Tech Overview : IM and P2P Management

The Necessity for IM & P2P Management

Businesses not only have to confront the hidden information security risks that come along with instant messaging software but also the heavy bandwidth usage caused by peer-to-peer (P2P) software. The majority of businesses choose not to block them, and simply rely on the trust from their employees that they will use them appropriately. Even though P2P should be banned, IM software provides businesses with considerable convenience. The dilemma often encountered is whether to ban them completely or allow employees to continue secretly using them for non-work related chat.

Powerful Management Controls

An array of management controls are provided by the Nusoft Internet Recorder. Not only can it effectively block a range of bandwidth-intensive P2P software, it can also place restrictions for users to access IM software to ensure businesses can continue enjoying the benefits that they bring.

Gain Complete Control over P2P Software

IP addresses can be used as the management basis for determining whether to block or allow users from using P2P software. Complete blocking or permitting can be configured. Under normal circumstances, it's recommended for business to completely block the use of P2P to avoid potential virus infections and business bandwidth depletion. Currently Nusoft Internet Recorder is capable of blocking eDonkey (eMule) , BT, WinMX, Foxy, KuGoo, AppleJuice, AudioGalaxy, Direct Connect, iMesh, MUTE and Thunder 5.

Gain Complete Control over IM Software

The management of instant messaging software can be implemented through any particular user's instant messaging logon name or IP address. Management controls of users are not just limited to completely blocking or allowing instant messaging software, they also include:

- Allow users access only after successful authentication with the device or through RADIUS, LDAP, or a mail server.
- Block encrypted instant messaging to ensure the integrity of the business's security.
- Block any file transfers made through instant messengers, to protect any confidential business files from being leaked out.
- Allow or block specific user's access to instant messaging software.

Nusoft Internet Recorder will also block any users attempting to go through web messengers as well as record their conversations, effectively preventing any employees from evading the company's Internet policies. The list of currently supported web-based instant messengers includes MSN (official MSN Web Messenger) , Yahoo Messenger, QQ, ICQ, AIM, Skype, Google Talk and Gadu-Gadu.

Signature patterns are utilized by the Nusoft Internet Recorder as a means of analysing transmitted packets, so any attempts by users to modify the connection's port number with the aim of avoiding detection will be ineffective. In addition, new signature patterns are constantly being revised by Nusoft's research team to ensure its ongoing effectiveness.

Product News : An Economical Solution for Small and Medium-Sized Businesses

Introducing the NUS-IR950

The NUS-IR950 is designed to record the online activities of up to fifty users. Ever since it was released in spring 2008, it has become the ideal choice for small and medium-sized businesses. It comes equipped with a multitude of functions, but it's only one-third of the price in comparison to other models in the Nusoft Internet Recorder series. Thus, it represents the best choice for small and medium-sized businesses.

Various Features Accommodate and Protect Your Network

Bridge mode and Sniffer mode deployment are available for selection, with the addition of a bypass function to protect the network during a hardware failure. When Bridge mode is utilized, it provides the most effective management of the network, whereas Sniffer mode has no influence on the network.

Remote backup allows recorded data to be backed up to a NAS, file server, Samba server, etc. The device's web UI can then be used to view records. With Remote Backup, there is no longer the worry of a lack of storage space due to the devices internal storage limitations.

When an internal PC disrupts the network by emitting an abnormal amount of packets, as would be the case when infected by a virus, the NUS-IR950 will provide an instant alert notification. If Bridge mode is deployed, the device can go one step further and immediately block the transmission of these packets, effectively protecting the normal operation of the network.

Increased Employee Productivity

In addition to providing the above-mentioned P2P and instant messaging management, the device records all of the internal employees' online activities including web-based email service and sessions created from FTP and Telnet connection. The overall result is a dramatic increase in employee productivity during working hours.