#214147

December 2014

Commissioned by
Penta Security Systems, Inc.

# Penta Security WAPPLES Web Application Firewall (WAF)

## Detection Effectiveness, Performance and Management Functionality Evaluation

## EXECUTIVE SUMMARY

Because the web is an essential business tool and in constant use by organizations small and large, it is also the most likely path for attacks to enter an organization. The threats are ever-changing and a challenge for most security vendors to detect. Failure to detect attacks can disrupt the flow of business; at the same time, legitimate users need to access the web server for convenience and efficiency. Penta Security has designed the WAPPLES web application firewall security engine to block web attacks, while providing accurate detection and minimizing performance degradation.

Penta Security Systems, Inc. commissioned Tolly to evaluate the effectiveness, performance and functionality of its WAPPLES WAF and compare that to a widely deployed competing product (identified in this report as Vendor X).

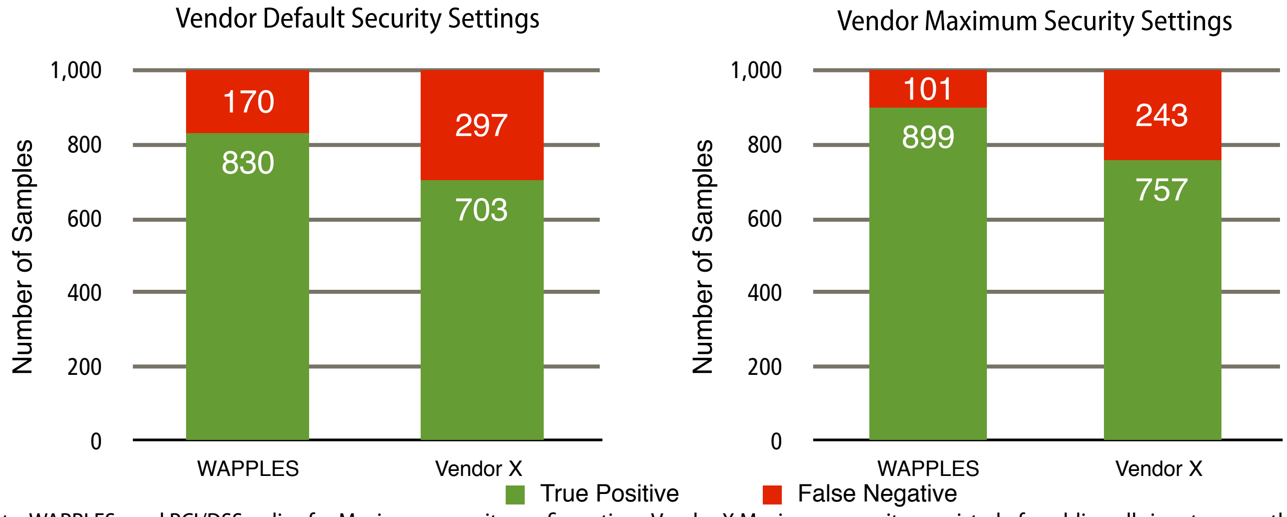
Tests showed that the Penta Security solution provided more effective security both at default and maximum settings, delivered higher performance at both settings and delivered greater functionality than the Vendor X solution.

## THE BOTTOM LINE

Penta Security WAPPLES outperforms Vendor X by providing:

1. Effective security, by detecting 89.9% of web attacks with maximum setting, compared to 75.7% for Vendor X
2. Significantly more accurate detection, with 4% false positives in maximum setting, compared to 29% false positives for Vendor X
3. Better web performance, with 4,000 more CPS, and 9,000 more TPS than Vendor X in maximum security settings
4. Less performance degradation, with 14.3% TPS performance degradation from default to maximum setting, while Vendor X recorded 42.3% degradation
5. More WAF functions, outperforming Vendor X by nine points out of 100

**WAF Effectiveness with Default and Maximum Security Policies**
**Using 1000 Attack Samples**
**(as reported by custom script )**


Vendor Default Security Settings

Vendor Maximum Security Settings

Note: WAPPLES used PCI/DSS policy for Maximum security configuration. Vendor X Maximum security consisted of enabling all signatures on the system. Green denotes that no data was compromised by the WAF, while red denotes that the attack was successful.

Source: Tolly, October 2014

Figure 1

# Test Results

## Effectiveness

### Threat Detection

As the core function of a WAF is to stop threats, Tolly engineers first evaluated the effectiveness of the two solutions. Solutions were tested in two configurations: 1) default , and 2) maximum security against a collection of 1,000 threats. See Test Methodology section for details. For an illustration of the WAPPLES detection architecture, see Figure 4.

In the test of default settings, WAPPLES WAF detected 83% of the threats compared with 70.3% for Vendor X. When both solutions were set to maximum security levels, WAPPLES WAF detected 89.9% of the threats compared with 75.7% for the competing solution. See Figure 1.

### False Positive Avoidance

Along with detecting threats, it is important for WAF solutions to avoid "false positives" where legitimate requests are mistakenly categorized as threats and stopped. Tolly engineers ran a test of 100 valid HTTP requests through both solutions, again, in default and maximum security settings.

In default setting, the Penta WAPPLES had zero percent false positives compared to 24% for the competing solutions. See Table 1.

**Penta Security Systems**

**WAPPLES**

**Web Application Firewall Effectiveness, Performance and Functionality**

Tolly. Certified

*Tested October 2014*

## Performance

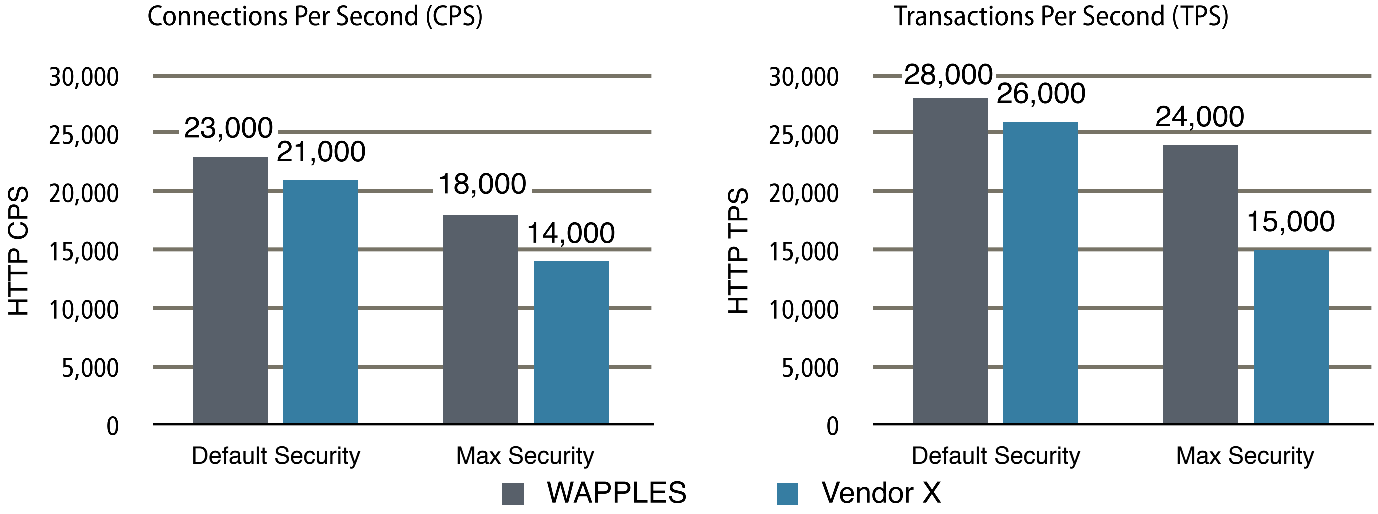
### In-Line Throughput

While providing protection, it is vital that the WAF not degrade performance for the organization. For this test, Tolly engineers

**WAPPLES Web Application Firewall Gigabit Ethernet Performance**

**Connection and Transaction Rate in Default/Maximum Security Configuration**

**(as reported by Spirent Avalanche Commander 4.30)**



Note: WAPPLES used PCI/DSS policy for Maximum security configuration. Vendor X Maximum security consisted of enabling all signatures on the system. CPS measured with one transaction per connection, TPS measured 10 transactions per connection, 1KB response object. A result of 25,000 implies that this test passed at 25,000 but failed at 26,000.

Source: Tolly, October 2014

Figure 2

used commercial test tools to evaluate the connection and transaction performance of each solution when deployed “in-line” in a Gigabit Ethernet network.

Security devices are typically evaluated by benchmarking performance in two areas: connection rate and transaction rate.

## Connections Per Second

Tolly engineers benchmarked the maximum rate of successful connections each device could sustain over the course of a three-minute test with only a single transaction per test. WAPPLES outperformed the competition when tested both with default and maximum security settings. With default settings, WAPPLES delivered 2,000 more CPS than the competitor while with maximum security settings, WAPPLES outperformed Vendor X by 4,000 CPS. See Figure 2.

### WAF Effectiveness - False Positive Rate

| Vendor | Product Configuration | |
|---|---|---|
| | Default | Max. Security |
| Penta Security WAPPLES | 0% | 4% |
| Vendor X | 24% | 29% |

Note: Collection of 100 valid traffic items used for testing. Delivered via same mechanism as detection tests.

Source: Tolly, October 2014 Table 1

## Transactions Per Second

Tolly engineers benchmarked the maximum rate of successful transaction each device could sustain over the course of a three-minute test with only a single connection running 50 transactions per test. WAPPLES outperformed the competition when tested both with default and maximum security settings. With default settings, WAPPLES delivered 2,000 more TPS than the competitor while in the maximum setting, WAPPLES outperformed Vendor X by 9,000 CPS. See Figure 2.

### Summarized Result of WAF Maximum Security Detection Test

| Task # | Task Category | WAPPLES Score | Vendor X Score |
|---|---|---|---|
| 1 | Prevent disclosure of error information in the server side response. | 4/4 | 4/4 |
| 2 | Equipped with a function to evaluate Web Requests and Responses based on security policies or countermeasure settings such as Block, Allow, or Warn. | 2/2 | 2/2 |
| 3 | Have a capability of checking various types of files for credit card information leakage prevention. | 4/4 | 4/4 |
| 4 | Support both whitelisting and blacklisting for actions, inputs, and data. | 2/2 | 2/2 |
| 5 | Have an ability to detect Simple Object Access Protocol (SOAP) based attacks. | 1/1 | 0/1 |
| 6 | Prevent hidden field manipulation and session cookie tampering. | 2/2 | 1/2 |
| 7 | Block uploading malicious files. | 1/1 | 1/1 |
| 8 | Prevent brute force attacks and HTTP DDoS attacks. | 2/2 | 2/2 |
| | Total | 18/18 | 16/18 |

Note: Cells in red denote sections where Vendor did not pass all items tested. Refer to Table 4 for detailed scores and test definitions. Products tested in maximum security configuration. Based on Web Application Firewall Evaluation Criteria (WAFEC), published by the Web Application Security Consortium.

Source: Tolly, October 2014 Table 2

## WAF Functionality Test Results Summary

| Task # | Task Category | WAPPLES Score | Vendor X Score |
|---|---|---|---|
| 1 | Provide automated updates on system software and signatures. | 10 | 10 |
| 2 | Provide rich CLI (Command Line Interface). | 10 | 6 |
| 3 | Provide comprehensive query system for detection logs. | 8 | 10 |
| 4 | Provide functionality to easily configure security policies. | 10 | 10 |
| 5 | Provide comprehensive reporting. | 10 | 10 |
| 6 | Support exchanging detection logs and system information with external systems. | 10 | 7.5 |
| 7 | Provide a function to back up its configurations and important data. | 10 | 7.5 |
| 8 | Provide a comprehensive dashboard so that users can check various information at a glance. | 10 | 8 |
| 9 | Provide a function to manage websites and web servers. | 10 | 10 |
| 10 | Provide a function for network setup. | 10 | 10 |
| Total | | 98 | 89 |

Note: Cells in red denote sections where Vendor did not pass all items tested. Refer to Tables 5 and 6 for detailed scores and test definitions. Based on WAFEC published by the Web Application Security Consortium.

Source: Tolly, October 2014

Table 3

## Distributed Denial of Service (DDoS) Attack Mitigation

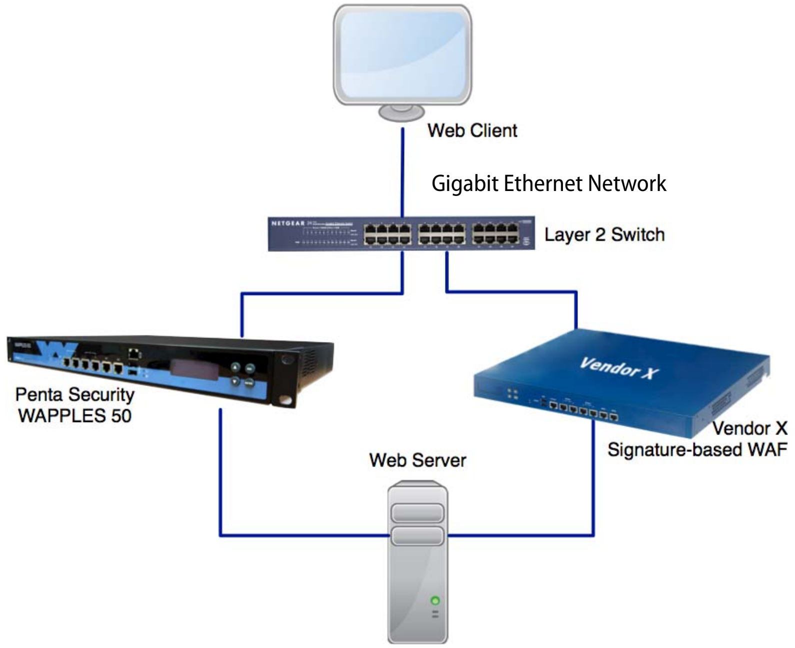
Tolly engineers benchmarked the devices to determine if 400 TPS throughput could be sustained while undergoing a DDoS attack. Both solutions passed this test.

## Detection and System Functionality

### WAF Evaluation Criteria

Tolly engineers ran an extensive battery of functionality tests on both solutions related to detection capabilities. The tests were largely based on Web Application Firewall Evaluation Criteria, published by the Web Application Security Consortium.

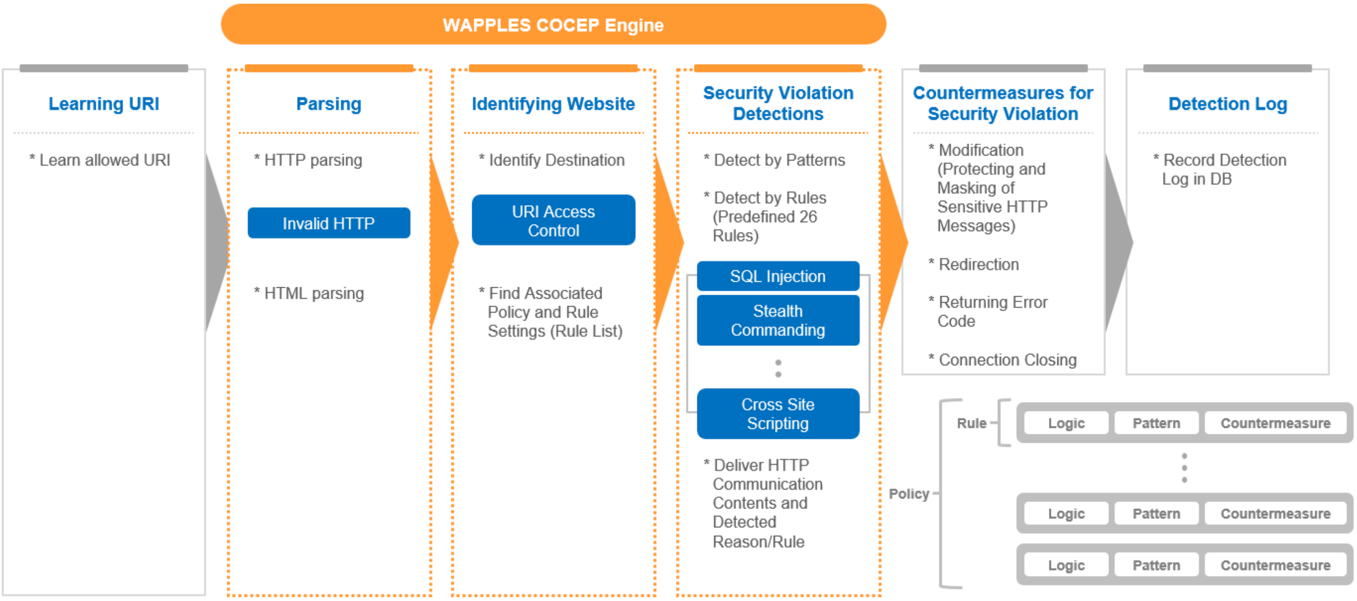
### Test Bed Topology



Source: Tolly, October 2014

Figure 3

**WAPPLES Detection Process**



Source: Penta Security, October 2014

Figure 4

## Detection Functionality

The detection functionality test consisted of 8 different areas. The WAPPLES solution scored 18 out of a possible 18. See Table 2.

The detailed results of the 40+ individual functionality tests can be found in Table 4.

## System Functionality

The system functionality test consisted of ten different areas. The WAPPLES solution scored a 98 out of a possible 100. See Table 3.

The detailed results of the 40+ individual functionality tests can be found in Tables 5 and 6.

# Test Setup & Methodology

## Environment

Tests were conducted in an isolated environment using one Penta Security WAPPLES-50 appliance (version 4.0.34.8). A signature-based web application firewall with the same throughput and similar technical specifications from a leading vendor was used as the competing product. See Table 7 on the last page. This device was updated to the latest firmware and signatures prior to testing. See Figure 3.

A Spirent Avalanche 2900 was used to determine the TPS and CPS supported by both of the devices under test (DUT). The standard Spirent tests were used to measure TPS and CPS of each solution.

Throughout the testing, the Maximum security configuration was the PCI/DSS policy for Penta Security WAPPLES, and all signatures enabled for Vendor X.

## Detection Effectiveness

To validate the effectiveness for large numbers of common Web attack samples, Tolly relied on 'WATH' (WAF Truth) an internal tool developed by Penta Security to automate false positive/negative testing.

This tool selected parameters from an attack database (including the expected response) and was able to perform a Web attack on the web server system.

Depending on the response received, the tool marks attacks as pass/fail.

A collection of 1,000 attacks were used to test the effectiveness of each solution, in both default and maximum security settings. This was run multiple times to ensure accuracy. The attack set was a random subset of attacks collected by Penta from Exploit-DB, 1337 Inj3ct0r, SQL Injection Wiki, fuzzdb and other online security communities.

### False Positive Avoidance

The false positive testing utilized the same 'WATH' tool. However, instead of sending malicious traffic, the tool was loaded with valid HTTP requests in an attempt to perform false positive testing.

One hundred samples collected from Exploit-DB, 1337 Inj3ct0r, SQL Injection Wiki, fuzzdb and other online security communities were tested in total, in both default and maximum security settings. Any response other than error code 400 (Bad Request) was treated as a pass.

## Performance

Spirent Avalanche Commander 4.30 was used to control the test. Each iteration was run for three minutes, with a ramp-up of one minute.

### Connections Per Second

For the CPS test, engineers configured Spirent to generate connections with a single 1KB 'text_plain' transaction, and to close the connection upon completion.

Engineers set a DUT in the designated operating mode, then configured Spirent to send 10,000 CPS. If a given test passed, the rate was increased by 1,000 CPS until 'unsuccessful' is returned by some of the Spirent clients. The reported result is the highest CPS with zero failures.

### Transactions Per Second

The TPS test used the same environment described above, however each client was set to make 50 transactions for each connection, so that the number of connections were not a limiting factor.

### DDoS Mitigation

HTTP Attack version 3.6 was used to test DDoS mitigation in two scenarios, Slow headers, and Slow post. The Slow headers method kept a connection alive by not including a 'CRLF' at the end of a request, while the Slow post method deliberately sent incomplete data to keep the connection alive. 400 concurrent connections were attempted to the web server through each WAF.

## Detection & System Functionality

A web server was used to demonstrate the functionality of each system. Penta Security prepared templates of various websites for use in the test.

These websites were pre-configured to be vulnerable to a wide range of methods, and meant to provide Web attacks for the WAF to detect and block.

Testing covered multiple related areas, outlined in detail in Tables 4-6. Engineers leveraged the WAFEC, published by the Web Application Security Consortium, as a base for the test definitions.

For each test, engineers first confirmed the exploit's effectiveness by attacking the web server directly. Then, a DUT, configured with its maximum security policy, was placed in front of the web server, and the exploit was retried.

Various HTTP tools such as the DHC chrome extension and programs in the BURP suite were used to assist with test goals.

If the Vendor X product failed to detect a given attack, configuration was modified as appropriate. Vendor X passed all tests with the exception of:

-Detection of a SOAP payload

-Detects HTTP requests containing manipulated hidden values through proxy tool

A policy could not be found or created to cover the above test items.

## Detection Matrix

| | Task Category | Task | Penta Security | Vendor X |
|---|---|---|---|---|
| 1 | Prevent disclosure of error information in the server side response. | Detects MS-SQL error information leakage. | *Pass* | *Pass* |
| | | Detects MY-SQL error information leakage. | *Pass* | *Pass* |
| | | Detects Oracle error information leakage. | *Pass* | *Pass* |
| | | Detects PHP error information leakage. | *Pass* | *Pass* |
| 2 | Equipped with a function to evaluate Web Requests and Responses based on security policies or countermeasure settings such as Block, Allow, or Warn. | Detects an attack request containing a simple web attack utilizing IMG tag. | *Pass* | *Pass* |
| | | Detects HTTP response messages containing the directory listing information. | *Pass* | *Pass* |
| 3 | Have a capability of checking various types of files for credit card information leakage prevention. | Detects PDF file that includes credit card information. | *Pass* | *Pass* |
| | | Detects Zip compressed file that includes credit card information. | *Pass* | *Pass* |
| | | Detects Xls file that includes credit card information. | *Pass* | *Pass* |
| | | Detects Doc file that includes credit card information. | *Pass* | *Pass* |
| 4 | Support both whitelisting and blacklisting for actions, inputs, and data. | Blocks HTTP requests that do not have user-agent field. | *Pass* | *Pass* |
| | | Bypasses HTTP requests that contain a specified HTTP field. | *Pass* | *Pass* |
| 5 | Have an ability to detect Simple Object Access Protocol (SOAP) based attacks. | Detection of SOAP Payload. | *Pass* | *Fail* |
| 6 | Prevent hidden field manipulation and session cookie tampering. | Detects HTTP requests containing tampered client's session cookie through proxy tool. | *Pass* | *Pass* |
| | | Detects HTTP requests containing manipulated hidden values through proxy tool. | *Pass* | *Fail* |
| 7 | Block uploading malicious files. | Blocks attempts to upload shell script file. | *Pass* | *Pass* |
| 8 | Prevent brute force attacks and HTTP DDoS attacks. | Blocks the Dictionary attacks to a login page through a brute force attack tool. | *Pass* | *Pass* |
| | | Blocks HTTP DDoS attacks through an automated DDoS tool. | *Pass* | *Pass* |

Note: Penta Security WAPPLES was configured with PCI-DSS policy. Vendor X product has all signatures enabled, custom policies created where possible.

Source: Tolly, October 2014

Table 4

## Functionality Matrix

| | | | Penta Security | | Vendor X | |
|---|---|---|---|---|---|---|
| | Task Category | Task | Result | Score | Result | Score |
| 1 | Provide automated updates on system software and signatures. | Provides GUI (Graphic User Interface) to accommodate a menu for automated updates. | Pass | 2.5 | Pass | 2.5 |
| | | Provides software updates online. | Pass | 2.5 | Pass | 2.5 |
| | | Provides signature (security pattern) updates online. | N/A - Pass | 2.5 | Pass | 2.5 |
| | | Notifies if there is any software or signature update. | N/A - Pass | 2.5 | Pass | 2.5 |
| | Section Score | | 10 | | 10 | |
| 2 | Provide rich CLI (Command Line Interface). | Allows users to configure Management IP from CLI. | Pass | 2 | Pass | 2 |
| | | Allows users to set up network bypass function from CLI. | Pass | 2 | Pass | 2 |
| | | Allows users to check the system status as well as resource usages from CLI. | Pass | 2 | Fail | 0 |
| | | Provides a function to show the system error logs from CLI. | Pass | 2 | Pass | 2 |
| | | Provides real-time information about the network from CLI. | Pass | 2 | Fail | 0 |
| | Section Score | | 10 | | 6 | |
| 3 | Provide comprehensive query system for detection logs. | Allows users to query the detection logs during a specified time/ date period. | Pass | 2 | Pass | 2 |
| | | Allows users to query the detection logs based on attack categories. | Pass | 2 | Pass | 2 |
| | | Allows users to query the detection logs based on website. | Pass | 2 | Pass | 2 |
| | | Allows users to query the detection logs based on risk or severity of attack. | Fail | 0 | Pass | 2 |
| | | Allows users to export detection logs to a file. | Pass | 2 | Pass | 2 |
| | Section Score | | 8 | | 10 | |
| 4 | Provide functionality to easily configure security policies. | Allows users to manage security policies/rules to provide various types of the levels of security. | Pass | 2.5 | Pass | 2.5 |
| | | Provides a function to configure access control in the GUI tool. | Pass | 2.5 | Pass | 2.5 |
| | | Automatically lock a session if the system does not get anything during a certain amount of time. | Pass | 2.5 | Pass | 2.5 |
| | | Provides audit logs for any administrative actions in GUI tool. | Pass | 2.5 | Pass | 2.5 |
| | Section Score | | 10 | | 10 | |
| 5 | Provide comprehensive reporting. | Allows users to set a period for reporting. | Pass | 2.5 | Pass | 2.5 |
| | | Allows users to set a website for reporting. | Pass | 2.5 | Pass | 2.5 |
| | | Allows users to set security policies/rules for reporting. | Pass | 2.5 | Pass | 2.5 |
| | | Allows users to configure graph formats for reporting. | Pass | 2.5 | Pass | 2.5 |
| | Section Score | | 10 | | 10 | |

Note: Penta Security WAPPLES was configured with PCI-DSS policy. Vendor X product has all signatures enabled, custom policies created where possible.

Source: Tolly, October 2014

Table 5

## Functionality Matrix (Continued)

| Task Category | | Task | Penta Security | | Vendor X | |
|---|---|---|---|---|---|---|
| | | | Result | Score | Result | Score |
| 6 | Support exchanging detection logs and system information with external systems. | Supports SNMPv2 and SNMPv3. | Pass | 2.5 | Pass | 2.5 |
| | | Supports syslog. | Pass | 2.5 | Pass | 2.5 |
| | | Exchanges various types of information. | Pass | 2.5 | Pass | 2.5 |
| | | Provides a web API to exchange information. | Pass | 2.5 | Fail | 0 |
| | Section Score | | 10 | | 7.5 | |
| 7 | Provide a function to back up its configurations and important data. | Allows users to store configuration data as files in local storage. | Pass | 2.5 | Pass | 2.5 |
| | | Allows users to back up the configuration data via FTP/SFTP. | Pass | 2.5 | Pass | 2.5 |
| | | Allows users to restore the configuration from backup. | Pass | 2.5 | Pass | 2.5 |
| | | Allows users to check the list of backups. | Pass | 2.5 | Fail | 0 |
| | Section Score | | 10 | | 7.5 | |
| 8 | Provide a comprehensive dashboard so that users can check various information at a glance. | Allows users to adjust the type of visual graphs. | Pass | 2 | Pass | 2 |
| | | Provides a table information so that users check the detailed information. | Pass | 2 | Fail | 0 |
| | | Provides information on network traffics in a real-time manner. | Pass | 2 | Pass | 2 |
| | | Provides information on CPU and RAM usage in a real-time manner. | Pass | 2 | Pass | 2 |
| | | Provides information on the recent attacks. | Pass | 2 | Pass | 2 |
| | Section Score | | 10 | | 8 | |
| 9 | Provide a function to manage websites and web servers. | Allows users to register sub-directories of a website to apply the different security policy from the parent website. | Pass | 2 | Pass | 2 |
| | | Provides access control over each website. | Pass | 2 | Pass | 2 |
| | | Allows users to make alias or nickname for websites. | Pass | 2 | Pass | 2 |
| | | Supports multiple ports for the same domain name, such as www.domain.com:80, www.domain.com:8080, or www.domain.com:8000. | Pass | 2 | Pass | 2 |
| | | Allows users to upload SSL/TLS certificates in order for the system to analyze the encrypted HTTP messages. | Pass | 2 | Pass | 2 |
| | Section Score | | 10 | | 10 | |
| 10 | Provide a function for network setup. | Provides the hardware bypass function, and it allows users to configure to turn on or off the function, or to turn on automatically when it comes to the system failure. | Pass | 2 | Pass | 2 |
| | | Provides the software bypass function, and it allows users to configure to turn on or off the function. | Pass | 2 | Pass | 2 |
| | | Provides a simple network firewall function, which allows users to configure to block/allow a specific IP or port number. | Pass | 2 | Pass | 2 |
| | | Provides a function to block network traffics based on website domain name. | Pass | 2 | Pass | 2 |
| | | Provides QoS function that blocks or bypasses network traffic if the traffics exceed the capability of the system hardware. | Pass | 2 | Pass | 2 |
| | Section Score | | 10 | | 10 | |

Note: Penta Security WAPPLES was configured with PCI-DSS policy. Vendor X product has all signatures enabled, custom policies created where possible

Source: Tolly, October 2014

Table 6

## About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 25 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at sales@tolly.com, or by telephone at
+1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

## Target Products Specifications

| Area | WAPPLES-50 | Vendor X |
|---|---|---|
| Throughput | 100Mbps | 100Mbps |
| Memory | 4 GB | 8 GB |
| Network Interface Cards | 2 x 1GbE Copper<br>4 x 1GbE Copper | 2 x 1GbE Copper<br>4 x 1GbE Copper |
| Chassis Size | 1U | 1U |

Source: Vendor specifications, October 2014

Table 7

## Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

214147 qfmh1 jt-kt-2015-02-12-VerJ