Security
Empowers
Business

TOP 10 REASONS TO DEPLOY BLUE COAT PROXYSG IN CONJUNCTION WITH NEXT GEN FIREWALL TECHNOLOGY

SECURITY INSIGHTS BRIEF

The Threat Landscape is Evolving. So Should Your Defenses.

New technologies – and new threats – are causing major changes in security defense strategies and technologies. One of these changes is the introduction of the Next Gen Firewall (NGFW) technology by several vendors including Palo Alto, Check Point, Fortinet, and Juniper. Several of these vendors have claimed that their NGFW products can replace web filtering provided by Secure Web Gateway (SWG) solutions. While NGFW solutions undoubtedly provide an important value to enterprises and organizations, they do ***not*** replace the traditional SWG technology that is already in use. Here are 10 important reasons to deploy Blue Coat ProxySG appliances ***to complement*** NGFW solutions.

Top 10 Reasons to Deploy ProxySG with NGFW Solutions

1 Secure Web Gateway and NGFW Technologies Serve Different Purposes

The 2014 edition of the Gartner Magic Quadrant for Secure Web Gateways (SWG)[1] once again named Blue Coat a leader. Currently, there are no NGFW vendors named to this quadrant. Similarly, there are no SWG solutions named in the 2014 Gartner Magic Quadrant for Enterprise Network Firewalls.

All leading analyst firms currently distinguish NGFW from SWG, recognizing both as discrete security technologies with separate markets. Although NGFWs collapse stateful firewall and intrusion prevention into a single solution, leading analysts do not suggest that NGFWs replace or perform the functions of a leading SWG, such as Blue Coat's ProxySG.

Talking to leading analysts, we have surmised they do not expect the two technologies to overlap anytime soon.

[1] Gartner Magic Quadrant for Secure Web Gateways, Lawrence Orans, Peter Firstbrook, 23 June 2014.

2 Blue Coat WebPulse Offers Superior Capabilities Not Provided by NGFW

Blue Coat has more than 10 years of experience in web filtering technology. This is longer than many NGFW vendors have been selling their solutions. In order to protect against malicious traffic, one first has to see it. Blue Coat gathers intelligence on emerging threats from over 75 million users, and by processing more than 1 billion requests per day. This provides a level of visibility that is unmatched by the leading NGFW vendor. Blue Coat's own testing identified the top 125 malicious URLs and passed them through both the Blue Coat Secure Web Gateway and the leading NGFW. While Blue Coat flagged all the URLs, the NGFW had significant issues. These included:

- **76 URLs were classified by the NGFW as 'Unknown'.** This means 61% of the bad sites would not even be classified by the NGFW technology.
- **Only 5 URLs were identified as malware**, meaning the other 95% could potentially get through.
- **There were several serious mis-classifications on the part of the NGFW.** Some sites were classified as Search Engine, or Personal Site. These URLs would not be blocked by even the most diligent firewall admin.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Security
Empowers
Business

3 Blue Coat Offers the Most Flexible Categorization Engine on the Market

Blue Coat's categorization engine is capable of assigning up to four categories to each URL. This allows policies to be set surgically 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.

Take Tumblr as an example. The leading NGFW vendor categorizes this domain as a personal and blog site. In reality, this site contains various content types – some of which can be offensive to users as shown in the following table.

URL	BLUE COAT WEBFILTER (multiple categories, comma-separated)	LEADING NGFW
TUMBLR.COM	Mixed Content/Potentially Adult, Web Hosting	Personal Sites and Blogs
NUDE-SELF-PICS.TUMBLR.COM	Pornography	Personal Sites and Blogs
KEEP-CALM-AND-GET-NAKED.TUMBLR.COM	Pornography, Mixed Content/Potentially Adult	Personal Sites and Blogs
REALAMATURESEX.TUMBLR.COM	Pornography	Personal Sites and Blogs
PPJ4222.TUMBLR.COM	Pornography, Mixed Content/Potentially Adult	Personal Sites and Blogs
POSTNAKEDANONYMOUS.TUMBLR.COM	Pornography, Mixed Content/Potentially Adult	Personal Sites and Blogs

This problem, however, is not unique to Tumblr. One can find similar mis-categorizations with other sites such as Imgur:

WWW.IMGUR.COM	Mixed Content/Potentially Adult	Online Storage and Backup
IMGUR.COM/R/REALGIRLS/IKX8D	Pornography, Mixed Content/Potentially Adult	Online Storage and Backup
IMGUR.COM/R/NUDE	Pornography	Online Storage and Backup
IMGUR.COM/R/FEMALESGONEWILD/9C9EU	Pornography	Online Storage and Backup

Sites like ESPN contain both Sports and Audio/Video content. It is not unusual for organizations to allow Sports-related content, while blocking Video/Audio content.

ESPN.GO.COM/	Sports/Recreation	Sports
ESPN.GO.COM/VIDEO/CLIP?ID=ESPN:11167016	Sports/Recreation, Audio/Video Clips	Sports
ESPN.GO.COM/VIDEO/CLIP?ID=ESPN:11168788	Sports/Recreation, Audio/Video Clips	Sports

With the leading NGFW, it would be impossible to easily block sections of these sites while allowing access to the rest of them.

4 Blue Coat Offers More Granular Categorization at the URL Level

In addition to a better categorization engine, Blue Coat ProxySG categorizes URLs, while the leading NGFW vendors tend to categorize only domains. The Blue Coat approach enables users to activate more granular policies that allow IT security teams and administrators to block only malicious content while providing access to the larger site.

Imagine what happens if malicious content is found on a major site like Microsoft or CNN. With the leading NGFW, the full site needs to be blocked, whereas ProxySG can block the single URL, while granting access to the rest of the site.

5 NGFW Performance Numbers Can be Misleading

NGFW performance numbers tend to be function-specific. While it is common for NGFW vendors to specify the throughput for firewall, threat protection, and VPN functionalities separately, these are individual, best-case numbers. Consequently, these numbers would certainly decrease once the user activates firewall ***and*** threat protection in parallel, for example.

It is important to distinguish this from the actual performance of the appliance in a real-world environment, as overall performance is generally a key selling point of NGFW solutions.

6 NGFWs Achieve Impressive Numbers By Foregoing Critical Security Measures

NGFWs are designed to allow traffic through the device in order to properly categorize the application, an approach that *Network World* stated “could easily result in unintended consequences and insecure configurations – a valid concern” during their **Clear Choice** test.

The Blue Coat ProxySG solution, on the other hand, is a true proxy – it can terminate connections and forward the content in a newly established connection. This means ProxySG can view the full payload object before making a decision about it, thereby eliminating the possibility of forwarding malicious content before categorizing the content. This is a major differentiator, as there are known attacks where TCP packets are sent in small chunks and out of order to fool any potential in-line IPS/DPI devices. These packets would be reassembled at the other end and would look legitimate to the client side. Because a proxy reassembles the packets before forwarding it, it is not vulnerable to this type of attack.

Additional advantages of using Blue Coat ProxySG to close security gaps include the following:

- Unlike the leading NGFW vendor, ProxySG provides true user authentication, as opposed to simply identifying users against Active Directory. This capability enables administrators to apply user-based policies more confidently. The result is significantly simpler security policy creation and enforcement.
- Some leading NGFWs employ user identification that attempts to assign IP addresses to users. This approach can easily be bypassed if a user moves to a new machine, asks for a new IP address, or hides behind a network using Network Address Translation (NAT). Furthermore, this approach makes it impossible to distinguish between system activity and user activity. This can also make it difficult to distinguish between multiple users on the same system, making the identification process virtually worthless.
- Full proxy capabilities also provide the ability to do things like Internet Content Adaptation Protocol (ICAP), Dynamic Real-Time Rating (DRTR), JavaScript Defanging and other types of content-transformation. TCP stream devices like NGFWs simply cannot do this.
- Furthermore, a full proxy solution can perform deep packet inspection and examine large attachments through integration with ProxyAV and Content Analysis System products; a fact that a stream-based solution is not capable of handling due to its lack of simultaneous visibility into the full payload.

7 Blue Coat’s Unique Web Content Caching Technology Saves Customers Significant Bandwidth

Through the use of CachePulse technology, ProxySG customers regularly pull rule updates that allow them to bypass the anti-caching methods deployed by content providers. Using this technology, Blue Coat customers have realized HTTP bandwidth reductions of up to 65 percent – with additional savings realized via numerous TCP and application layer efficiencies that cannot be deployed by next generation firewalls.

Security
Empowers
Business

8 Blue Coat's Stream Splitting Technology Enables ProxySG to Request High-Volume Data Streams Once – While Forwarding to Multiple Requestors

Roughly 95% of all streaming content on the web today can be positively affected by the stream splitting technology on ProxySG appliances. As more requests for the stream are made, more bandwidth savings are realized. For example, two users requesting the same stream can result in a 50% bandwidth savings, while 1,000 users requesting the same stream (CSPAN, World Cup Finals, Final Four, etc.) can result in 99.99% bandwidth savings. While this technology is certainly a significant advantage for externally hosted streaming services, it also enables organizations to deliver mass communications via online streaming – without the network congestion issues or the complexity inherent in traditional multicast solutions.

9 Blue Coat Offers Highly Flexible and Granular Policy Controls

The ability to craft policy based upon hundreds of potential variables is a hallmark of the Blue Coat ProxySG solution. Access may be granted, restricted, redirected, rate limited, and more based upon hundreds of potential 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.

10 ProxySG Secure Web Gateway is Based on an Open Architecture Platform

Blue Coat's best-of-breed approach and open architecture enables easy integration with complementary security solutions. These include solutions such as the Big Data Security Analytics Platform, SSL Visibility and Encrypted Traffic Management solution, as well as numerous third-party products. Leading NGFWs lack this level of openness and ecosystem integration.

We believe these represent just a few of the top reasons why NGFW and Secure Web Gateway technologies are complimentary in nature – and should work together to provide a layered defense against advanced attacks and threats targeting organizations. Neither technology by itself is sufficient to fully protect an organization.

Learn More

Blue Coat stands ready to assist you with additional evaluation criteria, answers to your specific questions about ProxySG appliances, or a demonstration of the capabilities outlined above.

Learn more about Blue Coat's market-leading Secure Web Gateway by visiting www.bluecoat.com/products/proxysg.

Blue Coat Systems Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA
+1.408.220.2200

EMEA Headquarters
Hampshire, UK
+44.1252.554600

APAC Headquarters
Singapore
+65.6826.7000