



Could rate limiting be the end of DOS?

IP-enabled technology brings its own range of problems to a network. Could rate limiting be the solution, asks **Dean Jones**

» 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 denial-of-service (DOS) and distributed denial-of-service (DDOS) attacks.

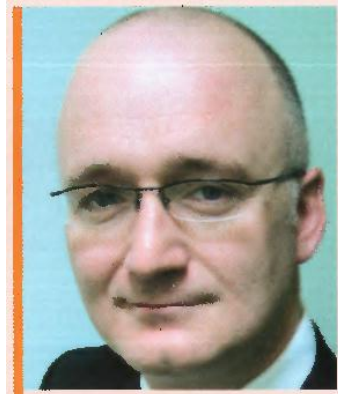
Recent calls for ISPs to bear more responsibility for the prevention of DOS attacks have set the scene for debate on the neglected issue of Virtual LAN security. Although improved communication between ISPs and their business customers would help, organisations must take the initiative in protecting every port on their corporate network if they are to stay safe. The uptake of IP-enabled technology (devices that operate outside the firewall) means that it is too late for industry to rely on a changed approach from ISPs.

VARs can step in here to demonstrate their knowledge of techniques, such as rate limiting, which can restrict the flow of information per second through a particular port. This keeps just enough bandwidth available for critical applications, but prevents external attacks from having any impact on the network.

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

Although the ACL has been a central feature of the secure network since the mid-1990s, it is no longer sufficient as a standalone measure. ACLs are simply a list of permit/deny rules relating to an IP address or socket number. They identify a particular user, or the service a user is attempting to run. Traditionally this list is accessible via the router itself. While it makes sense to continue providing the onboard ACL on the router interface, there is a need for change as hackers constantly alter their tactics.

The main weakness of ACL is that there are so many lines to input. It is



Dean Jones: Organisations must take the initiative in protecting every port on their corporate network if they are to stay safe.

not possible to deliver these lines via a tool as the process is command-line driven. Instead, it is necessary to open a console and connect to each single 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. Instead, layers of security must be built into each port if interaction between new devices is to be controlled and a specific class of service guaranteed.

Multi-layer frame classification can offer the same level and quality of ACL capability, but in a switch environment, rather than a routing environment. This provides the level of sophistication necessary to address this problem. Layers of security must be built into each port.

Closer consultation between ISPs and their customers would be useful, but this is speculative talk and will fall short of fully protecting networks from intrusion, even if it is successfully realised. Rate limiting is among the most effective means of fighting DOS and DDOS attacks. It allows organisations to fine tune policy and ensures that nothing is left to chance.

Resellers should use this expertise to empower their customers to think beyond theory. They cannot afford to be absorbed by hype, nor to have their actions determined by political wranglings that are beyond their control, or they may not reach the desirable conclusion in the long run.

Dean Jones is UK channel manager at Enterasys Networks.