



## Secure your data and your budget

### INTERNET GATEWAY MANAGEMENT SERVICE

#### – WHAT TO LOOK FOR

- The service provides a full suite of functionality, including content filtering, firewall, virus blocking and isolation.
- The service is 'plug and play' and does not require major overhauls and reprogramming of existing IT systems
- The service can be provided through a periodic subscription rather than via a very costly start-up price
- Usage reporting can be carried out at any time and according to desired parameters
- The interface is easily understood by non-expert staff and changes to filters etc. Can then be made with a few clicks

For any organisation, private or public, computer network security is critical. This has always been the case, but as we push through a time of financial crisis, managers need to ensure that every dollar spent is strictly necessary. For local government authorities the intense scrutiny they can be under from ratepayers and media makes demonstrating this fiscal responsibility even more crucial. But having to recover from a catastrophic security incident is something that no council can afford.

Fortunately there is a very economical way of avoiding security threats whilst simultaneously boosting staff productivity and increasing the flexibility of your network. It is called an Internet Gateway Management Service (IGMS).

The electronic threats to any organisation's network vary from the annoying (spam) to the malicious (viruses) to the outright criminal (theft of data). Sometimes these menaces originate from outside the organisation. But more often, they are the result of employee behaviour and occur from visiting corrupted websites or opening hoax email attachments.

The costs of these attacks obviously vary and are sometimes hard to calculate. Is it a case of lost time? The loss of confidential data? The loss of customer goodwill? What can be shown is that in financial terms the effects of a compromised network can be devastating. The AusCERT Australian Computer Crime and Security Survey (2006) listed theft of proprietary information as the single greatest source of security-related loss for Australian corporations, with an average cost being greater than \$2 million.

The challenge is greater when there are staff operating across multiple facilities, on the road or from home. This entails either setting up a dedicated private network (expensive) or using the public Internet to allow staff to log into central resources remotely. However, whilst the Internet provides a serviceable and low-cost option, this approach does leave a large breach in security.

*Sometimes these menaces originate from outside the organisation. But more often, they are the result of employee behaviour and occur from visiting corrupted websites or opening hoax email attachments*

*Threatening and suspect sites can be easily and automatically blocked through a continually-updated list. This closes the biggest loophole in data security: employee behavior. Even when employees make innocent mistakes, the IGMS provides a safeguard.*

Any traffic over the public Internet is open to compromise, either deliberate or accidental. All kinds of malware can be imported into internal systems, leaving the organisation open to the threat of intrusion, system failure and loss or theft of data.

An IGMS can help plug this security gap in an efficient and inexpensive way. The best of these services can combine firewall, web filtering, email sanitization, infection isolation and reporting features into a single service. They work by combining some simple on-site equipment that interfaces with a remote Network Operations Centre run by the service provider – similar to the way that a pay TV box works. This installation should be as simple as plugging in the box, and because it sits between the Internet and the user's systems, there will be no need for expensive upgrades to existing IT equipment or software.

The IGMS is much more than a simple anti-virus program. It creates an encrypted network, offering a certified level of enterprise level security whilst still working via the public Internet. Staff in branch offices or temporary sites can log into centralized systems over a phone line and have the same level of security as if they were in the same building. The automatic detection and elimination of intrusions and worms offers an immediate solution to these types of attacks and a good IGMS can instantly identify a compromised computer and quarantine it, leaving the rest of the network to continue on with business.

Additionally, the control functions of a good IGMS mean that employee Internet usage can be monitored and controlled. Threatening and suspect sites can be easily and automatically blocked through a continually-updated list. This closes the biggest loophole in data security: employee behavior. Even when employees make innocent mistakes, the IGMS provides a safeguard.

At a time when every organisation needs to watch its budget, a reputable IGMS offers a networking functionality that puts local government authorities on a par with the biggest private firms, at least in terms of network security...and all at a fraction of the price.