

Total Control for Web and Real-Time Internet Communications

About FaceTime Unified Security Gateway

Unified Security Gateway is a secure Web gateway appliance that enables organizations to integrate management, security and compliance of Web usage, greynet applications such as public IM, Skype and P2P, and enterprise-class unified communications platforms such as Microsoft's OCS and IBM Lotus Sametime.

KEY FEATURES

- Adaptive proxy and connector architecture provides seamless monitoring and control over both, consumer and enterprise UC applications
- Provides visibility and control for greynet application use with support for more than 40 IM and 65 P2P applications
- Enables unified policy management and enforcement across all real-time Internet traffic
- 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)
- Ensures tamper-proof logging and archival of online conversations and file transfers towards non-repudiation of archived messages
- Integrates with existing IT and anti-malware infrastructures to deliver best-in-class security services with zero latency

The Reality of Real-time Communications

Today's workforce expects instant messaging and other real-time communications tools - Web conferencing, Voice over IP, and social networking - to be "always on", just as their predecessors viewed email. The edge of the corporate network is rapidly moving beyond the physical network perimeter to include the broader community of customers and trading partners, and end users are driving the process.

Instant messaging, P2P networking, web conferencing, Voice over IP, and other web-based applications - are downloaded by users in the workplace, regardless of whether enterprise instant messaging and other IT-sanctioned unified communication tools are available. These greynets are characterized by their evasive behavior, which renders them invisible to IT and introduces a significant security risk into the enterprise. Because they can't be seen, they can't be managed, and they can't be secured. Greynets are vectors for malware, open up client-side code vulnerabilities to hackers, and facilitate data leakage; their real-time nature enables them to evade traditional security measures.

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 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

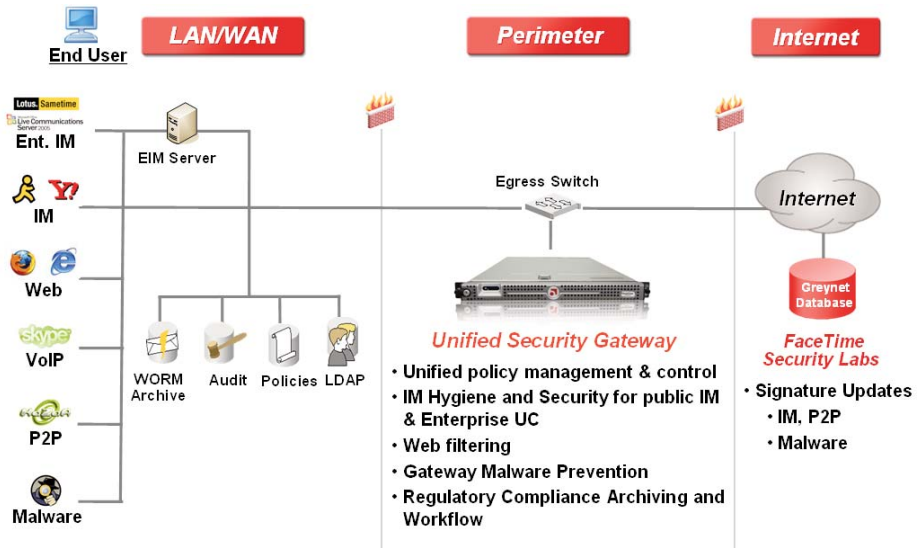
"The market is demanding a secure Web gateway (SWG) solution that provides not only traditional URL filtering but also malicious software (malware) filtering, as well as application control for Web applications such as instant messaging (IM) and, eventually, voice over IP (VoIP or internet telephony)."



Unified Security Gateway

FaceTime's Unified Security Gateway delivers next-generation greynet 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 greynets in the enterprise
- Enforce security and usage policies across real-time communication 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 communication channels



Deployment Topology for Unified Security Gateway

UNIFIED SECURITY GATEWAY FEATURES

Security

Web Gateway

- Filter over 21 million sites in 54 predefined categories and more than 7 million URLs according to 73 predefined categories
- Visibility and control over 65 P2P applications
- 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 other real-time channels
- Targeted agentless remediation of infected, non-compliant endpoints

Instant Messaging

- Visibility and control for more than 40 IM applications
- 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

- 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 EIMs such as Microsoft LCS/OCS and IBM Lotus Sametime
- Unified policy management and enforcement for all real-time Internet traffic
- Leverage directory structures for policy enforcement at user/group levels
- Integration in to existing network infrastructures 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>