

Managing Skype and other Real-Time Communications in the Enterprise

About FaceTime Internet Security Edition

FaceTime Internet Security Edition enables the safe and productive use of Skype and other real-time applications including web browsing, IM, P2P, and social networking sites. Purpose-built and integrated to provide total visibility and control, FaceTime Internet Security Edition allows organizations to implement powerful policies that detect, secure, manage and enable real-time collaborative applications while blocking malware, minimizing information leakage, and controlling employee Internet use.

KEY FEATURES FOR SKYPE CONTROL AND MANAGEMENT:

- Provides visibility into Skype usage within the enterprise
- Controls the use of Skype by version at the gateway
- Controls for usage of over 15 Skype features including file transfers and personalization
- Blocks malicious URLs in Skype chat
- Manages Skype traffic by allowing it on a specified port or through a specified proxy
- Manages Skype supernode behavior on corporate network
- Set comprehensive policy management at company, group and user levels with ongoing scheduled enforcement
- Centralized management and reporting through dashboard and detailed reports
- Ongoing technical partnership with Skype extends the solution for future releases of Skype clients



“ Because the Skype client is a free download...most businesses have no idea how many Skype clients are installed on their systems or how much Skype traffic passes over their networks. The problem is that Skype doesn't demand that vulnerable clients be updated, and without administrative management controls to force this, the VOIP client leaves corporate networks open to attack. ”

Lawrence Orans
Research Director, Gartner

Value and Risks of Skype in the Enterprise

Three years ago, there were five million users of Skype. Today, that number is 276 million – and those users have racked up more than 100 billion minutes of talk time using only the free Skype-to-Skype voice and video calls since the company launched in 2003. It is the fastest growing communications network in history, and a significant proportion of its users today are inside corporate networks.

Skype's appeal to the corporate world is unsurprising: the tool is free, the service is largely free, and IM, voice, and video conferencing are all included in a single application. The latest versions offer functions specifically designed for business use, including a web-based business control panel. While it's most widely known and used as a Voice over IP (VoIP) application for free long distance and international telephone calls, Skype is a complex peer to peer (P2P) network and as such exhibits all the stealthy and evasive behavior characteristic of typical greynet applications. It constantly scans for open ports on the network through which it can re-route traffic.

What's more, any computer running Skype connected to the Internet with a routable IP address can become a Supernode and route other users' Skype traffic through it, increasing both bandwidth consumption and the potential for exposure to threats propagating over this channel. Uncontrolled use brings serious risk to the enterprise from inbound malware threats and outbound information leakage.

Skype communications are all classified as electronic communications for the purposes of data protection and related compliance legislation, including e-discovery. IT departments need to manage the productive use of these applications while protecting against their misuse.

Because all communications over Skype are encrypted, monitoring with traditional tools is virtually impossible.

How FaceTime Can Help

FaceTime Internet Security Edition (FISE) is the only solution that provides a comprehensive gateway-to-endpoint approach to managing and securing the use of Skype and other real-time communication applications within the enterprise. With FaceTime, IT organizations can benefit from a single point of control for all real-time communications, social networking, and web filtering, resulting in simplified administration and lower operational costs. FaceTime provides a platform that combines the highest efficacy with the fastest performance, acknowledged by the company's receipt of the Network World Best of the Tests 2007 Award.

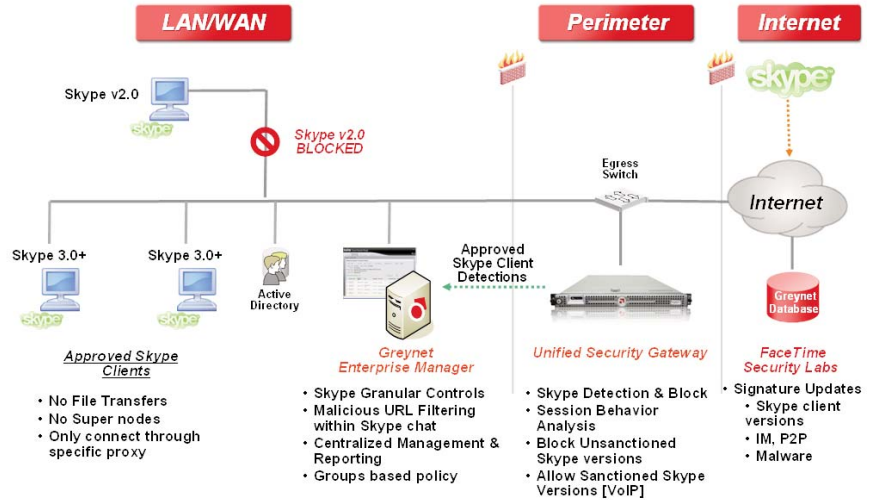
What can't be seen can't be controlled - so the first step in gaining control over Skype usage in the organization is visibility at the gateway. FaceTime's Unified Security Gateway (USG) provides IT with total visibility into Skype traffic on the network. It is purpose-built for the security of real-time communications and fits seamlessly within the enterprise network without the need to change other network elements such as firewalls or anti-virus. Once visibility is obtained, Greynet Enterprise Manager (GEM) enables the enforcement of Skype usage policies at the client and blocks any malicious URLs coming in over Skype chat sessions. This powerful combination allows IT managers to set, enforce policies and secure Skype traffic on their network.

“ Today, 33 per cent of Skype's users in North America are utilizing Skype for business purposes. As a result of our work with FaceTime, network administrators now have centralized management capabilities in addition to the cost savings, simplicity and productivity advantages Skype offers to businesses. ”

Kurt Sauer
CSO, Skype

FaceTime Internet Security Edition comprises two components:

- Unified Security Gateway (USG) is a secure gateway appliance that integrates management, security and compliance of Web communications (including Web 2.0 & Social Networks), consumer-driven applications such as public IM, Skype, P2P and enterprise-class Unified Communications suites.
- Greynet Enterprise Manager (GEM) provides total visibility and control with integral targeted malware infection remediation over real-time communications channels. Working in conjunction with USG, GEM delivers clientless, non-intrusive targeted remediation and inoculation to efficiently clean and prevent malware infections at the desktop.



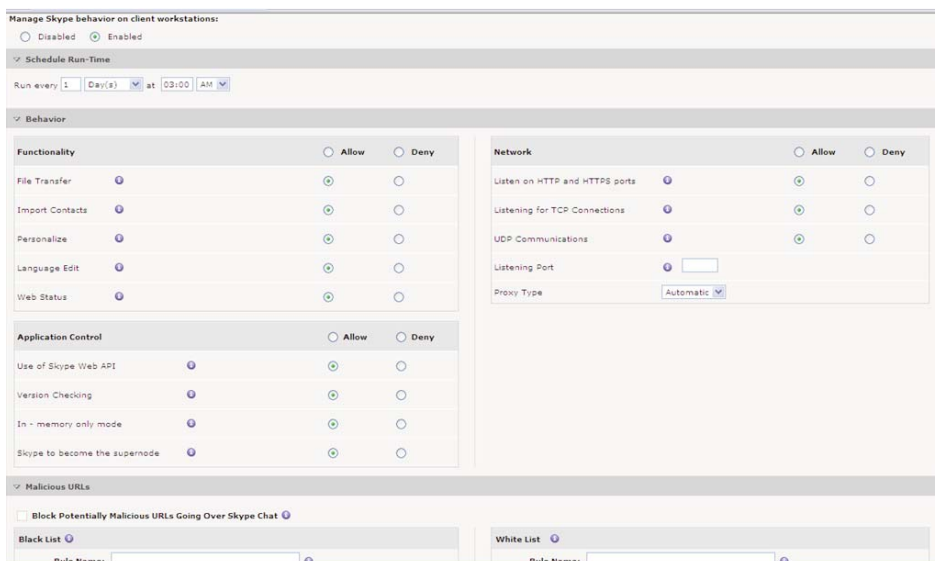
FaceTime Internet Security Edition brings together the benefits of Unified Security Gateway and Greynet Enterprise Manager to deliver the first fully-integrated solution to secure, manage and control web browsing and greynet applications.

Use USG to:

- Provide controls for the Skype versions that can be used within the enterprise. Any version below the designated version (e.g. 2.0) will be blocked at the gateway
- Standardize on the use of a single version of Skype within the enterprise
- Filter older versions of Skype which have known vulnerabilities/attacks
- Monitor and deliver graphical reports of Skype usage

Add GEM to:

- Block malicious URLs in Skype chat
- Centrally manage the enforcement of selected Skype features across specific endpoints
- Automate the scheduled enforcement of policies to prevent circumvention
- Aggregate reports from multiple USG appliances to provide organization-wide visibility into Skype usage
- Monitor and deliver graphical reports of Skype usage



FISE also enables organizations to:

- Secure and centrally manage the safe use of the web and real-time communication applications.
- Reduce operational expenses by consolidating all Internet communications security controls into a single unified solution.
- Provide visibility into and control of real-time traffic channels
- Monitor and control access to Web sites to prevent inappropriate use of company resources
- Block malware at the Internet gateway, before it can impact the business
- Trigger targeted clientless remediation of infected endpoints
- Improve decision making about security issues and Internet usage with unified real-time reporting
- Optimize value of enterprise IM and UC deployments by blocking the use of unauthorized communication tools

