

EQUIINET WHITE PAPER

Virus Scanning at the Internet Gateway

The Internet has made information available to more people more quickly than ever before. While overwhelmingly positive in general, the downside is that the Internet has also made it easier for harmful computer code to reach office and home computers.

We live in an information age when new viruses are appearing on a daily basis and those viruses that command the most media attention are not necessarily the biggest problem. Once on your LAN (local area network) computers, viruses can destroy data, damage entire networks and cause computer crashes, as well as being used as delivery mechanisms for hacking tools.

More and more organisations are opting for the peace-of-mind of virus scanning at the gateway, or boundary, of their local network and the Internet. Such ‘boundary scanning’ acts both as a complement to desktop virus scanning and directly tackles the growing threat of email-based viruses.

This paper examines the driving forces behind this trend and the solutions that are being developed.

The problem with emails

A recent survey conducted for message managers Pitney Bowes found that the average Fortune 1000 employee was handling 50 emails a day. Large organisations can receive upwards of 50,000 mail messages a day, some getting as many as a million.

According to technology analysts IDC, by 2005 there will be 35 billion emails sent daily. This level of traffic combined with the proliferation of email-aware viruses means that email is now the main route by which viruses enter organisations. Some companies can stop tens or even hundreds of viruses a day at the gateway.

Tiers of virus protection

Scanning at the gateway is one of a number of tiers of virus protection that an organisation can choose to implement. While this paper stresses the benefits of gateway scanning, virus checking at the desktop, in local file servers and via managed services are all valuable and valid forms of protection.

Desktops, laptops and other end-user devices are at the heart of an organisation and this is where virus scanning has traditionally focused. Gateway scanning sits above all the organisation's PCs and servers – at the boundary between the local LAN and the external Internet. The outermost tier of virus scanning, involves managed services run by a third party – such as an ISP – which typically reside outside the organisation.

Why scan at the Gateway?

Gateway scanning offers organisations a new level of security at the network's boundary and can be used either as a second line of defence for organisations with PC-based virus scanning, or as an alternative to the administrative headache of loading anti-virus software onto individual PCs. It also takes responsibility for protection and updates away from the individual user, and once set up relieves the network manager from the bigger responsibility of worrying about the whole organisation.

Often the network manager in small and medium sized organisations is undertaking this role on a part time basis – he also has another full time job to undertake. Having the time to implement virus signature and engine updates across numerous different PCs with differing operating systems is not an ideal or realistic proposition – nor is relying on individual users to get it right. Put in this position, network managers are seeking simplification and hence view the automation of gateway or external managed solutions as attractive.

However attractive the thoughts of letting an external organisation solve the problem, this is not the total solution either. A major benefit for gateway (and indeed desktop) solutions

over externally managed services is that they scan for viruses in emails sent across an internal network – i.e. all emails sent between fellow employees of the same organisation will flow through the gateway's virus scanner and stop internally generated infection. Other major benefits over external services include, the ability to block viruses emanating not only from the organisation's designated main email accounts, but also any other mail accounts at other ISPs, that are used on a permanent or ad hoc basis. For example a rogue user collecting email from a private account to his desk-top PC, will by-pass the external managed service and potentially infect the whole organisation.

Where gateway scanning particularly adds value above and beyond both simple desktop and external scanning is when networks are opened up for mobile users and visitors temporarily plug their notebooks into a network. While a network manager may be able to implement adequate policies and actual deployment of anti virus solutions on desktop PCs, the likelihood is he has far less control over portable computers. These PCs, by their very nature, are more likely to have anti virus solutions that are not kept up to date and are being connected to multiple sources of infection. Scanning at the gateway automatically prevents viruses being spread by visitors or mobile workers when they connect into the organisation's LAN.

Gateway scanning works by checking emails against pre-loaded 'virus signatures'. If they contain any viruses, the email will be quarantined or deleted and warning emails describing the problem can be sent to the sender, the addressees and the administrator.

Such a process makes life much simpler for the administrator as the gateway device – usually an email server or a multifunctional server appliance - automatically keeps things up to date. It's also far simpler for the ordinary computer user, because the anti-virus process is completely transparent. Experience has shown that automation of Internet and email security is vital, as PC users rarely do what's good for them if left to their own devices.

Another significant added benefit of gateway scanning is that it relieves pressure on an organisation's precious bandwidth by facilitating updates through a central point rather than numerous PCs updating individually. The gateway device can receive updates centrally, and then download them to individual PCs on the network.

Whilst viruses obtained via web browsing are less of an issue than email-based viruses, similar gateway solutions are also being introduced to combat web-based viruses. Again, this battle has traditionally been fought at the desktop level, with all the resulting administrative and efficiency drawbacks already addressed in this paper.

The Gateway device

Gateway virus scanning functionality is contained within a device such as an email server or a multifunctional server appliance (which incorporates an email server) that sits at the edge of the network. Most organisations sending and receiving emails will have an email server and an increasing number are opting for server appliances, which give them comprehensive functionality in one straightforward package.

Secure server appliances go beyond acting as email server with in-built virus scanning capabilities – they additionally act as a router, a firewall, a web server, a file server, a cache and a content filter all in a plug-and-play device that is simple for the layman to install. They are ideal for smaller businesses where there's limited IT expertise on staff, although they are equally applicable in larger organisations where they can piggyback onto existing equipment even if there's no need for all their functionality. The server appliance is also the obvious place to implement a corporate wide security policy. Not only can it undertake corporate wide virus checking, it can undertake a wide spectrum of other security, control, and value added services.

A server appliance will support standard protocols such as SMTP (Simple Mail Transfer Protocol) and POP (Post Office Protocol) and can act in combination with other servers running email products such as Lotus Notes/Domino and Microsoft Exchange, and are

particularly effective where the security scanning and filtering overhead is off loaded to the appliance to process.

The server appliance can also assist in a multi-tiered anti-virus approach. It can perform the gateway virus scanning functions, and in addition act as a central storage location for desktop virus signature deployment amongst attached PCs. Particularly where organisations are running peer to peer networks, or do not want to devote file server resources to desktop AV distribution – these task can be undertaken by the server appliance.

Secure server appliance suppliers such as Equiinet have continually added to the functionality their products offer and the introduction of subscription-based virus scanning has been a natural extension of the product offering.

In Equiinet's case, their NetPilot device incorporates the SAVI virus scanning software from Sophos Anti-Virus and customers subscribe for regular signature updates as new viruses are discovered.

Sophos, based in the UK like Equiinet, has detected and protected against more than 6,000 new viruses in the first six months of 2002, showing how quickly new dangers proliferate.

Conclusion

The war against computer viruses needs to take place on many fronts and encouragingly there are now multiple complementary solutions to help in this fight. In today's communication age, gateway scanning is playing a vital role in keeping corporate networks free from the dangers that lurk in emails and on websites.

Summary

The following is Equiinet's view of the various Pros and Cons of the three major virus-scanning approaches.

Virus Checking at the Internet Gateway

Pros

The ideal place to implement an organisation wide all-embracing security policy.
Centralised installation, administration, and updates.
Typically more cost effective than desktop solution.
Other content and porn scanning services.
Can block web downloads as well as virus scan emails.
Checks internal mail for local LAN infection.
Prevents infection when users collect from alternative or private email accounts.
Ensures portable PCs plugging into local LAN are scanned.

Cons

Cannot prevent single station infection via floppy or CD etc.

Virus checking on the User PC

Pros

Prevents infection via floppy or CD etc.
Detects viruses from email or web downloads.

Cons

Needs to be rigorously administered and kept up to date on all desk-top and portable PCs
Typically the most expensive solution per station.
Needs separate management station for enterprise solution administration.
Provides no other value added services or security measures.

Virus Checking via External Third Party Service

Pros

Third party takes responsibility for installation and updates.
Some services use multiple virus scanning engines.
Some services offer other useful scanning services e.g. porn.

Cons

Only scans emails - not downloads or browser traffic.
Cannot prevent infection when users collect from alternative or private email accounts.
Cannot virus check internal mail for locally created infection.
Third party has access to all your incoming/out going emails and may archive them.

	Administration Overhead	Prevents local LAN Infection	Scans/Blocks Web Downloads	Comparative Cost	Other Services
Gateway/Email Server	Medium	Yes	Yes	Low to Medium	Yes
Desktop	High	Yes	Yes	Medium to High	No
Third Party Service	Low	No	No	Medium	Provider dependent