

LAN POLICING INCREASES PRODUCTIVITY...

THE PROBLEM

- Inappropriate messaging and website viewing on the corporate network during office working hours
- Excessive bandwidth usage resulting from inappropriate uses of the internet, slowing the corporate network
- Identifying the individuals misusing the internet
- Maintaining appropriate and professional standards

THE SOLUTION

The installation of a LAN Policing for Productivity (LPP) appliance. The appliance manages the traffic within a network, ensuring network protection in the following ways:

- High degree granular control prevents inappropriate website viewing, thus the network is protected and professional standards are upheld
- Excessive and unnecessary bandwidth usage is limited
- The identification of individual users abusing internet privileges

WHY AN LPP APPLIANCE?

The LPP appliance provides a complete solution; comprising hardware and InterGate software. Additionally, the LPP appliance prevents the use of instant messaging, peer to peer, Skype and video streaming. Not only does this allow the network to operate at its required speed, it also prevents possible security breaches of the network and stops potentially harmful contents being viewed.

To counteract those who abuse network privileges, intelligent reporting not only identifies the IP address, it also distinguishes between individual users. The ability of administrators to police the network provides assurance to senior staff members that employees are using the internet in the most efficient and productive way. Additionally, maintaining professional standards on the corporate network limits the possibility of viruses attacking the network and being sent to clients via email.



High Performance Traffic Management from Keyfort

Corporate networks are continually facing advancing threats from email traffic, thus the protection needed to guard them needs to be just as sophisticated. The Email Management System with multi-threaded policy & compliance provided by Keyfort is one such system. It provides for:

- A cleaner, safer corporate network
- The enforcement of organisational email policies
- The monitoring and control over inbound and outbound email traffic
- The monitoring of email traffic
- Identification of emails that do not comply with set policies
- Less than 10 minutes a week spent administering emails, freeing up the IT team
- Corporate information is protected against network attacks

WHAT IS ALL THIS EMAIL MANAGEMENT TALK?

Like many tasks in life, stopping spam, viruses and phishing emails does not have a one off solution. It's an ongoing task requiring clear thinking, rapid acquisition of intercept information and an ability to adapt rapidly to meet new threats. Good email management systems do this by using analytical theorems and by 'talking' to focal intelligence servers on the Internet, thus keeping abreast of spam/virus/phishing outbreaks (time zero response) followed up by virus signatures which become available in the subsequent hours.

Whereas the finer definition of spam depends upon the interests of the recipient, all virus and phishing emails need to be blocked before they reach the recipient. In addition, internally generated emails including email shots, attachments and inappropriate words require an email policy defined by user/department/organization and time of day. Therefore a good email system not only needs to differentiate between email types to be blocked, but it must also be able to differentiate between internal users and apply the organization's email policy accordingly.