Key findings and conclusions:

- Check Point SWG-12600 security appliance exhibits best rate to date, 91.3%, for classifying the one million most popular websites into known undesirable categories.
- URL classification and detection rates in Adult (97.1%) and Gambling (93.4%) categories are highest validated so far in ongoing testing.
- Highest blocking rates using current, in-the-wild and legacy malware sets, 90.3% and 81.8%, respectively.
- Blocking rates of greater than 90% in application control testing with URL filtering disabled and enabled.
- Granularity of application control allows security policies for website access to be set for individual users, groups of users or all users.

Check Point submitted the SWG-12600 Secure Web Gateway for evaluation in ongoing standardized testing for Web control, the Miercom Web Security Industry Assessment 2014. Hands-on testing assessed the capability of the SWG-12600 in crucial areas of functionality for a Secure Web Gateway: classification of URLs into malicious and potentially malicious categories, URL filtering, malware blocking and application control.

The Check Point 12600 is a datacenter-grade security appliance, the high-end model of three in the Check Point 12000 Series. In addition to two onboard 1GE copper ports, three available expansion slots can be used to configure a variety of network options, such as 1GE copper, 1GE fiber and 10GE fiber connections. The default configuration includes eight 1GE copper ports and a four-port 1GE.
copper expansion card. Fully loaded, the 12600 has a total of 26x1GE ports or 12x10GE ports.

Four different security configurations are possible for the 12600 depending on the software modules utilized. In addition to Secure Web Gateway, it can be configured as Next-Generation Firewall, Next-Generation Data Protection or Next-Generation Threat Protection.

The SWG-12600 can be deployed in-line, as a monitor/tap, or as a proxy in a data center to provide real-time, multi-layered protection against Web-borne malware. Key specifications include being able to handle 22,000 HTTP transactions per second and supporting up to 10,000 users.

The SWG-12600 tested had the latest Check Point cyber-security software release, R77.10, which works on the GAiA secure operating system.

**URL Coverage and Classification Test**

The objective was to determine how many of the one million most popular URLs the SGW-12600 could correctly classify into pre-defined or known malicious and potentially malicious categories. The malware blocking functionality of the SWG-12600 was disabled.

The performance of the SWG-12600, a blocking rate of 91.3%, was the best to date in ongoing testing. A comparison of the performance of the SWG-12600 and the Industry Average is shown in Figure 1 on page 1.

**URL Filtering**

Thousands of URLs were in each category as a result of the initial test, classification of the one million most popular URLs. The URL filtering capability of the SWG-12600 was challenged by a separate test using the URLs in each category. Default security policies as well as the policies needed to filter for each 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 functionality enabled the SWG-12600 to exceed the Industry Average in the Adult, Gambling and Phishing categories.

Figures 2 and 3 show a comparison of the URL filtering performance of the SWG-12600 against the Adult and Gambling URLs and the Industry Average. The SWG-12600 exceeded the Industry Average for Adult URLs by 4.9% and for Gambling URLs by 8.0%.

Also, the performance of the SWG-12600 exceeded the Industry Average for Phishing URLs by 14.1%, achieving a blocking rate of 77.9%. The Industry Average is 63.8%.

**Malware Detection**

The SWG-12600 also was tested using two sets of malware samples: a current, “in-the-wild” set of
Samples in both sets were obtained from open and private sources and were collected via direct download. The priority in assembling the sample sets was to maximize the number of current, lethal viruses included. Samples were not collected via download from Internet-based email because Internet-based email is usually encrypted with HTTPS by a third-party server. If a security appliance does not possess the server certificate, it cannot examine the payload.

Initially, baseline testing was conducted using each malware sample set. All security functionality on the SWG-12600 was disabled. No samples in each set were blocked.

For actual testing, antivirus functionality was enabled to block malware.

The SWG-12600 made the best performances observed to date, a blocking rate of 90.3% against the current, "in-the-wild" set and 81.8% against the legacy set.

A comparison of the blocking rate of the SWG-12600 and the Industry Average for the current, "in-the-wild" set is shown in Figure 4. The comparison for the legacy set is shown in Figure 5.

**Application Control**

Testing assessed the ability of the SWG-12600 to block applications and the traffic created by them.

Web 2.0 applications are increasingly used to enable the dynamic relationships 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, may detract from employee productivity and expose the enterprise network to malware, increasing the probability of compromising the network and even causing the loss of valuable company data.

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

The SWG-12600 had the latest Application Control library, which consists of more than 5,700 applications and more than 300,000 social networking widgets.

**Figure 4: Check Point SWG-12600 Blocking, Current, “in-the-Wild” Malware**

<table>
<thead>
<tr>
<th>Percentage Blocked (%)</th>
<th>Check Point SWG-12600</th>
<th>Industry Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>90.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>68.4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Miercom Web Security Industry Assessment, February 2014

**Figure 5: Check Point SWG-12600 Blocking, Legacy Malware**

<table>
<thead>
<tr>
<th>Percentage Blocked (%)</th>
<th>Check Point SWG-12600</th>
<th>Industry Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>81.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>58.2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Miercom Web Security Industry Assessment, February 2014
The Check Point SWG-12600 has a comprehensive, intuitive interface for creating policies and rules. Multiple rule sets can be mixed and matched to provide security control for different ports and networks. The high level of granularity available in the interface can cover just about any network security deployment. This view of the Check Point SmartDashboard shows utilization of R77.10 firmware.

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.

Figure 6 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.

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. As shown in Figure 7 on page 5, 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.

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 8 on page 5.

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.

An RFC 2544 throughput test was conducted while URL filtering was in progress against Gambling URLs. The SWG-12600 maintained 1GE (port line rate) with zero frame loss.

Also, a simulated DoS flood attack was launched in an attempt to overburden the resources of the
The SWG-12600 continued to block Gambling URLs. No anomalies were observed. The SWG-12600 continued to block Gambling URLs.

**Bottom Line**

Comprehensive, hands-on testing of the Check Point SWG-12600 Secure Web Gateway was conducted as part of ongoing standardized testing of Web control, the Miercom Web Security Industry Assessment 2014.

The SWG-12600 had strong results in areas that are crucial for a Secure Web Gateway: classification of URLs into malicious and potentially malicious categories, URL filtering, malware blocking and application control.

The SWG-12600 has a large, ever-growing Application Control library of applications and web widgets available. The library and the high level of granularity that can be built into security policies enable the SWG-12600 to provide excellent protection from new, emerging threats.

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

**Figure 7: Check Point SWG-12600 Blocking Options for Facebook**

![Check Point SWG-12600 Blocking Options for Facebook](image)

Source: Miercom Web Security Industry Assessment, February 2014

*The check mark indicates that users are blocked from using Facebook-chat. Each of the 23 portions of Facebook has a risk rating, which is visible along with a description in the right pane.*

**Figure 8: Check Point SWG-12600 Blocking Rate, URL Filtering Disabled/Enabled**

![Check Point SWG-12600 Blocking Rate, URL Filtering Disabled/Enabled](image)

Source: Miercom Web Security Industry Assessment, February 2014

*With URL filtering enabled, the blocking rate of the SWG-12600 improved by over 5%.**
How We Did It

The Check Point SWG-12600 Secure Web Gateway, running firmware version R77.10, was evaluated using a Miercom client, Spirent Studio Performance application traffic simulator, BreakingPoint FireStorm and Ixia XM12.

The Industry Averages in this report are the result of validated, ongoing testing of comparable security products from Blue Coat, Check Point, Cisco, FireEye, McAfee, Palo Alto Networks, Symantec, Websense and other leading vendors.

URL Coverage Classification Accuracy  The URL of each of the one million most popular websites, based on worldwide traffic rating, was obtained in January 2014. The cache of the SWG-12600 was adjusted to allow processing of the URLs in runs of 100,000.

URL Filtering by Specific Category  For each category of potentially malicious and malicious URLs, a database was created in Excel.

Malware Blocking/Current, in-the-Wild and Legacy Samples  The SWG-12600 was deployed in Normal Mode, the default setting. It was connected to a Dell S6000 switch linked to a Linux server, a Dell PowerEdge 1950, that hosted the current, "in-the-wild" and legacy malware sample sets. Apache JMeter client residing on the Test Client, a Dell Latitude 6430u laptop, requested each malware sample housed on the Dell PowerEdge 1950 server.

Malware samples were obtained from open source listings as well as private, proprietary sources. Open sources included Maliciousbytes, EPP.com, virustotal.com, virussign.com, cramit.com and contagiodump.blogspot.com.

Application Control  Spirent Studio Performance software running on a Miercom server managed a Spirent Studio Security application simulator, which generated application traffic on the test network.

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 users who want to recreate them, with the appropriate test and measurement equipment. Those interested in repeating these tests are advised to contact Miercom at reviews@miercom.com for more details on the configurations applied in this testing. A Miercom professional services sales representative can provide assistance.
Miercom Performance Verified

The performance of the Check Point SWG-12600 in areas that are crucial for a Secure Web Gateway was verified by Miercom in a hands-on testing evaluation.

The SWG-12600 proved to be superior in identifying and classifying URLs into known categories, utilizing URL filtering, blocking malware and enforcing application control policies.

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, NoJitter, Communications News, xchange Magazine, 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.