Secure Web Gateway: The Power of Proxy

Tim Balog, CISSP
Solution Engineer Manager
Federal Sales

June 13, 2018
Agenda

1. Symantec Today
2. Role of the Proxy
3. Symantec Secure Web Gateway (SWG)
4. SWG Platform
5. Web Security Service
6. SWG Integrations
7. Summary
Fiscal Crisis
The Industry Faces a Looming Fiscal Spending Crisis

$ SECURITY OPERATING COSTS

- Existing Technology Footprint
- Annual Security Improvement
- New Regulations
- Labor Cost Increases
- Subscription Expense Growth
- Maintaining a Dual Environment (Legacy and Cloud)

CURRENT SECURITY BUDGET

6-8% ANNUAL BUDGET INCREASE

6-8% ANNUAL BUDGET INCREASE
Symantec | At a Glance

- 175M endpoints under protection
- $5B+ FY18E revenue
- 2100+ patents
- Leader in 5 Gartner MQs (CASB, SWG, EPP, DLP and MSS)
- 350,000+ customers worldwide
- ~3,500+ company wide R&D
- 9 SOC threat response centers
- 9 Trillion telemetry points
Broad Portfolio of Cyber Security Solutions
Most recent published release from Gartner, Forrester Wave, and Radicati
Delivering Protection in The Cloud Generation

INTEGRATED CYBER DEFENSE PLATFORM

- **ENDPOINT**
  - Advanced Threat Prevention
  - Information Protection
  - Compliance Enforcement
  - Analytics
  - Encrypted Traffic Management

- **PROXY**

- **EMAIL**

- **CLOUD APPS**

- **THREAT RESEARCH**
  - Massive Global Threat Telemetry
  - State of The Art Security Analysis
  - Best-in-Class Global Cyberwarriors
  - Automated Threat Intel Fed to Platform

Copyright © 2018 Symantec Corporation SYMANTEC PROPRIETARY- LIMITED USE ONLY
Role of the Proxy
The Power of a Proxy in Security

proxy

noun  |  \prək-sə\n
: a person who is given the power or authority to do something (such as to vote) for someone else

: power or authority that is given to allow a person to act for someone else
How Proxies Work

1. Admin creates policy
   - Authentication
   - Authorization
   - Anti-virus scanning
   - Content filtering

2. Requests arrive at ProxySG

3. Policy processing engine decides whether to allow or deny or perform other actions

Client

Server

CPL

Visual Policy Manager

Admin
Effective Prevention

Proxy Architecture Compared to Next Gen Firewall

Malicious payload detected by content analysis, blocked from delivery

Malicious payload delivered to end user
Deployment options

• Physically inline

• Virtually inline

• Out-of-path
Symantec Secure Web Gateway
Symantec Secure Web Gateway

Symantec SWG Delivers:

- Negative Day Threat Defense
- Hybrid Delivery Model
- Strong User Authentication
- Visibility Into Encrypted Traffic
- Integration with ATPs Across Industry
- Control Over Web & Cloud Usage
- Performance & Reliability
- Accelerated Cloud App Performance
- Scalability & Lower TCO
ProxySG

Product Profile

Description
Physical or virtual appliance SWG solution delivering an advanced set of technologies working together to protect your organization in the cloud, across the web, social media, applications and mobile networks.

Differentiators
- Market leader (Gartner, Forrester, Radicati) for over a decade; 15K global enterprises depend on SG
- Cloud deployment for branch offices and remote users, centrally managed with Universal Policy
- Demonstrably superior results for threat prevention and information security/compliance
- Best in Class SSL inspection - received only “A” rating for secure inspection (recent 3rd party report)
- ICD outcomes – reduced effort to remediate threats between network and endpoint, improved

Key Customer Issues / Pain Points Solved

1. Web, cloud, mobile has all collapsed onto http/https, exposing NGFW limitations; need strong security control point to protect enterprise (threats and infosec)

2. Complicated web/cloud AUP enforcement and logging requirements to satisfy corporate, regulatory and data privacy mandates

3. SSL/TLS encryption “blind spots” creates vulnerabilities

4. Poor existing gateway threat prevention architecture leaves enterprise exposed to advanced threats

5. Use of unsanctioned cloud apps creates risk of loss of compliance sensitive data
Symantec is Named a Leader in 2017 Gartner Magic Quadrant for Secure Web Gateways: A Leader for the 10\textsuperscript{th} Time*

*This is a reflection of the Blue Coat (Now Symantec) ProxySG.

Source: Magic Quadrant for Secure Web Gateways, Lawrence Orans, Peter Firstbrook, 12 June 2017, Gartner, Inc.

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from Symantec. Gartner does not endorse any vendor, product or service depicted in our research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. 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.
Zscaler Weaknesses

- DLP, bandwidth control, Web 2.0 controls, and other advanced features are only available on higher-priced packages of the Zscaler Web Security solution.

- Zscaler no longer offers email security as part of its service portfolio, which may disappoint customers looking to source both web and email security from a single vendor.

- Zscaler offers a cloud-based firewall service as an add-on to its SWG service. The firewall service, however, is not intended as a replacement for enterprise firewalls or UTM appliances, it is primarily suitable for small businesses, branch offices, roaming laptops or kiosks.

- Zscaler customers have reported instances of performance degradation, which have affected user satisfaction with the solution.

- Zscaler customers reported scaling issues and faulty functioning of VPN functionality as affecting their deployments.
Proxy-based Secure Web Gateway

Critical Network Control Point for Security and Compliance

- Appliance (ProxySG, ASG)
- Virtual Appliance (VSWG, SG-VA)
- Web Security Service (WSS)

+ Symantec Intelligence Services (IS) or Symantec Web Filter (WF) subscriptions

Web Access Governance & Threat Protection

File Extraction & Orchestration Services (ATP, DLP)

Powerful, Open Policy Platform - In Cloud, On Prem, Virtual, AWS
## URL Threat Risk Levels

### Eliminate The Riskiest Traffic Without Over-Blocking

<table>
<thead>
<tr>
<th>Risk Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Level 10:</strong></td>
<td>solid evidence of malicious (rated in database)</td>
</tr>
<tr>
<td><strong>Risk Level 9:</strong></td>
<td>probably malicious</td>
</tr>
<tr>
<td><strong>Risk Level 8:</strong></td>
<td>stronger evidence of maliciousness</td>
</tr>
<tr>
<td><strong>Risk Level 7:</strong></td>
<td>shady behavior (including Spam, Scam, PUS, etc. but possibly malicious)</td>
</tr>
<tr>
<td><strong>Risk Level 6:</strong></td>
<td>exercise caution; very new sites, or some evidence of shady behavior</td>
</tr>
<tr>
<td><strong>Risk Level 5:</strong></td>
<td>may not be safe; no established history of normal behavior</td>
</tr>
<tr>
<td><strong>Risk Level 4:</strong></td>
<td>still probably safe (or starting to establish a history of normal behavior)</td>
</tr>
<tr>
<td><strong>Risk Level 3:</strong></td>
<td>probably Safe</td>
</tr>
<tr>
<td><strong>Risk Level 2:</strong></td>
<td>other top sites; consistently well-behaved</td>
</tr>
<tr>
<td><strong>Risk Level 1:</strong></td>
<td>big names; long history of good behavior; huge traffic</td>
</tr>
<tr>
<td><strong>Risk Level 0:</strong></td>
<td>Customer Whitelist</td>
</tr>
</tbody>
</table>

**Categorize and rank 1.2 billion of Web/URLs requests Per day**

**Provide granularity with 11 Risk Levels**

**Block 99.9% and over 50M malware threats daily**
Categories, Intelligence Services, and Threat Risk Levels

Blue Coat Category Descriptions

- Abortion
- Adult/Mature Content
- Alcohol
- Alternative Spirituality/Belief
- Art/Culture
- Auctions
- Audio/Video Clips
- Brokerage/Trading
- Business/Economy
- Charitable Organizations
- Chat (IM)/SMS
- Child Pornography
- Computer/Information Security
- Content Servers
- Controlled Substances
- Dynamic DNS Host
- E-Card/Invitations
- Education
- Email
- Entertainment

DATA FEED

- CONTENT CATEGORIES
- SECURITY CATEGORIES
- URL THREAT RISK LEVELS
- GEO LOCATION
- BASIC WEB APPLICATION
- CONTROLS

10 “Risk Levels”

Dozens of “Risk Groups”

Hundreds of “Risk Factors”
Discovered 430 million new unique pieces of malware last year

1B malicious emails stopped last year

228M social engineering scams blocked last year

23,000+ Cloud applications discovered and protected

40B web attacks blocked last year

1.1 Billion previously unseen web requests scanned daily

2 Billion emails scanned per day

175M Consumer and Enterprise endpoints protected

9 global threat response centers with 3500+ Researchers and Engineers
Secure Web Gateway

ProxySG and Advanced Secure Gateway

Proxy All Endpoints
- Terminate and decrypt traffic
- Emulate all device types
- Extract content for inspection
- Integrate authentication

Control Web & Cloud Governance
- Discover & control shadow IT risk
- Block web-borne threats
- Enforce access policy & audit usage of web & cloud

Prevent Threats & Orchestrate Content
- Pre-filter sandbox with advanced content inspection
- Send content to DLP, sandbox, analytics, etc.
- Open integration architecture to quickly add new services

Enhance the User Experience & Performance
- Video Acceleration and Split Tunneling
- Asymmetric Caching of Content
- Optimized Protocol Support
Proxy All Endpoints

Architecture for Content Extraction and Device Emulation

1. Authenticate Users
   - Integrate identity management

2. Terminate & Emulate
   - Secure all endpoint types

3. Decrypt Selectively
   - Privacy compliance

4. Extract Content
   - High Risk
   - Suspicious
   - Unsanctioned
   - Low Risk
   - Healthcare
   - Sanctioned

Proxy

Policy Select

Bypass

Decrypt

ICAP/s-ICAP Stream

Copyright ©2018 Symantec Corporation SYMANTEC PROPRIETARY-LIMITED USE ONLY
Control Web and Cloud Access

Access Governance and Policy Enforcement

- 21,000+ Cloud apps
- 60 attributes of risk and business readiness
- Drive Shadow IT control policy on Proxy/SWG

- 84 Total categories
- Across 55 languages
- Dynamic, real time rating

Cloud Access Security (CASB)

Web Threat Protection

- 12 Security categories to block 90% of all threats
- Malnet stop zero day exploits
- URL Threat Risk – increases security without over-block

Web App Firewall (WAF) & RP

- OWASP Top 10 application protections
- Dynamic intelligence to maximize cache

Global Intelligence Network

- OWASP Top 10 application protections
- Dynamic intelligence to maximize cache

Internet

Copyright ©2018 Symantec Corporation SYMANTEC PROPRIETARY-LIMITED USE ONLY
SWG Platform
Providing Advanced Threat Protection
The Cloud-Generation SWG Strategy

Build Superior Advanced Threat Protection

- Pre-filter & integrate sandboxing with Content Analysis (CA)
- Simplify ATP Architecture with Advanced Secure Gateway (ASG: Proxy + CA)
- Link malware detection and endpoint remediation (EDR) to simplify incident response
- Deploy an inline, active Web App Firewall to scale application protection
- Increase web security and simplify policy with URL Threat Risk

Move to Cloud Security  Scale True Hybrid Deployments  Decrypt SSL-TLS Responsibly
Passing files to other devices

**On Prem:**
- **ProxySG** – decrypt, extract content, send via iCAP
- **Content Analysis** – pre-filters files (dual AV, WL, predictive), API to (any) Sandbox
- **Malware Analysis** – targeted emulation / virtual detonation

**Cloud Service:**
- **Web Security Service** – cloud proxy
- **Malware Analysis Service** – cloud sandbox
Content Analysis / Malware Analysis (Sandboxing)

**Product Profile**

**Description**
Symantec Content Analysis leverages extensive threat intelligence and protects against advanced threats through file reputation matching, multiple anti-malware and analysis techniques, and sophisticated sandbox detonation.

**Differentiators**
- Multiple layers of threat inspection (Hash reputation, Advanced Machine Learning, Dual Antimalware engines)
- Adds centralized inspection to Proxy, SMG, SEP and ATP
- Dynamic, customizable sandboxing (Emulation/Virtualization) on-box or cloud
- Key reason Symantec is “Top Leader” in Radicati’s APT Protection Market Quadrant report

**Key Customer Issues / Pain Points Solved**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need centralized, sophisticated and customized inspection beyond Proxy, email, endpoint</td>
<td>Symantec Content Analysis leverages extensive threat intelligence and protects against advanced threats through file reputation matching, multiple anti-malware and analysis techniques, and sophisticated sandbox detonation.</td>
</tr>
<tr>
<td>Too many security tools and too many alarms lead to missed attacks and high costs</td>
<td>Add centralized inspection to Proxy, SMG, SEP and ATP</td>
</tr>
<tr>
<td>Have some inspection capability of “known” threats, need custom sandbox to find “unknowns”</td>
<td>Dynamic, customizable sandboxing (Emulation/Virtualization) on-box or cloud</td>
</tr>
<tr>
<td>I have FireEye, I need to improve accuracy and reduce the number of alerts and reduce cost</td>
<td>Key reason Symantec is “Top Leader” in Radicati’s APT Protection Market Quadrant report</td>
</tr>
</tbody>
</table>
Reducing the Incident Response Queue

ProxySG

Web Threats
URL Category & Risk Score

Content Analysis

Content Inspection & Orchestration

Whitelist/Blacklist Hash Reputation

Dual AV Malware Signature

Static File Analysis Malicious Character

Mal. Analysis

Behavioral Analysis Sandbox

Incident Response

SA/ATP: E
Content Analysis

Improve detection, reduce sandbox capacity requirements

- Decrypt SSL, ICAP documents to sandbox
- Block web-based threats, C&C traffic
- High availability, inline, active blocking
- Enables centralized sandboxing

Leverage proxy to feed the sandbox

Pre-filter sandbox with content analysis

- Analyzes content before delivery to sandbox via API
- Applies multiple AV engines, white list
- File code analysis with machine learning finds zero-day threats
Symantec Malware Analysis

Add Emulated and Virtualized Detonation to Battle Advanced Threats

Leverage proxy to feed the sandbox

- Decrypt SSL, ICAP documents to CA
- Block web-based threats, C&C traffic
- High availability, inline, active blocking
- Enables centralized sandboxing

Pre-filter sandbox with content analysis

- Analyzes content before delivery to sandbox via API
- Applies multiple AV engines, white list
- File code analysis with machine learning finds zero-day threats

Target sandbox detonation for faster results

- YOUR standard OS images
- Faster analysis, with lower required CPU/memory
- Work with proxy to delay delivery until cycle completes
Content & Malware Analysis

Thorough Inspection = Better Protection

Content Analysis

Hash Reputation
- Custom user whitelist/blacklist + Risk Scoring
- 5 Billion file reputation database

Dual Anti-Malware/Anti-Virus
- Combine Kaspersky, Sophos or McAfee
- Files up to 5GB / Signature updates every 5 minutes

Predictive File Analysis
- Static Code Analysis / Machine Learning
- Parse and collect files / Match code to 4B “bad”

Dynamic Sandboxing
- VM + Emulation Sandboxing using custom “Gold Images” Behavior and YARA rule analysis

Global Intelligence Network

Web / Mail Threat Protection
- URL Reputation
- SSL Decryption
- Categorization / policy
- Spam detection
- Real-time blocking

Additional Sandbox

Proxy/SMG

Passes acceptable files to user

Signatures evaluated for known bad

Analyzes code for malicious character

Detonates only truly unknown files
Dramatically Reduce Sandboxing Costs

50% Reduced Sandbox Cost

- Reduce sandbox capacity 75%
- Dramatically fewer samples to process
- Centralized architecture “pools” sandbox
- Lower capital acquisition costs

90+% Savings on Incident Response Costs

- 4x better detection
- Trusted inline proxy position
- Prevents malware delivery
- Dramatically reduced alarms
Advanced Secure Gateway - ASG

**Simplify Your ATP Architecture**

Advanced Secure Gateway (ASG)

Authenticate, Enforce, & Log
See and Control Shadow IT
Block Web Threats & ATP C&C

---

Unify Access
Governance

Extract &
Orchestrated Files

Decrypt SSL, extract documents
ICAP documents
Prevent delivery based on verdict
Stream decrypted data to forensics

---

Inspect Files to Prevent Malware & Advanced Threats

- Whitelist/blacklist
- Dual A/V Signatures
- Static Code Analysis
- Filtering Sandbox Broker

---

Copyright ©2018 Symantec Corporation SYMANTEC PROPRIETARY-LIMITED USE ONLY
Web Security Service
Proxy From the Cloud - For the Cloud
Web Security Service

Product Profile

Description
Complete advanced network security stack delivered as a cloud service, including SWG and firewall services, content analysis, sandboxing, web isolation, DLP, and CASB capabilities.

Differentiators
- Most complete set of advanced network security services (SWG, FW, DLP, ATP, Isolation, CASB, SD-WAN)
- Performance/Uptime/Accessibility of global network with simple connectivity (SEP redirect, SD-CC)
- Best in class threat prevention (A rated SSL inspection, better detection 10X few false positives (Tolly Report), Web Isolation, CASB controls)
- Best in class DLP (always top of MQs and Wave reports)

Key Customer Issues / Pain Points Solved

1. Poor user performance & increasing cost of backhauling internet network traffic
2. Operational complexity and capex acquisition costs of full network security stack
3. SSL/TLS encryption “blind spots” creates vulnerabilities
4. Poor existing gateway threat prevention architecture leaves enterprise exposed to advanced threats
5. Complexity of managing a hybrid gateway deployment
Adoption of Cloud App Challenges

How Do I Move to Cloud Security to...

▷ Protect my users from ubiquitous threats?
▷ Secure data & comply with legal regulations?
▷ Effectively manage new devices and mobile users?
▷ Transition to cloud speed while maintaining flexibility?

...With the capability, reliability, performance of on-prem security systems
Symantec Web Security Service

Enterprise Class Access Security

- Configure Universal Policy For True Hybrid
- Take Remote Sites Safely “Direct to Net”
- Extend Web & Cloud Governance to Mobile

Symantec Web Security Service (WSS)

- For Remote Sites, Mobile Users, & Data Centers
- Assure a Safe & Simple Migration to Cloud

Headquarters Data Center

Regional Office

Roaming Users

Copyright ©2018 Symantec Corporation SYMANTEC PROPRIETARY-LIMITED USE ONLY
Symantec Web Security Service

Full Security Stack in the Cloud

Cloud delivered ProxySG Secure Web Gateway
Set granular policies to control web usage

Symantec Web Security Service

Cloud-only or mixed model (cloud & HW)
Market-leading enterprise-class feature set

Unified Management (Cloud & Premise)

Malware Scanning & Analysis

Information Protection

CASB
SWG Integrations
Leveraging Proxy’s Central Role in Cyber Security
Using Integrations to Bridge Organizations

**Web Isolation**

**Discovery:** How are you securing your user’s web browsing? What about phishing attacks?

**SecOps/Incident Response**

**Integration:** SWG + WI selectively isolates risky sites, enforces full isolation for privileged users, and isolates embedded e-mail URLs

**Value:** Expands user’s web access and boosts productivity while eliminating complexity for NetOps (constant updates to policy)

**Content Analysis**

**Discovery:** How are you preventing threats from web doc downloads? How about addressing high False Positives?

**SecOps/Incident Response**

**Integration:** Content downloads through SWG are pre-filtered by CA (and optional MA Sandbox)

**Value:** Improve malware detection rates by 4X, reduce false positives by over 90%

**DLP**

**Discovery:** How do you enable the inspection of outbound content for DLP? What about securing data in cloud apps?

**Risk/Compliance**

**Integration:** SWG securely decrypts outbound content and hands to for DLP for analysis. SWG blocks transfer if policy violated

**Value:** Reduce data leakage/compliance violations

**SEP**

**Discovery:** How do you remediate threats on your endpoints that are 1st identified in the network?

**Endpoint - IT Infrastructure**

**Integration:** SWG+CA flags new threat to GIN, which is fed to SEPM, which immediately initiates the appropriate remediation response

**Value:** Improved security, reduced complexity and manual effort

**CASB**

**Discovery:** How do control access to cloud applications and manage “Shadow IT”?

**Cloud Services – IT Infrastructure**

**Integration:** CASB Audit & SWG logs reveal cloud app use, exposing potential risks. SWG policy can then enforce AUP for cloud apps

**Value:** Compliance enforcement & security for cloud apps and data
CASB - Cloud & Web Access Governance

Web Security Service Policy Integration

CASB Audit

App Rating Database

Analytics

Audit – AppFeed

Logs

GIN

PROXY

Symantec Web Security Service

Intelligence of 23,000+ Apps

Shadow IT Visibility

Scalable Proxy Policy to Control & Manage Risk

Roaming/Mobile Users

Offices
Web Security and Information Protection

Extend Data Loss Prevention (DLP) Coverage to Cloud, Mobile, & Branch Users

1. Remote users? Direct to Net Branches? Leverage Cloud DLP with WSS.
2. Using Cloud SaaS Apps? Use CASB with Cloud DLP.
3. Have on-premise DLP already in place? Use it. One policy, effective everywhere.
Integrate EDR with Gateway ATP Sandbox

Content Analysis with Symantec Endpoint Protection (SEP)

1. Content Analysis identifies potential threat using information from the Global Intelligence Network and sent to Symantec Endpoint Protection (SEP) Manager to verify

2. SEP Manager checks with endpoints to identify which are infected and responds to ProxySG

3. Remediation: blacklist communicated to
   - ProxySG / Content Analysis
   - SEP Manager
Summary
True Hybrid Security

Deploy to Match Your Needs

Private

Physical

ProxySG & ASG Appliances

Virtual Appliances

Universal Policy

Virtual

VSWG SWG VA

IaaS

AWS AMI

Public

SaaS

Services

Web Security Service
## ProxySG appliance models

<table>
<thead>
<tr>
<th>Model</th>
<th>S200</th>
<th>S400</th>
<th>S500</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>License Capacity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recommended Employee Count</td>
<td>500</td>
<td>1200</td>
<td>2600</td>
</tr>
<tr>
<td></td>
<td>5000</td>
<td>6000</td>
<td>14,000</td>
</tr>
<tr>
<td></td>
<td>25,000</td>
<td>30,000</td>
<td>50,000</td>
</tr>
<tr>
<td><strong>System</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Drives</td>
<td>500GB SATA</td>
<td>2 x 500GB SATA</td>
<td>2 x 500GB SATA</td>
</tr>
<tr>
<td></td>
<td>2 x 500GB SATA</td>
<td>3 x 1TB SAS</td>
<td>6 x 1TB SAS</td>
</tr>
<tr>
<td></td>
<td>8 x 1TB SAS</td>
<td>8 x 1TB SAS</td>
<td>16 x 1TB SAS</td>
</tr>
<tr>
<td>Boot Device</td>
<td>Single 16GB SSD</td>
<td>2 x 16GB SSD (dual redundant)</td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>6GB</td>
<td>8GB</td>
<td>16GB</td>
</tr>
<tr>
<td></td>
<td>16GB</td>
<td>24GB</td>
<td>32GB</td>
</tr>
<tr>
<td></td>
<td>64GB</td>
<td>128GB</td>
<td></td>
</tr>
<tr>
<td>Onboard Ports</td>
<td>(2) 1000Base-T Copper ports (with bypass)</td>
<td>(2) 1000Base-T Copper ports (non-bypass)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(1) 10/100Base-T Copper, BMC Management Port</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optional NICs</td>
<td>4x10/100/1000Base-T (Copper with bypass capability)</td>
<td>4x10GbE Fiber-SX (Copper with bypass capability, full height slot only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4x1GbE Fiber-LX (with bypass capability)</td>
<td>4x10GbE Fiber-SX (Copper with bypass capability, full height slot only)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4x1GbE Fiber-LX (with bypass capability)</td>
<td>4x10Gb Base-T (Copper with bypass capability)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2x10Gb Base-T (Copper non-bypass)</td>
<td>2x10Gb Base-T (Copper with bypass capability)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2x10Gb Fiber (SR with bypass capability)</td>
<td>2x10Gb Fiber (LR with bypass capability)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2x10Gb Fiber (SR with bypass capability)</td>
<td>2x10Gb Fiber (LR with bypass capability)</td>
<td></td>
</tr>
</tbody>
</table>
A Full Network Security Stack Delivered In the Cloud

**Web Security Service**

- **Information Protection**
  Enterprise grade DLP from Symantec or data orchestration to your preferred vendor

- **Advanced Threat Protection**
  Multiple antimalware inspection engines & sandbox, plus complete web isolation (Spring 18)

- **Secure SSL/TLS Decrypt to Enable Inspection**
  Strong cipher & protocol support doesn’t degrade security, with privacy compliant selective decrypt

- **Advanced User Authentication**
  User and group policy integrated with SYMC VIP and leading 3rd Identity Services

- **Complete Network Security and the Power of HTTP Proxy to Secure Access**
  Deep Proxy for Web, Mobile, & Cloud Applications

**High Availability, High Capacity Global Access Backbone That Accelerates User Performance**
New Virtual Appliances: GEN 2 SG VA’s

Scale to 1.6Gbps on Vmware ESX

- On-demand Proxy Capacity
- Forward Proxy and Reverse Proxy / WAF

<table>
<thead>
<tr>
<th></th>
<th>Gen 2 SWG VA</th>
<th>Gen 1 SWG VA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Max Throughput</strong></td>
<td>100M-1.6Gbps</td>
<td>100Mbps</td>
</tr>
<tr>
<td><strong>Max Conns</strong></td>
<td>250,000</td>
<td>10,000</td>
</tr>
<tr>
<td><strong>Pricing Base</strong></td>
<td>CPU-based pricing</td>
<td>Users</td>
</tr>
<tr>
<td><strong>Pricing Options</strong></td>
<td>1, 2, 4, 8, or 16 cores</td>
<td>25, 50, 100, 500, 1000, 2500 Users</td>
</tr>
<tr>
<td><strong>S, M, L Connection Capacity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BCWF/BCIS</strong></td>
<td>Not included</td>
<td>Included</td>
</tr>
<tr>
<td><strong>SKU Stub</strong></td>
<td>SG-VA-SE</td>
<td>VSWG</td>
</tr>
<tr>
<td><strong>Platforms</strong></td>
<td>ESX</td>
<td>ESX, Hyper-V, AWS</td>
</tr>
</tbody>
</table>
Seamless Hybrid with Universal Policy

- Simply Extend Policy to Cloud Web Security Service
- Consistent Policy for On-Prem, Mobile Users, Virtual
- Centralize Reporting, Admin, & Policy with Management Center
Management Center/Reporter

Product Profile

Description
Protects websites from the OWASP Top 10 threats blocking known attack patterns with both signature-based, and signature-less content nature detection engines.

Differentiators
- Symantec integrations offer reporting and management from a single pane-of-glass and enable Unified Threat Reporting combining multiple threat intelligence sources.
- Pre-built and custom reporting capabilities with advanced filtering and analysis tools
- Improves the scalability, security and cost effectiveness SYMC network protection deployments

Key Customer Issues / Pain Points Solved

1. Need to manage an increasingly complex, growing infrastructure with a fixed budget and no additional headcount

2. Need to improve the consistency of devices and policy, which can become fragmented with a growing stack and our move to the cloud

3. Increasing load on web and cloud traffic makes uptime of my security stack a mission critical requirement
Thanks.