

« Web filtering

FaceTime USG 320



Supplier FaceTime Communications
Price From £8,695 for 250 users (exc VAT)
Contact www.facetime.com

FaceTime's USG (unified security gateway) appliances aim to deliver a far greater degree of control over web access than standard web filtering and combined UTM solutions.

Anti-spyware plus IM and P2P application controls come as standard but these latest versions now have a built-in awareness of social networking sites such as MySpace and Facebook. By categorising these kinds of sites, FaceTime has enabled the appliances to block or allow specific activities on a site.

Another new feature is support for Active Directory. Access policies can be applied to specific AD users or groups, making the appliances more versatile.

The USG 320 is the second in a family of four appliances. It is delivered as a good quality Dell PowerEdge 1U rack server and can handle 150Mbps throughput and up to 1,000 users. It has a couple of gigabit ethernet ports with the first used to monitor all web traffic.

We found deployment simple, as we attached the appliance to our HP ProCurve 2848 switch and configured port mirroring. The second port is used for dedicated management access but it also brings FaceTime's IM proxy into play. This delivers even greater control over IM applications such as Windows Live Messenger.

The IM proxy can analyse all messages in real time in both directions, add disclaimers to messages, check for banned words and phrases and issue challenges to users attempting to send messages. These can also be archived to the SQL database on the appliance or an external one. FaceTime's new reporting features add legal discovery facilities. We can also pull up reports on all activity to see which systems were trying to access blocked website categories and spyware sites.

FaceTime supports enterprise IM applications including Microsoft LCS/OCS and Lotus SameTime and can monitor and block selected traffic plus user activities and archive these as well. The appliance was first placed in a passive discovery mode where it used Layer 7 packet inspection to identify all application-related activities on the network. We had systems running Windows Messenger, the Vuze Bittorrent client, BBC's iPlayer and tools such as the GoToMyPC remote administration tool.

All were identified with the system's IP address and the amount of traffic they were generating.

USG 320's web interface opens with a complete overview of all activity, including colour-coded traffic graphs showing each application class. It provides summaries for each component and tabs allowing you to view statistics for IM, P2P, greynet, malware and web filtering. Facebook, MySpace, iPlayer and GoToMyPC usage was duly logged under the greynet section.

Enforcement for any or all of

the five main categories can be switched on and the range of options is impressive. For IM, P2P and greynet there are literally hundreds of applications to choose from and they can be blocked or allowed on an individual basis.

FaceTime does not mess about with spyware, as it employs a large database of known problem sites which it uses to filter and block access. It also carries out packet analysis to determine the content, and uses pattern matching plus packet sequence recognition.

During testing we were able to block Live Messenger. In discovery mode the appliance logged all activity, including the IP addresses of the participating stations and their contact names. iPlayer, Vuze and GoToMyPC clients received warning messages saying access was blocked and spyware sites we had previously visited were no longer accessible. The web filtering component also performed well.

The USG 320 cannot provide



anti-virus scanning. You will however, be hard-pushed to find a security appliance that can offer the same level of controls over IM and P2P and combine these with excellent web content filtering and spyware protection.
Dave Mitchell

SC MAGAZINE RATING	
Features	★★★★★
Performance	★★★★★
Ease of use	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for money	★★★★☆
OVERALL RATING	★★★★★

For Simple deployment, superb IM and P2P controls, system- and user-based access policies, social networking aware
Against Monitoring mode does not support anti-virus scanning
Verdict An excellent range of access controls for IM and P2P applications

FaceTime

FaceTime Communications Inc

400 Thames Valley Park
 Reading, Berkshire
 RG6 1PT
 Tel: +44 (0) 118 9637 469
 Email: emea@facetime.com

1301 Shoreway, Suite 275
 Belmont
 California, 94002
 Tel: 001 650 631 6300
 Email: info@facetime.com