Key findings and conclusions:

- Check Point SWG-12600 scored highest in testing, 91.3%, for classifying the one million most popular websites into known categories.
- Detecting and blocking rate for URL filtering in Adult (97.1%) and Gambling (93.4%) categories.
- Excellent granularity of security policies that allows access limits for websites to be set for individual users, groups of users or all users.
- Registers success rate of 97.0% in application control differentiation with URL filtering enabled.
- Application Control library is updated continually; currently consists of more than 4,800 applications and more than 240,000 social network widgets.

Check Point submitted the SWG-12600 Secure Web Gateway for evaluation in ongoing standardized testing for Web control, the Miercom Web Security Industry Assessment 2013. Hands-on testing assessed the SWG-12600 appliance versus two competing products in this class: the Websense Web Security Gateway (WSG) software platform, Version 7.6, running on a commercial off-the-shelf (COTS) server and the Blue Coat Proxy SG300-5 appliance.

Crucial areas of functionality for a secure Web gateway were put through a series of challenging processes, including malicious URL coverage, undesirable URL blocking efficacy and application control. Other Web security and performance tests were also performed.

The SWG-12600 is a comprehensive security solution designed for the data center as well as the perimeter of the enterprise network that...
The Check Point SWG-12600 provides secure Web access by monitoring network traffic in real time. It can be deployed inline or as monitor/tap and can also act as a proxy.

Check Point’s SWG-12600 is recommended for up to 10,000 users. A higher number of users can be supported with a valid license.

For testing, the R76 version of security firmware was run on the SWG-12600. R76 supports IPv4 and IPv6 and works on a GAiA secure operating system.

The SWG-12600 is the high-end model of five Secure Web Gateways offered. It has a default configuration of 12x1GE ports, with optional 1GE and 10GE expansions of up to 26x1GE ports or 12x10GE ports.

All Check Point Secure Web Gateways enable secure use of Web 2.0 by providing real-time, multi-layered protection against Web-borne malware. All use the Check Point Software Blade Architecture, which consists of software modules or blades that enables tailoring of security functionality based on end-user specifications.

**URL Classification and Coverage Test**

The objective of this test was to determine how many of the one million most popular websites the three secure Web gateways could correctly classify into pre-defined or known categories.

During the tests, the blocking functionality of each product was disabled. The SWG-12600 successfully classified 91.3% of the URLs. The product test performance is shown in Figure 1 on page 1.

**URL Filtering by Specific Categories**

This testing assessed the capability of the Web gateways to detect and block URLs in specific categories which were deemed to be undesirable, potentially malicious or malicious. Thousands of URLs in each category were collected from the initial classification of the one million websites. Each product underwent a separate test for each category. Default security policies, as well as the policies necessary to filter for each specific category, were enabled.

Check Point Secure Web Gateway appliances receive real-time URL updates from cloud-based categorization that blocks millions of malware and phishing websites. This enabled the SWG-12600 to have the best performance in URL Filtering–Adult (by 15% or more) and URL Filtering–Gambling (30% or more). See Figures 2 and 3 for complete results.

The Check Point appliance also earned the top spot in URL Filtering–Hacking Tools (37% or more) and URL Filtering–Phishing (22% or more) as shown in Figure 4 on page 3.

**Application Control**

Testing assessed the performance of the SWG-12600 and competing products in detecting and/or blocking applications and the traffic created by those applications.

---

The Check Point SWG-12600 detected and blocked 97.1% of known Adult URLs. This is an improvement of 15% or more over the Websense WSG and Blue Coat Proxy SG300-5 products.

The Check Point SWG-12600 scored 93.4% in the filtering test for known Gambling URLs.
Application control is a strength of Check Point Secure Web Gateways. The other products tested here had limited application control functionality.

Web 2.0 applications are increasingly used to enable the dynamic relationships some businesses use to stay competitive. However, overwhelmingly popular applications such as Facebook, IM and YouTube can create havoc for the enterprise network. They consume valuable bandwidth, impact employee productivity and expose the enterprise network to malware, increasing the probability of compromising the network and even cause loss of valuable company data.

To mitigate the risks and maximize the value of Web 2.0 applications for end-user organizations, it is necessary for a secure Web gateway to identify, monitor, report on and implement controls over Web-based applications.

The SWG-12600 had the latest Application Control library, which consists of more than 5,000 applications and more than 300,000 social networking widgets.

The Application Control library enhances network security and employee productivity by creating granular security policies for users and groups of users. The policies identify, block or limit usage of Web applications and Web widgets, such as those used in instant messaging, social networking, video streaming and online games.

A high degree of granularity can be built into a security policy. Using Facebook as an example, 23 portions of the application can be enabled or disabled. A policy can be set in the SWG-12600 that allows access to parts of Facebook that are beneficial to conducting business while preventing access from others that sap employee productivity, such as the chat area.

Figure 5 shows the Application and URL Filtering Policy Interface of the SWG-12600, which offers a myriad of combinations to network administrators. The interface is comprehensive yet easy to use.

The Check Point SWG-12600 performed nearly three times better than its nearest competitor in categorizing hacking tools.

In URL Filtering–Phishing, the performance of the SWG-12600 was 20% better than the Websense software and three times better than the Blue Coat Proxy SG300-5.
Application control is a strength of the SWG-12600. This plus the fact that the competing products have limited application control functionality contributing to this result, the SWG-12600 outperformed the nearest competitor by more than 30% in the test of application control with URL filtering enabled.

Two application control tests were run, one with URL filtering disabled and the other with URL filtering enabled.

The SWG-12600 was the clear winner in both, registering a blocking rate that was more than 30% greater than the nearest competitor.

With URL filtering disabled, the SWG-12600 achieved a blocking rate of 91.6%. With URL filtering enabled, the blocking rate was 97.1% as shown in Figure 6.

The sample size for both tests was more than 3,000 unique protocol/application combinations.

Throughput, CPU Protection Tests

Additional tests evaluated the performance capabilities of the SWG-12600 while Web control testing was in progress.

In the RFC 2544 throughput test, the SWG-12600 maintained 1GE (port line rate) with zero frame loss while filtering malicious traffic.

A simulated DoS flood attack was launched in an attempt to overburden the resources of the SWG-12600. No anomalies were observed. The SWG-12600 continued to detect the malicious traffic and continued to protect the network from Web-borne threats.

Bottom Line

The performance of the Check Point SWG-12600 Secure Web Gateway was verified as part of the Miercom Web Security Industry Assessment 2013.

The SWG-12600 had strong results in the areas that are crucial for a secure Web gateway. Classification of URLs into known categories, URL filtering for specific categories, application control and application control with URL filtering enabled all exceeded the performance of other tested products.

The large, ever-growing Application Control library of applications and Web widgets of the Check Point appliance and the high level of granularity that can be built into security policies are highly beneficial and provide an excellent source for protection from new, emerging threats.

The SWG-12600 exhibited the performance required for a data center and perimeter deployment to be able to safeguard the enterprise network from Web-borne threats while providing end users with a positive Web experience.
How We Did It

The devices under test included the Check Point SWG-12600 Secure Web Gateway, running firmware version R76, the Blue Coat Proxy SG300-5 appliance, version 6.2.7.2, and the Websense Web Security Gateway, running software version 7.6. Each device was evaluated using a Miercom client, Spirent Studio Performance application traffic simulator, BreakingPoint FireStorm and Ixia XM12. Competitive vendors were notified of this testing and afforded an opportunity to challenge these results. Official responses from Websense and Blue Coat are addressed in separate reports.

URL Classification Accuracy  The cache of the DUTs was adjusted to allow processing of the URLs. The SWG-12600 handled 10 runs of 100,000 URLs, as did the COTS server running Websense WSG software. The Blue Coat Proxy SG300-5 was able to handle five runs of 200,000 URLs.

URL Filtering by Specific Category  For detecting/blocking categories of undesirable, potentially malicious and malicious URLs, a database was created in Excel for each category. Miercom used multiple sources to obtain URLs for use in security testing. The URL of each of the one million most popular websites, based on worldwide traffic rating, was obtained in June 2013.

Application Control  Spirent Studio Performance software running on a Miercom server managed a Mu Dynamics Mu-4000 application simulator, which generated application traffic on the test network. The Mu-4000 ran Spirent Studio Security software.

A Layer 2 switch forwarded traffic to the secure Web gateways for a block/pass decision. Traffic that was allowed to pass was routed back to the Mu-4000 via another Layer 2 switch.

Throughput and CPU Protection Tests  The Ixia XM12 was used to generate traffic in the RFC 2544 throughput test. The BreakingPoint FireStorm was used to generate the DoS attack against the SWG-12600.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Current or prospective customers interested in repeating these results may contact reviews@miercom.com for details on the configurations applied to the Switch Under Test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a product selection.
Miercom Performance Verified

The performance of the Check Point SWG-12600 was verified by Miercom in a hands-on testing evaluation.

The Secure Web Gateway proved to be superior in identifying and classifying URLs into known categories, and offering URL filtering for specific categories and application control with URL filtering enabled.

With a large and continually updated Application Control library and a high level of granularity built into security policies, the SWG-12600 proved its strengths in safeguarding the enterprise network.

Miercom is proud to award the Check Point SWG-12600 the Performance Verified Certification.

About Miercom’s Product Testing Services

Miercom has hundreds of product-comparison analyses published over the years in leading network trade periodicals including Network World, Business Communications Review, Tech Web - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom’s reputation as the leading, independent product test center is unquestioned.

Miercom’s private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry’s most thorough and trusted assessment for product usability and performance.