

FaceTime Unified Security Gateway (USG) is an enterprise-class appliance that secures and manages the compliant use of unified communications (UC), including enterprise instant messaging (EIM) like Microsoft LCS/OCS, IBM Lotus SameTime, web conferencing, chat, Voice over IP, and other collaborative technologies. USG additionally enables corporations to take control over public instant messaging (PIM - for example, Yahoo!, MSN, GoogleTalk), P2P (eg Skype) and other consumer-driven tools that proliferate throughout today's real-time enterprises. USG fits seamlessly into typical network topologies and leverages existing security infrastructure to offer the highest level of security and compliance with zero latency and a low total cost of ownership.

USG empowers enterprises to:

- Get visibility into and control over the use of sanctioned and unsanctioned real-time applications in the enterprise.
- Enforce security and usage policies across real-time Internet 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.
- Enable secure real-time communications and enforce policies at a single point without creating a single point of failure
- Optimize effectiveness with an integrated solution that provides a unified control center for all data channels.

FaceTime USG combines best-in-class IM management, archival and compliance, perimeter real-time application security, malware prevention, and URL filtering into a single purpose-built hardened Linux appliance.

With flexible two or three port deployment modes (see Figure 2 and 3, right), USG delivers a single security and compliance solution that addresses all real-time communications channels without impacting their productive use.



Figure 1: Four USG models are available, depending on the number of users and network throughput requirements.

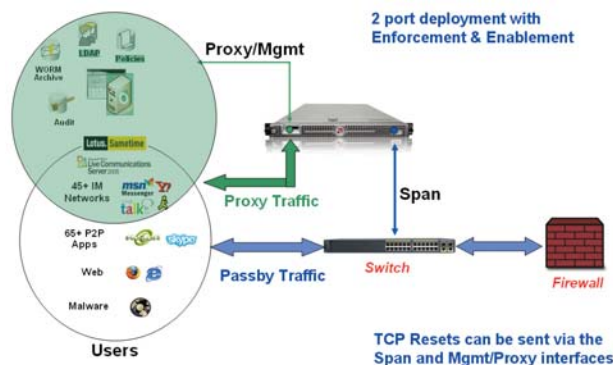


Figure 2: 2-port deployment for USG

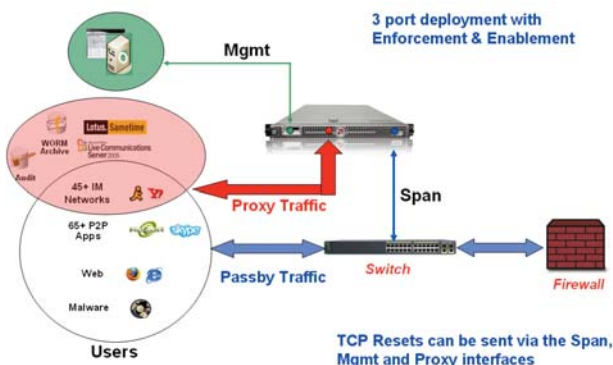


Figure 3: 3-port deployment for USG

Security:

- Comprehensive protection against worms, viruses, spyware, and other malware
- Scans file transfers over IM using existing anti-virus tools
- Patent-pending anti-SpIM preserves productivity and bandwidth
- Intellectual property protection through information leak prevention
- Content filtering and archiving/logging of all online conversations

Compliance:

- Tamper-proof, non-repudiated logging, auditing, and archival
- Distinguishes between authorized and unauthorized IM connections
- TrueCompliance™ supports compliance regulations and e-Discovery requirements

Management:

- Unified policy management based on user/group, location, greynet application, method and actual content
- Apply powerful, granular policies for total visibility and control
- Enterprise-class logging and monitoring

Enterprise-grade deployment:

- Adaptive proxy and connector architecture ensures safe use of well-behaved greynets and EIM/UC
- Zero-latency high-performance hybrid pass-by enforcement for unsanctioned greynets such as P2P, anonymizers, and spyware

FaceTime Communications, Inc.

1159 Triton Drive Foster City, CA 94404

(888) 349-FACE (3223) toll free

(650) 574-1600 phone

(650) 574-2700 fax

General Information: info@facetime.com Sales: sales@facetime.com