

Secure and Enable the New Internet

Unified Security Gateway (USG) is a secure Web gateway that integrates traditional URL filtering, anti-malware and anti-virus with content protection, control and security over Web 2.0 applications such as social networks, instant messaging and Unified Communications (UC).

KEY FEATURES

- Monitor and control content posted to social networks, Twitter, blogs and sent via webmail
- Control inbound Web content – block elements of Web content or media that fall outside of policy
- Provide visibility and application level control for more than 3,000 native and Web 2.0 applications, including social networks, IM, P2P, and IPTV
- Enforce corporate Web usage policies through block, allow or personalized “coaching” and custom filtering categories
- Onboard Sophos anti-virus engine scans content received over HTTP/HTTPS, FTP, IM and UC channels
- Protects against inbound and outbound threats (SpIM, spyware, rootkits, worms, botnets and Trojans)
- Secures real-time content across all communications channels, preventing inadvertent or malicious leakage of information
- Allows tamper-proof logging and archival of IM and UC conversations and file attachments
- Integrate with Web/FTP proxy server, such as Blue Coat, through an ICAP-based connector or deploy in simple pass-by mode with no changes to existing network configurations
- Time and bandwidth allocation quota setting across Web and real-time communications
- Insight reporting engine and intuitive report creation wizard provides a “birds-eye” view of user traffic across all Internet channels – including Web, P2P, IM & UC

The Internet has Changed

Today's Internet is dominated by connectivity and collaboration. As organizations and users alike are utilizing a combination of enterprise and publicly available tools, applications and communities, the internet and corporate networks are awash with Web 2.0 applications such as social networks, instant messaging, VoIP, gaming and sharing applications.

In a corporate environment administrators are faced with the challenge of managing and securing the converging worlds of enterprise communications and collaboration tools such as Microsoft Office Communications Server and IBM Lotus Sametime on the one hand with publicly available social networks and Web 2.0 applications on the other.

Traditional security tools such as firewalls and URL filters are bypassed by thousands of applications, such as streaming audio and video, file sharing and collaboration tools, which are capable of hopping from port to port, using encryption and non-standard protocols. Proactively managing and securing employee Internet and communication tool usage requires a nuanced, responsive policy with granular control of information and access.

“Secure Web Gateway’s must, at a minimum, include URL filtering, malicious-code detection and filtering and application controls for popular Web-based applications, such as instant messaging (IM) and Skype.”

Gartner

A Secure Web Gateway for the Collaborative Internet

FaceTime's Unified Security Gateway 3.0 combines content monitoring, management and security of Web 2.0 applications, such as social networks, instant messaging and Unified Communications, with URL filtering, anti-malware and Web anti-virus protection.

USG 3.0 enables organizations to safely harness the power of the collaborative Internet. USG gives granular control of not just Web sites and applications but also of content posted to social networking sites and blogs, which can now be monitored, secured and recorded – reducing outbound data leakage and enabling compliance with industry regulations and legal discovery requirements. A highly visual reporting engine gives an innovative birds-eye view of user behavior across Web, IM, P2P, UC and social networks. Integration of Sophos anti-virus scanning technology in combination with USG's URL filtering and malware engines reduces the risk of Internet-borne malware and viruses.

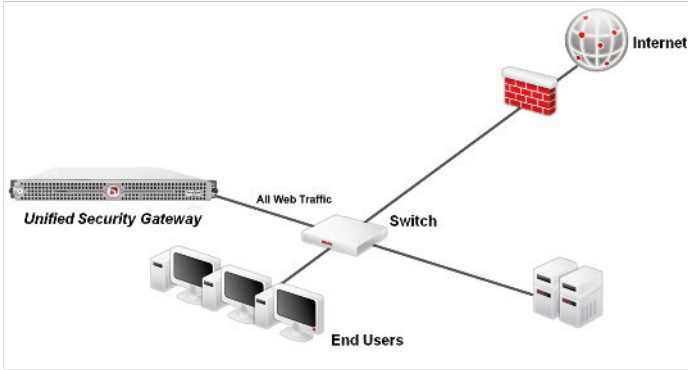
A fully customizable dashboard provides for full personalization and combines with straightforward policy management, statistics and system information. USG 3.0 integrates with LDAP and Active Directory servers to provide simplified group policy setting with granular controls include quota setting by employee, time and bandwidth – across all real-time communications modalities – including instant messaging and social networking sites.

An intuitive report creation wizard – and considerable standard report library – provides extensive real-time unified management of information across Web and real-time channels to ensure compliance with corporate and regulatory requirements.

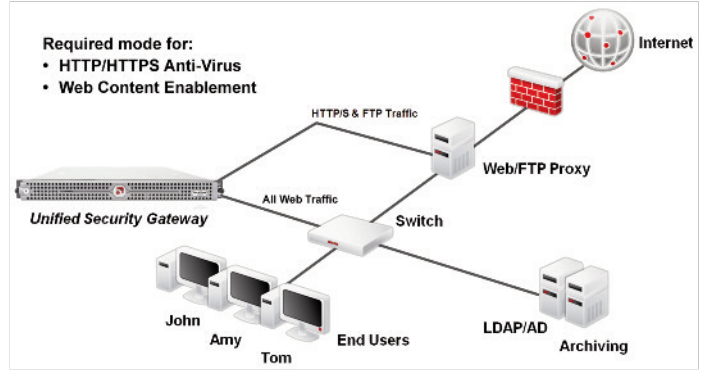


Unified Security Gateway

Pass-by (span port) deployment mode



ICAP-based Web proxy connector mode



USG 3.0 is simple to install and offers seamless integration with LDAP and Active Directory servers. USG 3.0 may be integrated with a Web/FTP proxy server, such as Blue Coat, through an ICAP-based connector or deployed in simple pass-by mode, which requires no change to existing network configurations.

UNIFIED SECURITY GATEWAY FEATURES

Application Control

- Visibility and control of 3,000 native and Web applications in categories from social networks, IM, P2P to IPTV & remote administration applications
- Real-time alert reporting on disallowed content transfers
- Protect investment in UC platforms such as Microsoft OCS and IBM Lotus Sametime by preventing use of native public IM tools
- Time of day and bandwidth controls by group and user as well as controls to download and use Web 2.0 applications

URL Filtering

- Enforce corporate acceptable Web policies through allow, block or “coach” access to categories or individual websites
- Dynamically filter millions of websites and URLs using predefined and custom categories
- Custom policies based on location, groups, users, file extensions and content types

Anti-Malware & Anti-Virus

- Real-time protection against malware, rootkits and botnets
- Stop access to malware-infected websites
- Prevent Web-based threats propagating through social networks
- Automated malware signature and application updates from Sunbelt Software & FaceTime Security Labs
- Onboard Sophos anti-virus engine scans content received over HTTP/HTTPS, FTP, IM and UC channels

Public IM and UC Enablement

- Support for IBM Lotus Sametime and Microsoft OCS (including R2)

- Support for enabling and securing public IM networks includes Yahoo, MSN, Windows Live, AOL and GoogleTalk
- Apply security policy and management controls to both UC messaging & public IM
- Block day-zero worms with challenge response and message throttling
- Prevent data leakage with granular IM content filtering and file transfer blocking
- Block risky, bandwidth-consuming SpIM
- Scan file transfers over IM using existing anti-virus infrastructure or onboard option
- Archive actual files transferred over IM for comprehensive review and audit process
- Create ethical boundaries by setting policies at user/group level for IM usage
- Apply IM disclaimer messages to educate users and meet legal, audit and regulatory requirements

Web Content Enablement

- Monitor and control content posted to social networks, Twitter, blogs and sent via webmail
- Control inbound Web content – block elements of Web content or media that falls outside policy
- Record Web content posted for legal and regulatory purposes

Implementation

- Simple pass-by mode with no change to existing network configurations
- ICAP-based Web based proxy connector deployment option
- VMware implementation provides for utilization of existing hardware

Management

- Dynamic fully customizable dashboard enables delivery of appropriate content to multiple administrators
- Manage productivity through time and bandwidth quota setting and allocation controls by group or user – across Web access, P2P usage, social networks and instant messaging
- Granular control (with LDAP and AD support) at group and user levels for location-independent policy enforcement across all modalities

Reporting

- Intuitive report creation wizard enables creation/modification of Graphical, Summary and Detailed reports
- Extensive library of standard reports
- Insight reporting engine provides birds-eye view of all user traffic and aggregates data from multiple USGs
- Automated scheduling and export options

License Modules

Basic License

- Control for 3,000+ Web Applications
- Hardware or VM Deployment

Additional License Options

- Web Content Enablement
- Public Instant Messaging Enablement
- Unified Communications Enablement

Recurring Fees:

- Annual Maintenance & Support
- URL Filtering Fees
- Anti-Malware Subscriptions
- Sophos Anti-Virus Subscriptions



FaceTime Communications, Inc.
(888) 349-FACE (3223) toll free
(650) 598-2820 fax
info@facetime.com

Worldwide Headquarters
1301 Shoreway, Suite 275
Belmont, CA 94002 USA
(650) 631-6300 phone
sales@facetime.com

EMEA Headquarters
400 Thames Valley Park
Reading, Berkshire, RG6 1PT UK
+44 (0) 118 963 7469 phone
emea@facetime.com