Solution Brief

Top 10 Advantages of a Proxy Deployment in Conjunction with a Next-Generation Firewall

Complementary Solutions Provide the Best Layered Defense

As the threat landscape continues to evolve and grow, a layered defense strategy becomes even more important. In the changing landscape, many Next-Generation Firewall (NGFW) vendors such as Palo Alto Networks, CheckPoint, Fortinet, Cisco, and Juniper, claim that their NGFW products can replace a web proxy provided by secure web gateway (SWG) solutions.

While NGFW solutions do provide value to enterprises, they do not replace SWG technology. The following list illustrates the importance of continuing to deploy Symantec Blue Coat ProxySG to **complement** NGFW solutions.

1 Purposefully Engineered to Enhance Security Posture

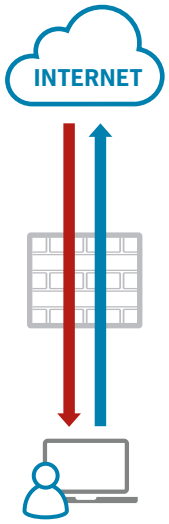
From an architecture perspective, NGFW simply repackages traditional firewall technology and incorporates some advanced firewall features, making it less secure than the full proxy architecture used by ProxySG. NGFWs use stream-based detection methodologies, examining the traffic as it streams by. This means that the firewall can only see a fleeting portion of malware at any given time, making it possible for malware to be delivered in many segmented pieces. Conversely, ProxySG waits for an entire object to be reassembled and scanned before allowing it to be delivered.

Symantec recently conducted testing using the **HTTP Evader** test site, which resulted in the leading NGFW allowing a significant percentage of successful evasions (121 evasions—nearly 16 percent of the total number of attacks), failing the test. It is important to note that these evasion techniques are well known, and have been successfully deployed against other inline devices like intrusion detection systems (IDS), intrusion prevention systems (IPS), and unified threat management (UTM) for many years.

For more information on how web proxy, in conjunction with NGFW, enhances your security posture, contact your sales representative for a copy of the technical brief, “Proxy Evasion Testing”.

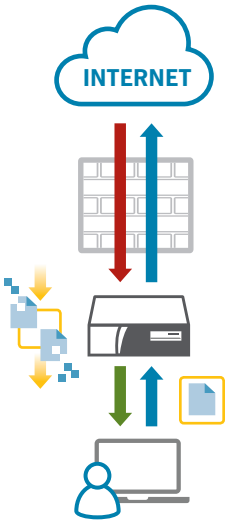
Figure 1. Why a Proxy-Based Secure Web Gateway is a Better Choice

Next-Generation Firewall or other stream-based security device



- No termination
- Stream scanning only

Next-Generation Firewall with Web Proxy



- Session termination
- Policy enforcement
- Web proxy

Symantec

2 Cloud Application Access Visibility and Controls That Exceed NGFWs

Using cloud applications has many benefits. However, security and data privacy professionals are challenged to provide security and governance for those cloud applications. The ProxySG is integrated with the Symantec cloud access security broker (CASB), providing extensive insight and controls over cloud applications used in the enterprise. The CASB Audit AppFeed integration provides visibility into more than 21,000 applications. With Audit AppFeed, administrators can see all sanctioned and unsanctioned applications being accessed via continuous analysis and reports. This visibility enables implementation of granular policies to control application use on the ProxySG. These granular policies can be based on application names and/or attributes. One of these attributes is the Business Readiness Rating (BRR). The BRR assigns a rating (from 1-100) to each application based on 70+ security attributes. The higher the score, the lower the risk. For example, it is possible to implement a policy to block all applications with a BRR score below 65.

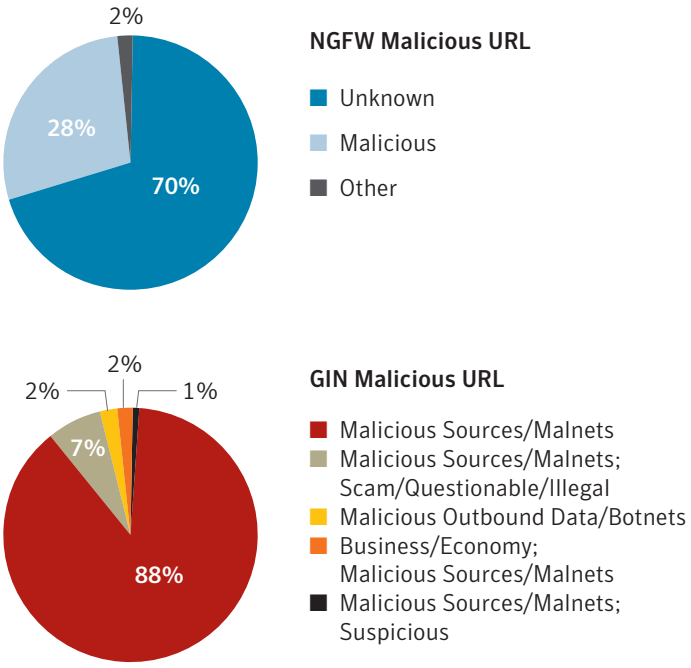
The Symantec Audit AppFeed capability helps IT and security professionals monitor and limit usage of sanctioned and unsanctioned applications through the ProxySG.

3 Global Intelligence Network Offers Superior Protection

Symantec has more than 20 years of experience in web protection technology—longer than many NGFW vendors have been selling their products. But in order to protect against malicious traffic, one first has to see it. Symantec gathers intelligence on emerging threats from more than 175 million users, and by processing more than four billion requests per day. This provides a level of visibility unmatched by the leading NGFW vendors. In an internal test, Symantec tested more than 200 malicious URLs and passed them through both Blue Coat ProxySG and the leading NGFW. While ProxySG blocked all of the URLs, the NGFW had significant issues. These included:

- Only 28 percent (60 URLs) were classified by the NGFW as malicious
- 70 percent (151 URLs) were classified by the NGFW as unknown—a significant amount of malicious content allowed on to the network by the NGFW
- Two percent (6 URLs) were classified as adult, phishing, web ad, and web hosting
- There were several serious misclassifications on the part of the NGFW: some sites classified as web advertising and web hosting sites were actually malicious and would not be blocked by even the most diligent firewall administrator.

Figure 2. Malicious URL Categorization: Leading NGFW and GIN



Furthermore, Symantec's dynamic real-time rating (DRTR) can uniquely identify and categorize never-seen-before URLs, eliminating the blind spots associated with zero-day attacks that most traditional URL filtering vendors face.

The Symantec Global Intelligence Network provides pertinent, near real-time information to the ProxySG, allowing it to identify and block the latest malicious contents.

4 The Most Flexible Categorization Engine on the Market

The ProxySG categorization can assign up to four categories to each URL allowing policies to be precisely set to match an organization's granular security policy. This is especially important with social media, where the website can have different content that caters to different user groups.

Table 1. URL Category Comparison

URL	Symantec GIN	NGFW
linkedin.com	Business/ Economy; Social Networking	Social Networking
linkedin.com/messaging	Business/ Economy; Email; Social Networking	Social Networking
facebook.com	Social Networking	Social Networking
facebook.com/games	Social Networking; Games	Social Networking
espn.com	Sports/Recreation	Sports
espn.com/watchespn	Sports/ Recreation; TV/ Video Streams	Sports
imgur.com	Media Sharing; Mixed Content/ Potentially Adult	Online Storage and Backup
imgur.com/r/nsfw	Pornography	Adult
imgur.com/r/gonewildcurvy	Pornography; Media Sharing	Adult
twitter.com	Social Networking	Social Networking
twitter.com/pornhub	Social Networking; Pornography	Social Networking

With ProxySG, popular websites can be assigned multiple categories. For example, LinkedIn.com/messaging is assigned three categories by GIN. However, the leading NGFW vendor categorizes this domain into just one category, and even incorrectly categorizes one of the Twitter sites, making it hard to block when inappropriate material is encountered.

When comparing classification of typical network traffic, the leading NGFW classified 52.8 percent of network traffic as "computer and internet info.," which does not provide enough granularity and visibility. The same traffic, analyzed by the Symantec GIN, resulted in a more granular categorization, allowing for improved monitoring and control policies for GIN users.

Table 2. URL Site Review for Checking and Validating URL Categorization

Vendor	URL Site Review
Symantec	sitereview.bluecoat.com/sitereview.jsp
BrightCloud	brightcloud.com/tools/url-ip-lookup.php
Cisco	senderbase.org
Fortinet	fortiguard.com/static/webfiltering.html
Palo Alto	urlfiltering.paloaltonetworks.com/testASite.aspx

Validation of the multiple categorizations of the URLs in Table 1, as well as URLs used for other popular websites, is accomplished using various site review links.

5 Next-Generation Firewall Performance Numbers Are Often Misleading

Next-Generation Firewall (NGFW) performance numbers are usually function specific. And while it is common for NGFW vendors to specify the throughput for firewall, threat protection, and VPN functionalities separately, they are individual, best case numbers. Consequently, these functional numbers tend to decrease once the user activates firewall and threat protection in parallel. For example, during a recent test, NSS labs reported that "*The Palo Alto Networks PA-7050 is rated by NSS at 42,324 Mbps, which is lower than the claimed performance; Palo Alto Networks rates this device at 60 Gbps.*" This is a far cry from the 120 Gbps total throughput that Palo Alto is officially advertising as its 7050 model's firewall throughput.

Because overall performance is generally a key selling point of NGFWs, it is important to distinguish data-sheet performance numbers from the actual performance of the appliance in a real-world environment. Past 3rd party testing has shown that when multiple features, including SSL inspection, are enabled the leading NGFW's performance is severely impacted. Overall performance is degraded more than 80%.

6 Unique Web Content Caching Saves Significant Bandwidth

A unique benefit of the ProxySG is that it sits between the source and destination. It intercepts and inspects the traffic by terminating the application session and then it reinitiates the connection to the target destination. The proxy acts on behalf of the client and can see the full content, allowing it to cache the most frequently requested content. This caching technology, provided through CachePulse, helps to accelerate the delivery of rich Web 2.0 content, video, and large files such as YouTube videos, Netflix streaming media, and Microsoft Windows updates.

CachePulse technology also tracks the ever-changing web, so as new sites emerge or popular sites change how they deliver content, new caching rules and instruction updates are automatically delivered from the CachePulse cloud to the appliance.

An analysis of this technology showed an average bandwidth reduction of up to 50 percent—with additional savings realized via numerous TCP and application-layer efficiencies that cannot be deployed by next-generation firewalls.

7 Highly Flexible and Granular Policy Controls

The ability to craft policies (Visual Policy Manger [VPM] or Content Policy Language [CPL]) based upon potential variables is a hallmark of the ProxySG solution. Access may be granted, restricted, redirected, rate limited, and more based upon hundreds of variables and tens of thousands of combinations. Examples include restricting unpatched or unsupported browsers (including legacy versions), unpatched or unsupported operating systems (including legacy versions), specific SSL/TLS versions, and cipher-suites.

8 An Open Architecture Platform

Symantec's best-of-breed technologies and open architecture enable easy integration with complementary security solutions. These include solutions such as the Big Data Security Analytics Platform, SSL Visibility, Data Loss Prevention, and Encrypted Traffic Management, as well as numerous third-party products. Leading NGFWs lack this level of openness and ecosystem integration, limiting deployment options to in-house anti-malware engines, web filtering, and sandboxing.

9 True User Authentication Flexibility

The ProxySG supports a wide range of authentication mechanisms that can accommodate many different existing environments. The flexible authentication architecture can use the following services: IWA, LDAP, RADIUS, local, client certificate, sequences, CA eTrust SiteMinder, Oracle COREid, policy substitution, SAML, Windows SSO, and Novell SSO. This versatility allows for a comprehensive authentication of users in your network. Several other vendors, such as Fortinet and Palo Alto Networks, are limited to AAA, local, LDAP, RADIUS, Kerberos, and TACACS+.

Furthermore, ProxySG offers true authentication, in which each user and new TCP connection are challenged to authenticate for access. Some of the leading NGFW vendors use a method known as user identification, in which a user is associated with an IP address and communication from that address is assumed to come from that user. This technique is not effective against multiuser environments, and is susceptible to basic techniques like IP hijacking.

10 Native Application Visibility and Control Exceeds the Leading NGFW Vendor

The ProxySG can natively classify more than 13,000 of the most-used web applications and provide 24 different granular application controls. Palo Alto Networks and Fortinet, on the other hand, support only 2354 and 2337 applications respectively—just a fraction of what is supported by ProxySG. A complete list of supported applications is available with the ProxySG solution.

Both the ProxySG and NGFWs allow an administrator to precisely define control policies in order to eliminate false positive events. For example, an administrator can block the download of audio files from iTunes while allowing books to be downloaded from the same site. However, with a ratio of 5:1 application visibility advantage, the Symantec Blue Coat ProxySG has a significant advantage over popular NGFW solutions. For example, while both ProxySG and leading NGFWs can control video downloads from popular websites (Facebook and Google), only ProxySG can recognize and control downloads from sites like Twitch.tv and StupidVideos, natively. This level of application visibility and control is not available in current NGFW solutions.

Deploy a Defense-in-Depth, Layered Strategy

In the fast moving web environment, where hackers frequently change their tactics, a defense-in-depth strategy of deploying the ProxySG in conjunction with an NGFW is essential for providing optimal protection. The ProxySG is engineered to withstand evasion techniques, making it a perfect complement to your NGFW. Its leading web-proxy technology identifies and blocks malicious web content, and its open architecture allows integration with best-of-breed products for an enhanced security posture.

These top 10 advantages represent just a few of the reasons why SWG and NGFW technologies are complementary in nature and why enterprises should implement them together for a layered defense against advanced attacks and targeted threats.

Contact your sales representative for more information on ProxySG and how it can enhance your security posture. Or visit our Advanced Web and Cloud Security website for more information.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec Corporation World Headquarters

350 Ellis Street

Mountain View, CA 94043 USA

+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com