
Meeting the burning need for firewalls

By Jason Walsh

With more work going on outside the office, the use of personal firewalls is more important than ever. Think of it this way: a mobile worker, whether mobile using a laptop or with a smartphone, is accessing company data and the network on a device that is effectively unsecured.

Connecting to the network from a hotel lobby, a wi-fi hotspot in an airport or an internet cafe is just another way of making the network less secure. But business doesn't stop at the front door and so mobile workers must also be protected.

"Personal firewalls are very important," said Conor Flynn of Rits. "Even enabling the built-in Mac OS X or Windows firewall is a start. Better still is a third-party solution."

Renaissance Contingency Services' Michael Conway agreed.

"Smaller businesses can get a UTM device that will suffice. The challenge for large organisations is 'where is the perimeter?' Mobile devices and multiple locations mean the perimeter ceases to exist," he said.

Third-party firewalls tend to have more up-to-date security measures and offer another key benefit to enterprise in the form of management.

"Most of these products have an enterprise

management solution," said Flynn. "That way even the administrator user on the laptop can be kept from changing the security settings."

A personal firewall is usually enough for a home user or home worker, but many sophisticated ones work in conjunction with corporate firewalls.

"We don't have a gateway solution, what we have is an integrated firewall in our Endpoint solution," said Dermot Hayden of Sophos. "The old idea of having your computers behind a secure network is no longer where it is. More often than not people are working outside as well as in the office so our firewall is network aware and built-in to the agent we deploy on the desktop."

The firewall included in Sophos Endpoint can switch itself off when it detects the computer is on a secured office network, turning itself on only when it is out in the wild.

"We're not suggesting this replaces the perimeter corporate firewall," Hayden said. "It will switch on once it's outside the corporate environment," he claimed Sophos identified 50,000 to 60,000 new pieces of malware every day and there were ever more ways for malicious software to sneak in.

"There are so many ways threats can be introduced into the corporate environment. This helps with laptops and includes device control for USB sticks, iPods and external hard drives," he said.