

Secure Web Gateway Virtual Appliance

2nd Generation

Symantec Secure Web Gateway Virtual Appliance combines the unparalleled security capabilities of ProxySG with the flexibility of virtualization. Together, they create a truly scalable virtual Secure Web Gateway appliance for the data center. A pillar of Symantec’s Integrated Cyber Defense, Secure Web Gateway Virtual Appliance allows strong web security and enables corporate and regulatory compliance. The use of virtual infrastructure on a common platform reduces costs and IT resources.

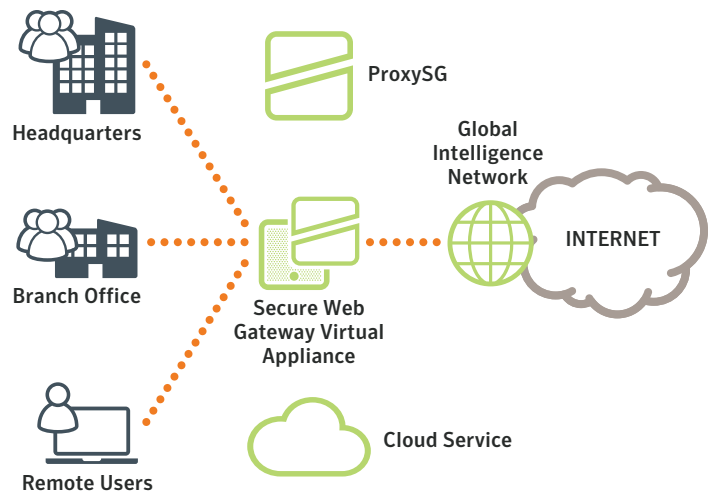
Web Security and Control

Enterprises struggle to cope with the increasing volume and innovation of web threats. The rapid adoption of mobile and new cloud applications compounds the problem as social networking, content streaming, blogs, media downloads, and other cloud-based apps are all prime targets of sophisticated malware.

Branch offices add another layer of vulnerability. Reduced on-site IT staff, offices dispersed around the globe, time zone differences, and shipping logistics are just a few of the issues that create security gaps that malware can exploit.

The Symantec Unified Security Solution offers organization-spanning web security, protecting users wherever they work. Secure Web Gateway Virtual Appliance extends ProxySG’s rich policy controls, allowing enterprises to fully protect their virtual environments. It centralizes reporting and visibility across all users, while consolidating management through the Symantec Management Center.

Secure Web Gateway Virtual Appliance makes use of the same Symantec Intelligence Services as the ProxySG. Backed by the Symantec Global Intelligence Network, customers receive a uniform level of high security, anywhere—at corporate headquarters, through virtual appliances at remote offices, or cloud services for field workers. Multi-dimensional categories, granular application controls, and the world’s most sophisticated civilian threat intelligence secure every user against the latest malware.



Secure Web Gateway Virtual Appliance solution can be deployed together with other products within the Symantec Unified Security Solution. The Global Intelligence Network powers all Symantec Security Products (ProxySG, Virtual Appliance and Cloud).

Advanced Threat Protection

For years, zero-day defense was considered to be the best security available. While safeguards against zero-day events can react extremely quickly to malware attacks, they still must wait for an attack to launch before acting on it. Distributed enterprises are particularly at risk since an attack at one branch office can quickly spread across the entire network.

Symantec has eclipsed zero-day defense with Negative-Day Defense. At any given time, the Global Intelligence Network monitors over 1,500 sources identified as attack and malware

launchers. By perpetually monitoring the source of two-thirds of all malware, Symantec pinpoints suspicious behavior and thwarts attacks at their origin. With Negative-Day Defense, Symantec defends against malicious attacks before they ever launch.

Secure Web Gateway Virtual Appliance also integrates seamlessly with the advanced threat capabilities of Symantec Content Analysis. Content Analysis offers hash reputation, file inspection—including dual anti-malware/anti-virus engines—predictive analysis, and dynamic sandbox brokering and integration.

Simple Deployment

Deploying physical security appliances is a challenge at remote offices with little space or onsite IT support. Not only do appliances take up highly valuable space, administrators must also learn how to integrate them.

Secure Web Gateway Virtual Appliance greatly simplifies application of the Secure Web Gateway, enabling hardware consolidation and alleviating IT administrative overhead. Running on VMWare ESX and ESXi, it shares the same server hardware with other virtual appliances. A deployment that once took days are now completed in hours.

Optimize IT Resources

Many enterprises are doing more with less IT resource by reducing on-site staff at remote offices. Fewer administrators are available to handle remote tasks, including network security, network infrastructure, and endpoints/laptops.

With Secure Web Gateway Virtual Appliance, IT administrators can manage just an application, rather than the entire appliance. Now, once-complex and time-consuming tasks like installing new appliances to expand the network are accomplished with a simple license upgrade.

Accelerate Disaster Recovery

Instead of duplicating all network and security infrastructure for redundancy, enterprises use rapid support to provide business continuity for remote offices. Even so, logistics and overhead cause delays in migrating to a new system.

With Secure Web Gateway Virtual Appliance, you can quickly deploy Secure Web Gateway in case of disaster recovery, and use a backup image of the system.

Enterprise Technical Support

When managing multiple remote and branch locations, it is essential that your security administrator has access to qualified technical resources. Symantec Secure One Services extends 24/7 technical and online support, customer care, service options, training and professional services.

An experienced and certified technical support staff is available at six interconnected support centers worldwide to respond rapidly and solve support requests. Secure One service options protect your business via software updates and easier management of your business and IT operations. Symantec systems training and professional services provide customized consulting support to bring your administrator quickly up to speed.

SG VA 2nd Generation (SWG Edition)

License

Connections	500 to 250,000, depending on license
Upgrades	Available to any larger license
Duration	1 and 3 years

Required Hardware Specifications

CPU	1 core up to 16 cores depending on license
Memory	4GB up to 128GB depending on license
Virtual Disks	Minimum 1 to 8 virtual drives depending on license
Disk Capacity	Minimum 100 GB to 800 GB depending on license

Minimum Software Specifications

VMWare	ESX and ESXi version 5.x and 6.x
SGOS	SGOS 6.7
Amazon Web Services	c4.large or m4.large required
KVM	Cisco CSP, CentOS, RedHat, Ubuntu
Hyper-V	C1 and C2 support only

Performance

Throughput	100 Mbps up to 1.6 Gbps depending on license and memory configuration
------------	---

Support

SW Support	Included in User License
------------	--------------------------

Certification

VMWare	VMWare-certified
Federal Certification	Please contact: DL-BC-GROUP-Federal_Certifications@symantec.com

Maximum connections will vary with user licenses. Please refer to the sizing guide for details.



350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com