

Content Security Gateway™ Series

Real-time Gateway Anti-Malware Appliances

TODAY'S MALWARE THREAT

Each year, the threat from viruses has grown larger¹. Moreover, spyware has emerged as a growing menace. Today's malware programs include viruses, worms, spyware, and other malicious software. They are used in mass attacks to disable or steal computing resources and in stealthy, targeted attacks to steal information. And they do so not only through email traffic but also through real-time web traffic. Malware programs are becoming more creative and sophisticated, making use of multiple components to attack in a blended way. It is now not unusual to combine traditional worms with new Trojan horse and backdoor spy programs. The internet has become a more dangerous place.

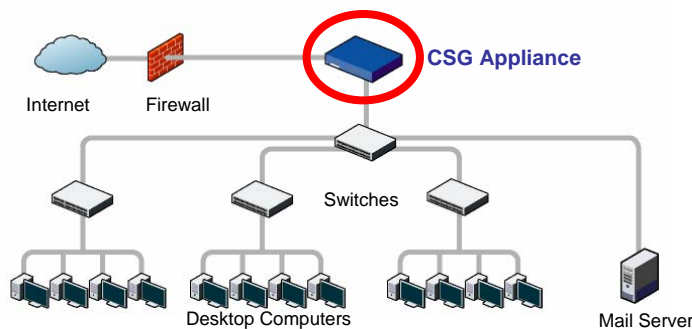
CONTENT SECURITY GATEWAY APPLIANCES

Developed by gateway AV pioneers, CP Secure's award-winning Content Security Gateway (CSG) appliances protect against the latest malware threats faced by IT professionals and their enterprise-class organizations. Current customers consider their CSG appliances mission-critical for the following reasons:

- **Effective**
In a word, CSG appliances work. They scan in real-time on HTTP, SMTP, POP3, IMAP, FTP, and HTTPS and stop all known spyware, viruses, worms, and other malware at the internet gateway, before they enter the network.
- **Simple**
CSG appliances are true appliances. They deploy in a matter of minutes, run and update automatically, and are managed and monitored securely through the web.
- **High ROI**
CSG appliances provide excellent value from day one. When the CSGs are deployed, they report the often astounding number of spyware and viruses that they are stopping and quickly prove themselves as indispensable. Moreover, as part of a layered defense, the appliances complement customers' existing security products, thereby preserving and enhancing customers' past security investments.

Customers use CSG appliances as their first line of defense against network-based malware because they trust the products and the company backing the products. They rest assured that they are secured against the latest malware threats, and they reclaim more of their time to pursue tasks at the core of their organizations' missions.

Diagram: Basic Deployment of CSG



KEY FEATURES

Real-time Scanning

Patent-pending stream-based scanning technology enables highly scalable scanning of real-time web traffic for stealthy, targeted malware. Stop malware at the gateway, without stopping the internet.

Comprehensive Protection

Provides both web and email security, covering six major network protocols: HTTP, HTTPS, FTP, SMTP, POP3, and IMAP. Uses dual CP Secure-Kaspersky scan engines and both signature-based and heuristic detection. Signature library includes all known spyware, viruses, and other malware. Optional integration with Websense.

Automatic Signature Updates

Malware signatures are automatically updated every hour. Critical new signatures are deployed several hours before they are available from leading AV vendors.

True Appliance

Deploys in-line in a matter of minutes, anywhere in the network. Runs automatically and unobtrusively. Simply set and forget.

Powerful Management Capabilities

Secure and intuitive web-based administration console. Set granular policies and alerts, check summary statistics and graphical reports, drill down to IP address-level data, and integrate log data with standard network management tools.

Enterprise-class Support

Highly responsive and even proactive. Includes live 24x7x365 support, assigned technical account manager, virtual on-site support, software product updates and upgrades, and hourly and emergency malware signature updates. A world-class team of engineers and malware experts ensures that customers' CSGs are defeating the latest-breaking malware threats.

Simplified Licensing

Includes hardware, all software applications for an unlimited number of users, and the first year of standard support and maintenance.

¹ JCSA Labs Virus Prevalence Survey 2004, April 2005. Average complete cost of recovery for each medium-large organization hit by a virus disaster (37% of 300 organizations surveyed) was over US\$900,000 in 2004.

Features of CSG Models



MODEL		2500	1500	1000+	300	110
SIZING GUIDELINES						
Customer Type		Enterprise	Enterprise	Enterprise	Small-Med.	Small-Med.
Number of Nodes		Thousands	Thousands	Thousands	Hundreds	Up to 100
HTTP Throughput (Mb/s)		480	314	260	68	50
SMTP Throughput (emails/hour)		2,760,000	1,380,000	1,080,000	420,000	300,000
CONTENT SECURITY						
Network Anti-Malware Applications:						
Web (HTTP, HTTPS, FTP)		•	•	•	•	•
Email (SMTP, POP3, IMAP)		•	•	•	•	•
Stream-Based Scanning		•	•	•	•	•
Inbound and Outbound Inspection		•	•	•	•	•
Dual Scan Engines		•	•	•	•	•
All Known Viruses Covered		•	•	•	•	•
All Known Spyware Covered		•	•	•	•	•
Automatic Signature Updates		Hourly	Hourly	Hourly	Hourly	Hourly
Heuristic Detection		•	•	•	•	•
Anti-Spam Application		•	•	•	•	•
Quarantine		•	•	•	•	•
Content Filtering Applications		•	•	•	•	•
URL Filtering Application		•	•	•	•	•
WebSense Integration Option		•	•	•	•	•
Software Licenses		All Included	All Included	All Included	All Included	All Included
Number of Users		Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
DEPLOYMENT						
Plug and Play		•	•	•	•	•
Inline Transparent Bridge		•	•	•	•	•
VLAN Support		•	•	•	•	•
RAID		•	•	•	•	•
Redundant Power Supply Units		•	•	•	•	•
Fail-open		•	•	•	•	•
Fail-over		•	•	•	•	•
Load-balancing Option ²		•	•	•	•	•
MANAGEMENT						
Secure Web-based Admin. Console		•	•	•	•	•
Dedicated Administration Port		•	•	•	•	•
Multi-User Accounts		•	•	•	•	•
Granular Policy Options		•	•	•	•	•
Summary Statistics		•	•	•	•	•
Granular Log Query		•	•	•	•	•
Syslog Support		•	•	•	•	•
Graphical Reporting		•	•	•	•	•
Automatic Outbreak Alerts		•	•	•	•	•
HARDWARE						
Gigabit Fiber Ports		2	2	2		
Gigabit Copper Ports		2	2	2		
Gigabit Copper Ports with Bypass		2		2		
Fast Ethernet Ports		1	1	1	3	3
Administration Console Port		RS232	RS232	RS232	RS232	RS232
LCD Display		•	•	•		
Power Supply		2 x 400W 100-240V	2 x 350W 100-240V	510W 100-240V	250W 100-240V	250W 100-240V
Operating Temperature	F	32° to 104°	32° to 104°	32° to 104°	32° to 104°	32° to 104°
	C	0° to 40°	0° to 40°	0° to 40°	0° to 40°	0° to 40°
Relative Humidity, Non-condensing		5% to 85%	20% to 80%	5% to 85%	10% to 90%	5% to 85%
Form Factor		2U	2U	2U	1U	1U
Dimensions (H x W x D)	inches	3.5 x 16.9 x 19.3	3.5 x 16.9 x 16.0	3.5 x 16.9 x 19.3	1.8 x 16.9 x 9.0	1.8 x 16.9 x 14.2
	cm	8.8 x 43.0 x 49.0	8.8 x 43.0 x 40.6	8.8 x 43.0 x 49.0	4.5 x 43.0 x 22.8	4.5 x 43.0 x 36.0
Weight	lbs	48.6	41.8	39.6	17.6	21.6
	kg	22.0	19.0	18.0	8.0	9.8
SUPPORT						
Standard Support		1st Yr Included	1st Yr Included	1st Yr Included	1st Yr Included	1st Yr Included
Enterprise Support Option		•	•	•	•	•
Replacement Hardware Option		•	•	•	•	•

GLOBAL HEADQUARTERS / NORTH AMERICA

20065 Stevens Creek Blvd.
Building C
Cupertino, CA 95014
USA
Tel: +1 888.722.6847
+1 408.873.7778
Fax: +1 408.873.7779
Email: info@cpsecure.com

EUROPE

Bendenweg 101
53121 Bonn
Germany
Tel: +49 228.85427.0
Fax: +49 228.85427.29

ASIA

4F-1, No. 432, Keelung Road,
Section 1
Taipei 110
Taiwan, ROC
Tel: +886 2.2723.0936
Fax: +886 2.2723.1791

ABOUT CP SECURE, INC.

Founded by gateway anti-virus pioneers, CP Secure, Inc. is a leading innovator of real-time anti-malware solutions for enterprise-class organizations. The company's Content Security Gateway appliances are powered by patent-pending stream-based scanning technology to protect some of the world's most demanding organizations against spyware, viruses, and other malware. CP Secure operates globally, in North America, Europe, and Asia, and may be found on the web at www.cpsecure.com.

² Support for third party enterprise-class load-balancing products.