

Managing Skype in the Enterprise with FaceTime Internet Security Edition

About FaceTime Internet Security Edition

FaceTime Internet Security Edition (FISE) empowers organizations to make safe and productive use of Skype and other real-time communication applications. Purpose-built and integrated to provide total visibility and control, FISE enables organizations to detect, secure, and manage these applications while preventing inbound malware threats, 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
- Set comprehensive policy management at company, group and user levels with ongoing scheduled enforcement
- Controls for usage of over 15 Skype features including file transfers and personalization
- Manage Skype traffic by allowing it on a specified port or through a specified proxy
- Manage Skype supernode behavior on corporate network
- 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

A year ago, there were five million users of Skype. Today, that number is 171 million - 30% of whom are business users - making it the fastest growing real-time communications network in history. Its 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 designed for business use.

While it's most widely 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 that exhibits all the stealthy and evasive behavior characteristic of greynet applications.

Skype 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 possible 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 solution to manage and secure 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 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.

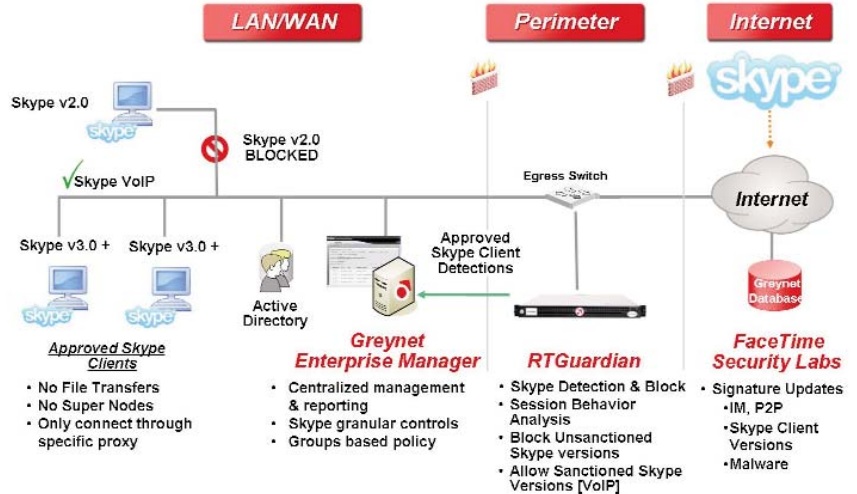
What can't be seen can't be controlled - so the first step in gaining control over Skype usage in the organization is visibility at the gateway. RTGuardian (RTG) provides IT with total visibility into Skype traffic on the network. It is purpose-built for the security of real-time communications and fits 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 secure enforcement of Skype usage policies at the desktop. This powerful combination allows IT managers to set and enforce central policies for Skype traffic that is permitted to cross the 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

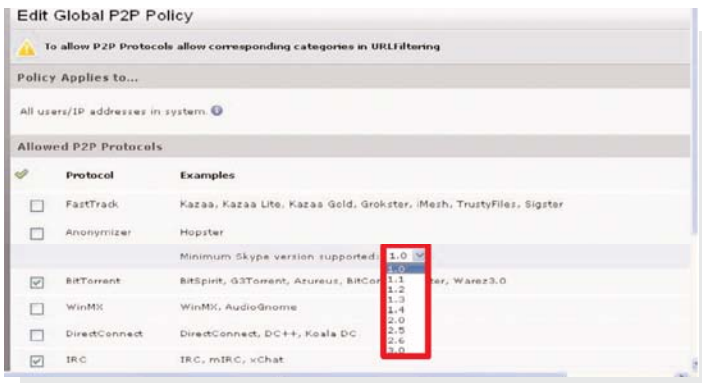
FISE comprises two key components:

- RTGuardian (RTG) is deployed at the gateway to secure unauthorized Skype and other real-time communications usage in the enterprise and prevent malware infections
- Greynet Enterprise Manager (GEM) is a centralized management, reporting and control server that enables the enforcement of granular policies and aggregate reporting for Skype and other real-time communications traffic across the organization



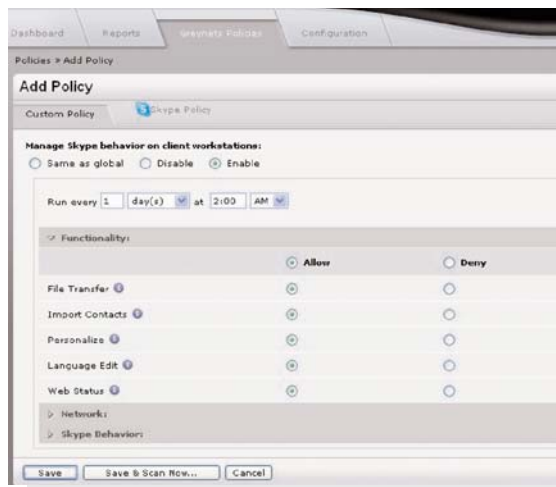
Use RTG to:

- 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:

- Centrally manage the enforcement of selected Skype features across specific endpoints
- Automate the scheduled enforcement of policies to prevent circumvention
- Aggregate reports from multiple RTG appliances to provide organization-wide visibility into Skype usage



FISE also enables organizations to:

- Detect, manage and secure all Internet activity with zero network latency
- Block malware over real-time communication channels at the Internet gateway
- Set web usage policy through LDAP integration and customize by IP addresses
- Monitor and control access to websites using integrated FaceTime WebFilter or Secure Computing SmartFilter
- Schedule automatic updates for URL and malware databases
- Deliver user and host level visibility through Active Directory integration
- Identify endpoints with phone-home spyware infections detected by RTGuardian
- Apply appropriate anti-spyware policies to scan, clean, and inoculate infected endpoints without the need for local agents
- Prevent spyware from downloading or executing on the client

Visit <http://www.facetime.com> for the complete FISE datasheet

