



- ▶ [Latest \(all topics\)](#)
- ▶ [Top stories](#)

- ▶ [All-in-One printer](#)
- ▶ [Apple Mac](#)
- ▶ [Audio](#)
- ▶ [Backup](#)
- ▶ [Book](#)
- ▶ [Broadband](#)
- ▶ [Camcorder](#)
- ▶ [CD drive](#)
- ▶ [Desktop PC](#)
- ▶ [Digital camera](#)
- ▶ [DVD drive](#)
- ▶ [Gaming](#)
- ▶ [Graphics card](#)
- ▶ [Hard disk](#)
- ▶ [Input device](#)
- ▶ [Laptop](#)
- ▶ [LCD](#)
- ▶ [Mobile phone](#)

Look To The VLAN To Tighten Security



[ENLARGE](#)

Organisations need to build several layers of security into each port on the IP-enabled corporate network if they are to fully protect themselves from DOS and DDOS attacks.

Recent calls for ISPs to bear more responsibility for the prevention of denial of service attacks have set the scene for much-needed debate on the neglected issue of VLAN security. Although improved communication between ISPs and their business customers would undoubtedly help, organisations must take the initiative in protecting each and every port on the corporate network if they are to stay safe.

The strong uptake of IP-enabled technology - that is, devices that operate outside the firewall - means that it is already too late for

industry to rely on a changed approach from ISPs.

Vendors and resellers alike can now step in to demonstrate their knowledge of techniques such as rate limiting, which can restrict the flow of information per second through a particular port - keeping just enough bandwidth available for critical applications, but preventing external attacks from having any impact on the enterprise network. The prioritisation of traffic, so that protocols such as SIP can be granted special privileged status, is an additional benefit of this technology.

Put simply, IP-enabled devices within a virtual network must be protected from each other, and not only threats originating from outside the network. The popular approach to network security fails to take this fact into account, and instead merely applies the tried-and-tested ACL list to a virtual network.

The Access Control List (ACL) has been a central feature of the secure network since the mid 1990s. ACLs are simply a list of permit/deny rules relating to an IP address or socket number, identifying a particular user or the service a user is attempting to run.

Traditionally this list is accessible via and applied to the router interface itself. While it makes sense to continue providing the tried-and-tested onboard ACL on the router interface, there is a clear need for change as hackers are constantly altering their tactics in the drive to exploit vulnerabilities and break into the corporate network.

The weak point of a traditional ACL is that there are so many lines to input. It is rarely possible to deliver these lines via a system level graphical management tool - instead the process is usually command line driven - and therefore it is necessary to open a console and connect to each individual router to make the configurations.

When an enterprise must handle a high quantity of edge switches on a port-by-port basis the process can become unmanageable. The need for change is now clearly in evidence and would ideally involve building layers of security into each port, so that interaction between new devices can be controlled and a specific class of service guaranteed.

With virus writers and hackers constantly changing tactics, enterprises must make the effort to understand how and why they can stay one step ahead of the game. The devastating effect a simple DDOS attack can have on an unprotected port demonstrates well how even the most dated, well-known and heavily documented methods of attack can cripple day-to-day business operations if a business has not already taken preventative action.

All the indications are that the IP-enabled device is the future for the corporate network, and if organisations are keen to reap the benefits of this technology then they must consider the security implications carefully. If the process is closely managed, IP technology can provide genuine business value without putting the network at unnecessary risk.

Rate limiting is also a measure that allows organisations to fine tune policy and ensure that nothing is left to chance. Resellers should be using this expertise to empower their customers to think beyond theory, which is what the recent debate over ISP responsibilities has amounted to. They cannot afford to be absorbed into the hype cycle and have their actions determined by political wranglings that are beyond their control and may not reach the desirable conclusion in the long run.

Dean Jones, Enterasys Networks, 20.12.05

[Comments \(0\)](#)