



EXCLUSIVE FaceTime Communications USG220

FaceTime deals efficiently with the ever-growing problem of IM, P2P and social networking in the workplace

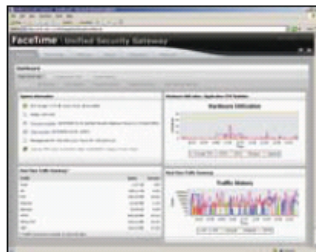
There was a time when many thought IM apps could bring benefits to business communications but, along with P2P apps and social-networking sites, they're now proving to be a pain. Security risks and loss in productivity are two major issues, but the problem is exacerbated because most UTM apps have limited facilities for dealing with these issues.

This is one area where FaceTime's latest USG220 appliance aims to deliver the tools to strictly control all IM and P2P apps and block spyware. It can identify systems that are infected with spyware without the need for installing local client utilities.

This latest version brings in a host of new features. The appliance now provides full web-content filtering, plus all access policies can be based on AD users and group membership, as well as hostnames and IP address ranges. However, the big deal comes with its awareness of social-networking sites such as Facebook and MySpace. FaceTime has categorised these sites, allowing the appliance to block or allow specific activities.

The app provides two network ports, one monitoring all traffic and the other used for management access and the new IM proxy feature. The latter provides finer control over IM apps since it can analyse messages in real time, look for banned words, and challenge users before sending messages. It can archive messages on the app or to an external SQL database, and offers a full range of eDiscovery search tools.

For testing, we connected the USG220 to an HP ProCurve 2848 Gigabit



The USG220 provides comprehensive features for monitoring social-networking sites.

switch with port mirroring configured. Initially, the appliance is run in a passive discovery mode, where it monitors all traffic and advises on all that it surveys. It employs packet inspection at Layer 7 and so offers a lot of information on application-related activity. The web interface opens with a dashboard providing a complete graphical rundown on network activity, summaries for each component and quick access to the latest reports.

We left the appliance lurking in the background for a few days and were impressed with its findings. It highlighted all instances of Windows Live Messenger and which systems were running them, revealed who was indulging in illicit entertainment, and showed which systems had the GoToMyPC admin tool loaded and ready for remote connections.

For IM activities it shows the IP address of the systems involved, the number of messages for each, and whether they went through the monitoring or proxy port. P2P apps will also be shown with the user and system



FaceTime's USG220 offers spyware and full web-content filtering.

SECURITY APPLIANCE

PRICE
100 users, £3,750
exc VAT

SUPPLIER
FaceTime
Communications
01189 637469

INTERNET
www.facetime.com

WARRANTY
3yr RTB

SPECIFICATIONS

Dell PowerEdge T1J rack server • 2.66GHz Intel Xeon 5150 • 2GB 667MHz DDR2 RAM • 80GB Western Digital SATA hard disk • 2 x Gigabit Ethernet • CentOS kernel • web browser management. Price includes first year web filtering and anti-spyware updates

identities, along with the amount of traffic being generated. We ran the Vuze client and could see clearly how much bandwidth it was sucking up as we watched some light entertainment.

The Enforcement mode is extremely versatile, as within a policy group you can block specific apps and apply web-filtering rules. For the IM, P2P and greynet sections there are hundreds of apps to choose from, while FaceTime's web filtering offers nearly 60 URL categories. The greynet section has more than 170 apps and for Facebook you can block it all or choose from 23 apps.

Advanced controls are only available from the default Group Policy, where you'll find all the extra features of the IM proxy. File-transfer privileges can be fine-tuned and files passed to an ICAP-compliant antivirus scanning server. You can create lists of restricted phrases, which can include credit card number formats. Users can be challenged before they send a message with suspect content, while messages containing URLs can also be blocked.

We had no problems blocking a range of apps including IPlayer, Vuze, Live Messenger and GoToMyPC. The USG220 also handled spyware sites well, as along with the URL category database it carries out packet analysis to determine the content and uses pattern matching and packet-sequence recognition.

With so many apps to monitor and possibly block, reporting needs to be comprehensive. The Reporting tab in FaceTime provides a complete overview of all activity, and you can select specific categories and drill down deeper for more information on the top blocked products, the systems trying to access them and, with AD policy groups in force, the offending users, too.

Despite the problems of unmonitored IM and P2P usage in the workplace, most security vendors still aren't taking this seriously. Fortunately, FaceTime is, and the USG220 not only delivers one of the most comprehensive solutions for monitoring and controlling these apps, it also adds spyware protection and full web-content filtering. **DAVE MITCHELL**

PERFORMANCE	★★★★★
FEATURES & DESIGN	★★★★★
VALUE FOR MONEY	★★★★★
OVERALL	★★★★★

An explanation of how we test products for PC Pro Business is on the cover disc