CONTENT FILTERS

Another utility that can contribute to the protection of the organization‘s systems from misuse and unintentional denial-of-service, and is often closely associated with firewalls, is the **content filter.**

A content filter is software filter-technically not a firewall –that allows administrators to restrict access to content from within a network. It is essentially a set of scripts or programs that restricts user access to certain networking protocols and internet locations, or restricts users from receiving general types or specific examples of Internet content. Some refer to content filters as reverse firewalls, as their primary focus is to restrict internal access to external material. In most common implementation models, the content filter has two components: rating and filtering. The rating is like a set of firewall rules for Web sites, and is common in residential content filters. The rating can be complex, with multiple access control settings for different levels of the organizations, or it can be simple, with a basic allow/deny scheme like that of a firewall. The filtering is a method used to restrict specific access requests to the identified resources, which may be Web sites, servers or whatever resources the content filter administrator configures. This is sort of a reverse control list (A capability table), in that whereas an access control list normally records a set of users that have access to resources, this control list records resources which the user cannot access.

The first types of content filters were systems designed to restrict access to specific Web sites, and were stand –alone software applications. These could be configured in either an exclusive manner. In an exclusive mode,, certain sites are specifically excluded. The problem with this approach is that there may be thousands of Web sites that an organization wants to exclude, and more might be added every hour. The inclusive mode works off a list of sites that are specifically permitted. In order to have a site added to the list, the user must submit a request to the content filter manager, which could be time-consuming and restrict business operations. Newer models of content filters are protocol

–based, examining content as it is dynamically displayed and restricting or permitting

Access based on a logical interpretation of content.

The most common content filters restrict users from accessing Web sites with obvious non-business related material, such as pornography, or deny incoming spam e-mail. Content filters can be small add-on software programs for the home or office, such as Net Nanny or surfControl, or corporate applications, such as the Novell Border manager. The benefit of implementing content filters is the assurance that employees are not distracted by non-business material and cannot waste organizational time and resources. The downside is that these systems require extensive configuration and on-going maintenance to keep the list of unacceptable destination or the source addresses for incoming restricted e-mail up-to-date. Some newer content filtering applications come with a service of downloadable files that update the database of restrictions. These applications work by matching either a list of disapproved or approved Web sites and by matching key content words, such as ―nude” and ―sex”. Creators of restricted content have, of course, realized this and work to bypass the restrictions by suppressing these types of trip words, thus creating additional problems for networking and security professionals.

Source : http://elearningatria.files.wordpress.com/2013/10/ise-viii-information-and-network-security-06is835-notes.pdf