

Total Control for Web and Real-Time Internet Communication

About FaceTime Unified Security Gateway

Unified Security Gateway is a secure Web gateway that enables organizations to integrate the management, security, and compliance of the full range of real-time communications, Web usage, including social networks and other dynamic communications environments, and enterprise-class unified communications such as Microsoft OCS and IBM Lotus Sametime.

KEY FEATURES

- Provides visibility and control for greynet application use with support for more than 40 IM and 65 P2P applications
- Enforces corporate web usage policies with customizable filtering categories and industry-leading URL databases
- Secures real-time content across all communications channels and prevents inadvertent or malicious leakage of information
- Protects against inbound and outbound threats (SpIM, spyware, rootkits, worms, botnets, and more)
- Adaptive proxy and connector architecture provides seamless control over both consumer and enterprise UC applications
- Allows tamper-proof logging and archival of online conversations and file transfers for non-repudiation of archived messages
- Integrates with existing IT and anti-malware infrastructures to deliver best-in-class security services with zero latency

“ The market is demanding a secure Web gateway (SWG) solution that provides not only traditional URL filtering but also malicious software (malware) filtering, as well as application control for Web applications such as instant messaging (IM) and, eventually, voice over IP (VoIP or internet telephony). ”

**Gartner
March 2007**

The Reality of Real-time Communications

The Web 2.0 landscape is alive with participation and collaboration. More than 200 social networking sites are available to anyone with a browser. Several have evolved into full-blown development platforms – Facebook alone supports almost 20,000 applications. From the enterprise side, it's become common practice for human resources to review candidates' social networking activities as part of the hiring process, and for knowledge workers, social networks have become an always-on focus group for testing and reviewing new ideas.

Today's young generation of workers grew up with instant messaging and are used to the immediacy of communication offered by social networks; it is natural for them to expect the same level of immediacy in the business environment, because they innately understand its value. They see no reason not to interact with social networks from inside the corporate network. However, as the line between corporate networks and social networks blurs, social networks and their applications – many of which involve real-time communications – become an issue for enterprise IT.

Unfortunately, most IT departments cannot actually see these new activities at all, because they bypass traditional corporate network protection measures. Research firm Gartner acknowledges this, noting that today's collaborative environment requires a security solution that combines URL filtering, malicious code detection and filtering, and application controls for applications such as instant messaging and Skype.

While enterprise instant messaging and unified communication platforms like Microsoft LCS/OCS and IBM Lotus SameTime deliver a measure of additional security, further controls are needed to ensure the level of security needed to meet regulatory compliance and e-Discovery requirements.

A Unified Solution for a Unified Platform

FaceTime Unified Security Gateway (USG) enables enterprises to enforce acceptable-use policies for real-time communications and improve visibility into, and decision-making about, security issues related to real-time Internet use. By providing a single point for enablement, access management, security, and control for web and real-time channels, USG delivers a security solution that addresses future as well as current threats while maximizing existing investments in security infrastructure. With flexible deployment options, USG fits seamlessly into existing network topologies to offer the highest level of security with zero latency and a low total cost of ownership.

FaceTime recognizes that real-time communications and social networks deliver real business benefits, and that IT needs a way to control, monitor and secure these communications that's efficient, compliant, and makes maximum use of existing investments in security technology. With almost a decade of experience in helping organizations to gain the greatest benefits from real-time communications while effectively controlling their insecurities, the company is ideally positioned to deliver a solution that's precisely focused on the point of greatest risk – the gateway. USG delivers on that knowledge with:

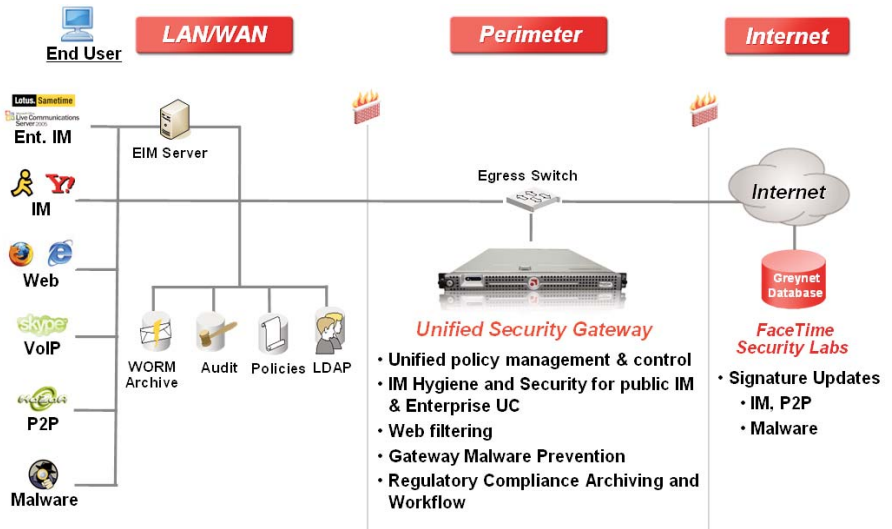
- Hardened, proactive security that's built on years of research and partnerships to put enterprises ahead of the game
- Flexibility and security in a single appliance, enabling organizations to evolve their real-time Internet security protection as their needs grow and change
- The ability to leverage existing investments in anti-virus and apply those traditional tools to the real-time communications environment



Unified Security Gateway

FaceTime's Unified Security Gateway delivers next-generation Internet protection through unified visibility, management and policy control across all unified communications channels. USG empowers enterprises to:

- Get visibility into and control over the use of sanctioned and unsanctioned communications tools in the enterprise.
- Enforce security and usage policies across real-time communications and web channels.
- Reduce the business risks from exposure to malware (worms, viruses, SpIM, spyware) and from data leakage.
- Ensure compliance with corporate and regulatory requirements through tamper-proof logging, archival and easy retrieval of electronic conversations.
- Leverage existing security investments by providing an infrastructure that addresses the real-time communications universe.
- Optimize effectiveness with an integrated solution that provides a unified control center for all real-time communications channels.



Deployment Topology for Unified Security Gateway

UNIFIED SECURITY GATEWAY FEATURES

Security

- Dynamically filter millions of websites and URLs using predefined and customizable categories
- Gain visibility and control over dozens of P2P networks and thousands of social network applications from Facebook and others
- Protect against spyware, rootkits, botnets coming over real-time channels.
- Enforce corporate acceptable usage policies for web access
- Block access to infected websites
- Prevent web-based threats propagating through social networks
- Targeted agentless remediation of infected, non-compliant endpoints

Instant Messaging

- Gain visibility and control over dozens of IM applications, including aggregators
- Block day-zero worms with challenge-response and message throttling
- Prevent data leakage with granular filtering and file transfer blocking
- Block risky, bandwidth-consuming SpIM
- Scan file transfers over IM using existing anti-virus infrastructure.
- Location-aware policy enforcement using endpoint IP addresses
- Map public IM buddy names to user names in enterprise directory

Compliance

- Unified reports for web, IM, and P2P channels, with detail reports on web channel activities
- Tamper-proof logging and archival for compliance and e-discovery requirements.
- Create ethical boundaries by setting policies at user/group level for IM usage
- Leverage and integrate with existing message archival solutions for comprehensive enterprise messaging insight
- End user disclaimers to educate users and meet legal, audit and regulatory requirements
- Configure rich compliance workflow to easily retrieve stored information.
- Archive actual files transferred over IM for comprehensive review and audit process.
- Record PIM conversations conducted over EIM clients in federated environments

Management

- Granular control at group and user levels for location-independent policy enforcement
- Prevent circumvention of UC platforms like Microsoft OCS and IBM Lotus Sametime.
- Unified policy management and enforcement for all real-time Internet activities
- Leverage directory structures for policy enforcement at user/group levels
- Integration with existing infrastructure with zero latency.

- Pre-defined and customizable reports in multiple output formats.
- Secure management console for centralized configuration, management, and reporting
- Supports use of external database for policies, logging and archival for scalability and availability

About FaceTime Communications

FaceTime enables the safe and productive use of the real-time Internet, including both public and enterprise instant messaging and unified communications platforms. Ranked number one by IDC in market share among instant messaging management vendors for the fourth consecutive year, FaceTime's award-winning solutions are used by more than 900 customers, among them nine of the ten largest U.S. banks. FaceTime supports or has strategic partnerships with all leading public and enterprise IM network providers, including AOL, Google, Microsoft, Yahoo!, Skype, IBM, Reuters, and Jabber.

For more information about FaceTime Communications, visit <http://www.facetime.com>