds queue limit for UDP: no
packets queued for packet capture: 5
whether to do packet capture after: yes
max. loop for packets processing: 1024
Not to Block HTTP Range request: no
to forward Active DNS          : no
packets sent of threat packet capture: 5
Always track the file name if possible: no
Allow virus hash signature checking: yes
Autogen Matching               : yes
Wildfire blocked file forward : yes
Content Allocator Usage        : 143872 KB (21% of 661376 KB)

Current CTD Version            : 1    (idx 1)
   TDB AHO Virus(valid) Wildfire(valid) Custom(valid) Autogen(valid)
   CTD Usage                   : 55552  KB (Actual 55445  KB)
   AHO Allocator Usage         : 46464  KB (Actual 46137  KB)
   Virus Allocator Usage       : 21632  KB (Actual 21361  KB)
   Wildfire Allocator Usage    : 6144   KB (Actual 5887   KB)
   Custom Allocator Usage      : 128    KB (Actual 49     KB)
   Autogen Allocator Usage     : 384    KB (Actual 332    KB)

No Alternate CTD
```

```
admin@PA-5220-13> show running application setting

Application setting:
Application cache                  : yes
Supernode                          : yes
Heuristics                         : yes
Cache Threshold                    : 16
Bypass when exceeds queue limit: no
Traceroute appid                   : yes
Traceroute TTL threshold           : 30
Use cache for appid                : no
Use simple appsigs for ident       : yes
Unknown capture                    : on
Max. unknown sessions              : 5000
Current unknown sessions           : 0
Application capture                : off

Current APPID Signature
   Memory Usage                    : 13568  KB (Actual 13294  KB)
      TCP 1 C2S                    : regex 8997   states
      TCP 1 S2C                    : regex 3852   states
      UDP 1 C2S                    : regex 3385   states
      UDP 1 S2C                    : regex 1429   states
```

Firewall interfaces configured in Layer 3 mode.

Interface	Interface Type	Management Profile	Link State	IP Address	Virtual Router	Tag	VLAN / Virtual-Wire	Security Zone	Features	Comment
ethernet1/1				none	none	Untagged	none	none		
ethernet1/2				none	none	Untagged	none	none		
ethernet1/3				none	none	Untagged	none	none		
ethernet1/4				none	none	Untagged	none	none		
ethernet1/5	Layer3	ping		100.1.1.254/24	default	Untagged	none	l3-trust		
ethernet1/6	Layer3	ping		200.1.1.254/24	default	Untagged	none	l3-untrust		
ethernet1/7	Layer3	ping		101.1.1.254/24	default	Untagged	none	l3-trust		
ethernet1/8	Layer3	ping		201.1.1.254/24	default	Untagged	none	l3-untrust		

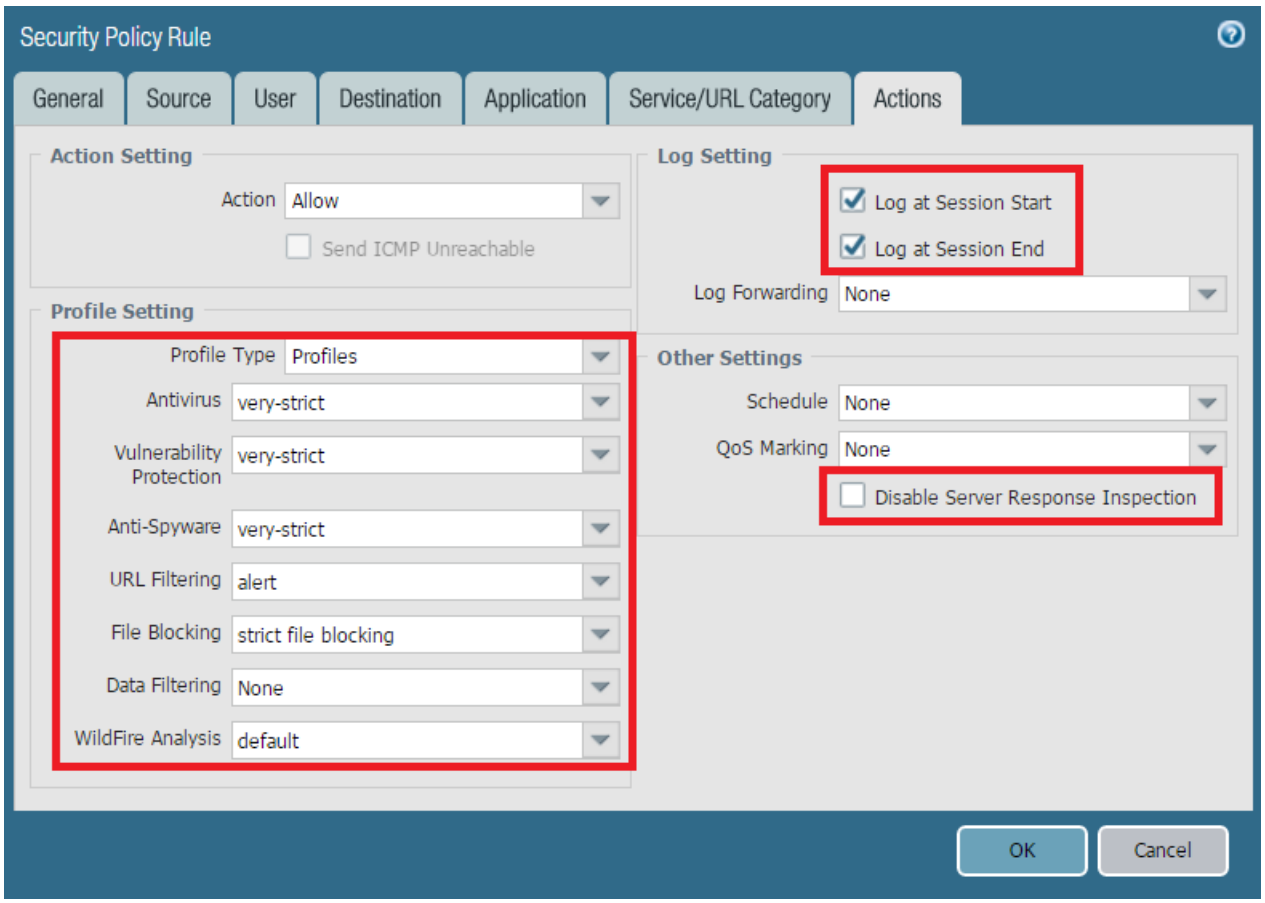
Following Source NAT is configured.

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	SNAT	none	l3-trust	l3-untrust	any	any	any	any	dynamic-ip-and-port 200.1.1.254,201.1.1.254	none

100 Security Policies used with each policy configured with Threat Prevention.

				Source				Destination						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
79	rule79	none	universal	l3-trust	101.1.1.30	any	any	l3-untrust	any	any	any	Allow		
80	rule80	none	universal	l3-trust	101.1.1.31	any	any	l3-untrust	any	any	any	Allow		
81	rule81	none	universal	l3-trust	101.1.1.32	any	any	l3-untrust	any	any	any	Allow		
82	rule82	none	universal	l3-trust	101.1.1.33	any	any	l3-untrust	any	any	any	Allow		
83	rule83	none	universal	l3-trust	101.1.1.34	any	any	l3-untrust	any	any	any	Allow		
84	rule84	none	universal	l3-trust	101.1.1.35	any	any	l3-untrust	any	any	any	Allow		
85	rule85	none	universal	l3-trust	101.1.1.36	any	any	l3-untrust	any	any	any	Allow		
86	rule86	none	universal	l3-trust	101.1.1.37	any	any	l3-untrust	any	any	any	Allow		
87	rule87	none	universal	l3-trust	101.1.1.38	any	any	l3-untrust	any	any	any	Allow		
88	rule88	none	universal	l3-trust	101.1.1.39	any	any	l3-untrust	any	any	any	Allow		
89	rule89	none	universal	l3-trust	101.1.1.40	any	any	l3-untrust	any	any	any	Allow		
90	rule90	none	universal	l3-trust	101.1.1.41	any	any	l3-untrust	any	any	any	Allow		
91	rule91	none	universal	l3-trust	101.1.1.42	any	any	l3-untrust	any	any	any	Allow		
92	rule92	none	universal	l3-trust	101.1.1.43	any	any	l3-untrust	any	any	any	Allow		
93	rule93	none	universal	l3-trust	101.1.1.44	any	any	l3-untrust	any	any	any	Allow		
94	rule94	none	universal	l3-trust	101.1.1.45	any	any	l3-untrust	any	any	any	Allow		
95	rule95	none	universal	l3-trust	101.1.1.46	any	any	l3-untrust	any	any	any	Allow		
96	rule96	none	universal	l3-trust	101.1.1.47	any	any	l3-untrust	any	any	any	Allow		
97	rule97	none	universal	l3-trust	101.1.1.48	any	any	l3-untrust	any	any	any	Allow		
98	rule98	none	universal	l3-trust	101.1.1.49	any	any	l3-untrust	any	any	any	Allow		
99	rule99	none	universal	l3-trust	101.1.1.50	any	any	l3-untrust	any	any	any	Allow		
100	rule100	none	universal	l3-trust	101.1.1.51	any	any	l3-untrust	any	any	any	Allow		

Confirming we are configured with Logging at session start and session end, no DSRI, and Threat Prevention.



Following AntiVirus profile is used for the test.

			Decoders			Application Exceptions		
Name	Location	Packet Capture	Name	Action	WildFire Action	Name	Action	Threat Exceptions
default	Predefined		http	default (reset-both)	allow			0
			smtp	default (alert)	allow			
			imap	default (alert)	allow			
			pop3	default (alert)	allow			
			ftp	default (reset-both)	allow			
			smb	default (reset-both)	allow			
strict			http	reset-both	reset-both			0
			smtp	reset-both	reset-both			
			imap	reset-both	reset-both			
			pop3	reset-both	reset-both			
			ftp	reset-both	reset-both			
			smb	reset-both	reset-both			
very-strict			http	reset-both	reset-both			0
			smtp	reset-both	reset-both			
			imap	reset-both	reset-both			
			pop3	reset-both	reset-both			
			ftp	reset-both	reset-both			
			smb	reset-both	reset-both			
alert			http	alert	alert			0
			smtp	default (alert)	default (alert)			
			imap	default (alert)	default (alert)			
			pop3	default (alert)	default (alert)			
			ftp	alert	alert			
			smb	alert	alert			

Following Anti-Spyware profile is used for the test.

Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture
default	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable
			simple-high	any	high	default	disable	
			simple-medium	any	medium	default	disable	
			simple-low	any	low	default	disable	
strict	Predefined	Rules: 5	simple-critical	any	critical	reset-both	disable	disable
			simple-high	any	high	reset-both	disable	
			simple-medium	any	medium	reset-both	disable	
			simple-informational	any	informational	default	disable	
			simple-low	any	low	default	disable	
very-strict		Rules: 1	any	any	any	reset-both	disable	disable
		Exceptions: 2						
alert		Rules: 1	alert	any	any	alert	disable	disable
		Exceptions: 2						

Following Vulnerability Protection profile is used for the test.

Name	Location	Count	Rule Name	Threat Name	Host Type	Severity	Action	Packet Capture
strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
			simple-client-high	any	client	high	default	disable
			simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable
very-strict		Rules: 1	very-strict	any	any	any	reset-both	disable
		Exceptions: 1						
alert		Rules: 1	alert	any	any	any	alert	disable

Following URL Filtering profile is used for the test.

Name	Location	Block List	Action for Block List	Allow List	Site Access	User Credential Submission
default	Predefined		block		Allow Categories (57) Alert Categories (0) Continue Categories (0) Block Categories (8) Override Categories (0)	Allow Categories (65) Alert Categories (0) Continue Categories (0) Block Categories (0)
alert			block		Allow Categories (0) Alert Categories (65) Continue Categories (0) Block Categories (0) Override Categories (0)	Allow Categories (65) Alert Categories (0) Continue Categories (0) Block Categories (0)

Following File Blocking profile is used for the test.

Name	Location	Rule Name	Applications	File Types	Direction	Action
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert
alert		FB	any	any	both	alert

Following Wildfire profile is used for the test.

Name	Location	Rule Name	Applications	File Types	Direction	Analysis
default	Predefined	default	any	any	both	public-cloud