SOCKS SERVER

Deserving of brief special attention is the SOCKS firewall implementation. SOCKS is the protocol for handling TCP traffic through a proxy server. The SOCKS system is a proprietary circuit level proxy server that places special SOCKS client-side agents on each workstation. The general approach is to place the filtering requirements on the individual workstation rather than on a single point of defense (and thus point of failure). This frees the entry router from filtering responsibilities, but it then requires each workstation to be managed as a firewall detection and protection device. A SOCKS system can require support and management resources beyond those usually encountered for traditional firewalls since it is used to configure and manage hundreds of individual clients as opposed to a single device or small set of devices.

Selecting the Right Firewall

When selecting the best firewall for an organization, you should consider a number of factors. The most important of these is the extent to which the firewall design provides the desired protection. When evaluating a firewall , questions should be created that cover the following topics:

1) What type of firewall technology offers the right balance between protection and cost for needs of the organization.
2) What features are included in the base price? What features are available at extra cost? Are all cost factors known?
3) How easy is to set up and configure the firewall?How accessible are the staff technicians who can competently configure the firewall?
4) Can the candidate firewall adapt to the growing network in the target organization?

The second most important issue is the cost. Cost may keep a certain make, model or type out of reach for a particular security solution. As with all security decisions, certain compromises may be necessary in order to provide a viable solution under the budgetary constraints stipulated by management.

Configuring and managing Firewalls:

Once the firewall architecture and technology have been selected, the initial configuration and ongoing management of the firewalls needs to be considered. Good policy and practice dictates that each firewall device whether a filtering router, bastion host, or other firewall implementation, must have its own set of configuration rules that regulate its actions.

In theory packet filtering firewalls use a rule set made up of simple statements that regulate source and destination addresses identifying the type of requests and /or the ports to be used and that indicate whether to allow or deny the request.

In actuality, the configuration of firewall policies can be complex and difficult. IT professionals familiar with application programming can appreciate the problems associated with debugging both syntax errors and logic errors. Syntax errors in firewall policies are usually easy to identify, as the systems alert the administrator to incorrectly configured policies. However, logic errors, such as allowing instead of denying, specifying the wrong port or service type, and using the wrong switch, are another story.

These and a myriad of other simple mistakes can take a device designed to protect user‘s communications and turn it into one giant choke point.

A choke point that restricts all communications or an incorrectly configured rule can cause other unexpected results. For example, novice firewall administrators often improperly configure a virus-screening e-mail gateway, which, instead of screening e-mail for malicious code, results in the blocking of all incoming e-mail and causes, understandably, a great deal of frustration among users.

Configuring firewall policies is as much an art as it si a science. Each configuration rule must be carefully crafted, debugged, tested, and placed into the access control list in the proper sequence. The process of writing good, correctly sequenced firewall rules ensures that the actions taken comply with the organization‘s policy. The process also makes sure that those rules that can be evaluated quickly and govern broad access are performed before those that may take longer to evaluate and affect fewer cases, which in turn, ensures that the analysis is completed as quickly as possible for the largest number of requests. When configuring firewalls , keep one thing in mind: when security rules conflict with the performance of business, security often loses. If users can‘t work because of a security restriction, the security administration is usually told, in no uncertain terms, to remove the safeguard. In other words, organizations are much more willing to live with potential risk than certain failure. The following sections describe the best practices most commonly used in firewalls and the best ways to configure the rules that support firewalls.