Tech Overview : Effective Record Searching

Businesses utilize developments in Internet technology to improve efficiency across a range of different areas such as communication. However, the Internet creates avenues for employees to use this technology discretely for non-work related activities, even to the extent of leaking confidential business information.

Monitoring employees' use of the Internet during business hours is of significant importance to businesses. The Nusoft Internet Recorder series (NUS-IR2500, NUS-IR1800 and NUS-1000G) excels at recording the online activities of employees in comparison to third-party firewalls.

Taking the NUS-IR2500 as an example, the device analyses all packets passing through the network in detail. Statistics provided via the management interface give a clear insight into the state and activity of the network. The characteristics of each packet such as the service (e.g., HTTP, instant messaging, etc.) and the associated user can be viewed.

Comprehensive Search Function

All the commonly used services, such as HTTP, SMTP, POP3, IM, FTP, Telnet and web-based SMTP/POP3 email can be recorded in the device's database. Using the search criteria provided by the device makes it easy for the IT administrator to locate any desired record.

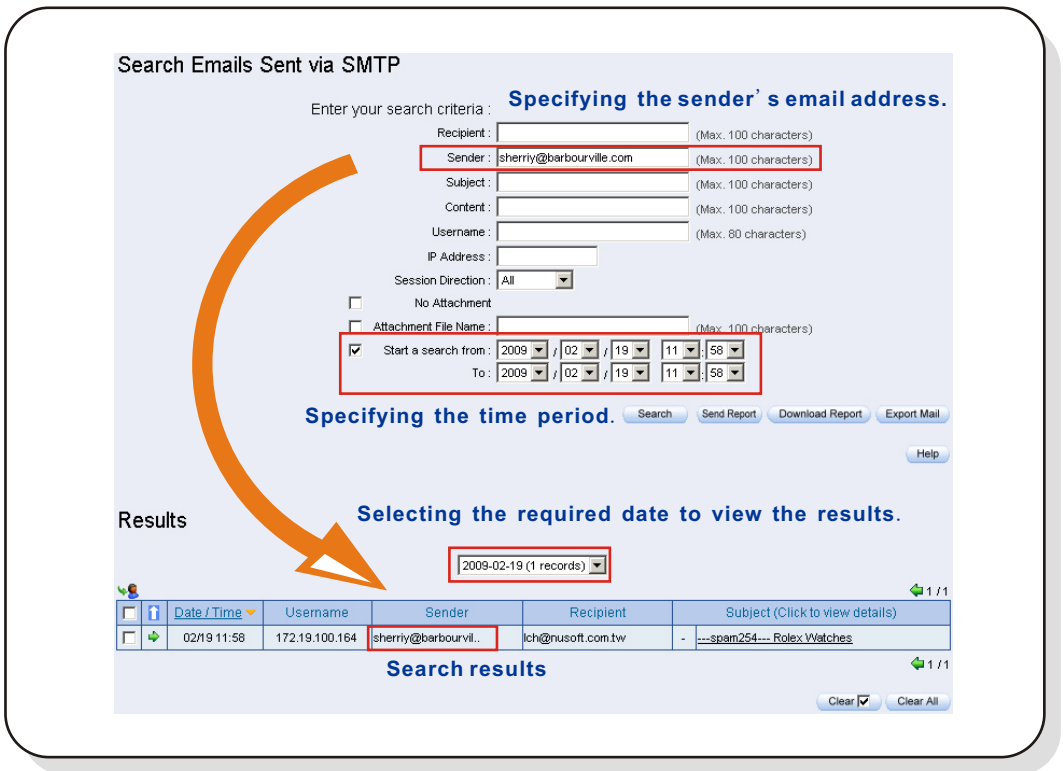

Figure 1 Searching a Web-Based SMTP Email

The above example shows an SMTP search. After the criteria were entered, the drop-down list shows the results from the selected date.

Email Content Viewing

This function provides a valuable tool for preventing the leakage of confidential information. The device will check inside the content of every email to locate any results matching the specified search criteria.

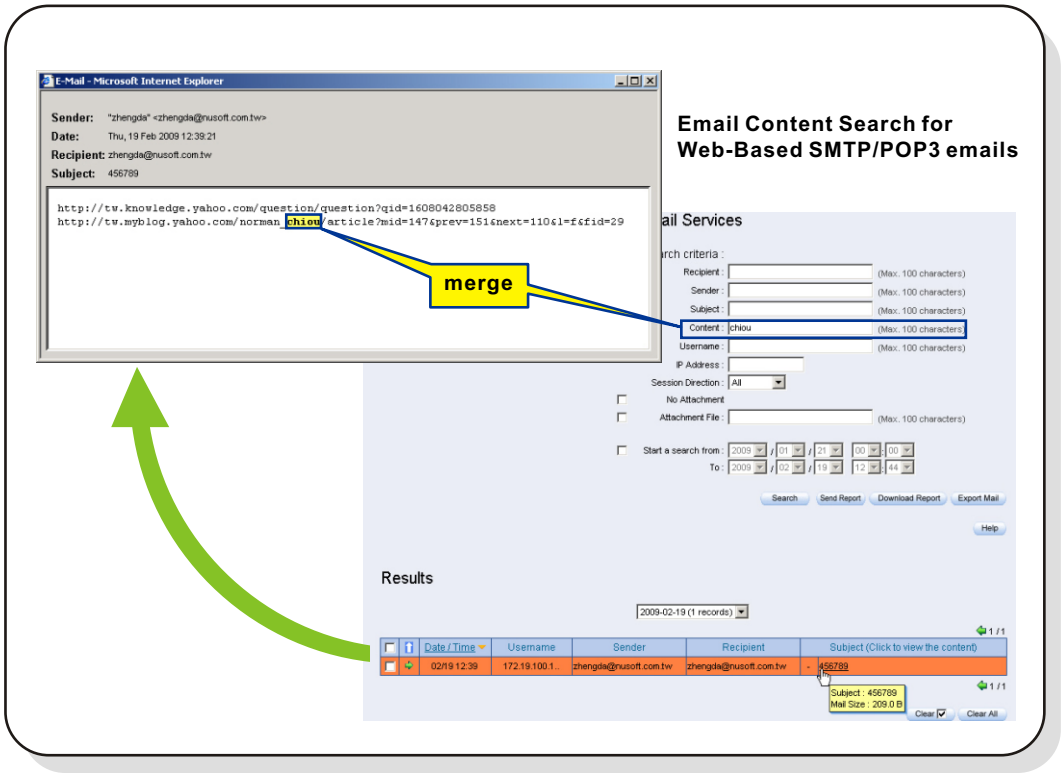

Figure 2 Searching a Web-Based Email by Its Content

As per the picture above, the device will locate any emails containing the keyword “merge”. From the returned search results, the device will also highlight the keyword from within the email making it easier to see.

Product / Search Capability	Nusoft Internet Recorder	Third-Party Internet Recording Devices
Major Services	Search criteria based on various email characteristics, allows a quick retrieval of the required email.	1. Regular email: Unable to search the contents of an email or its attachments. 2. Web-based email: Unable to search by sender, recipient, subject, content, etc. due to utilizing snapshots to record web-based emails accessed by users. 3. IM: The majorities are unable to search IM conversations or transferred files. 4. HTTP: Most only provide searches based on the URL and are incapable of searching based on the website's title or content.
Email Contents	Searches the contents of every emailbased on keywords, effectively preventing the leakage of any sensitive business information.	

Table 1 Search Capability Comparisons

Product News : Behavior Management Mechanisms

Despite the benefits that the Internet brings to businesses, the estimated cost of cyberslacking is around $1 billion per year. Consequently, the need for Internet recording devices to curtail this behavior has become a necessity.

Some manufacturers' network devices claim to have behavior management functionality. These are often gateways incorporating recording capabilities, but produce a mass of unorganized recorded data. They may also have firewall functions, load balancing and simple management functions. Overall, they lack the required Internet recording and management capabilities required by businesses.

Internet Recording devices need to produce records based on detailed traffic flow analysis and work alongside the network's firewall. This is because a firewall only has limited control and behavior management capabilities. However, most devices come with an array of features but are unable to perform specific functions adequately. Nusoft Internet recorder addresses these deficiencies, and provides network management and monitoring to complete your company's firewall.

Nusoft Internet Recorder's Behavior Management Functions

◎ Instant Messaging Authentication

To manage employees' instant messaging use, authentication provides the ideal control mechanism to permit specific users. Multiple forms of authentication are available by the device. There is no need to install a separate authentication server, the IT administrator can choose to utilize the device's internal authentication. However, an external authentication server (e. g. , RADIUS, POP3, LDAP, etc.) can be utilized if available.

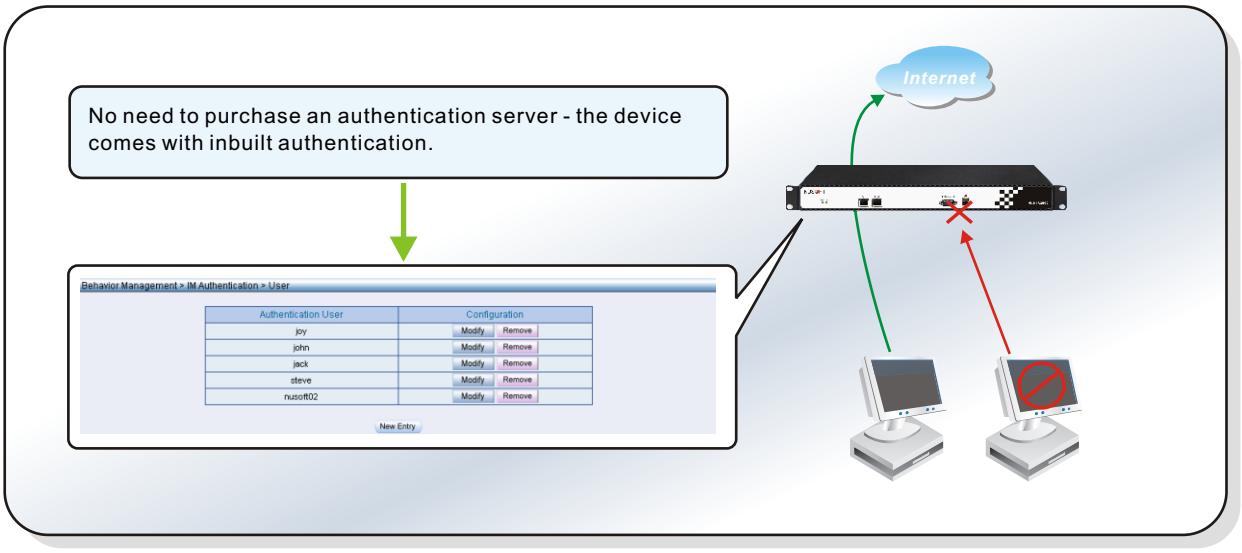

Figure 3 Utilizing the Device's In-built Authentication

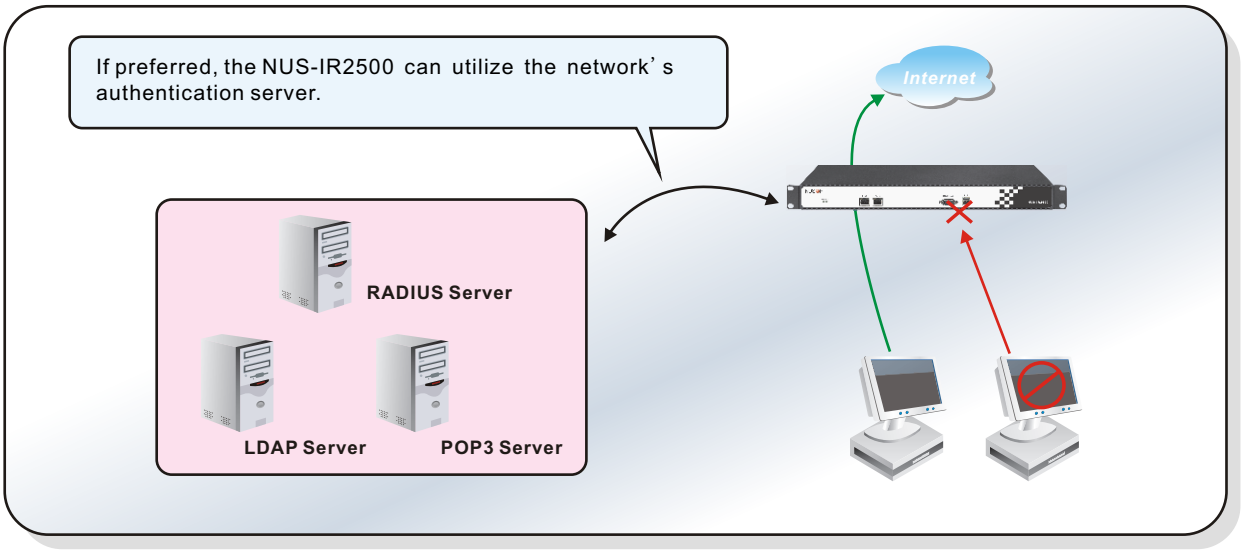

Figure 4 Utilizing the Network's Authentication Server

◎ Instant Messenger Management

Unlike most firewalls, the device effectively blocks specific users from using instant messaging software. Its management capabilities allow specific users or all users to be blocked. When all users are blocked, they can still be permitted access if they have successfully authenticated with the device. In addition, further management controls can be applied to each specific user, such as forbidding file transfers, etc.

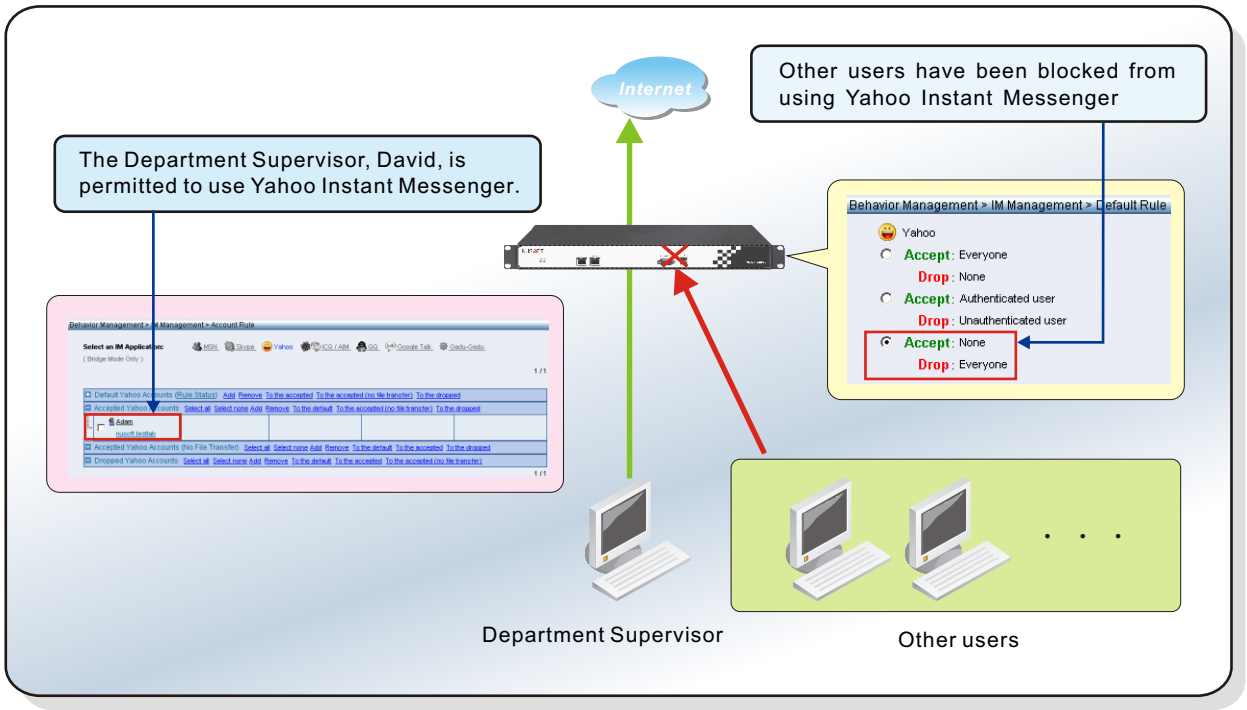

Figure 5 Controlling Users' Instant Messaging Use

◎ P2P Management

Most firewalls cannot effectively block the use of P2P software. This is due to the ease at which users can change their P2P software's port number to avoid being blocked. The device is able to block P2P software for everyone or selected individuals.

◎ Real-Time Flow Analysis (Excluding the NUS-IR1000G)

Most firewalls lack sufficient traffic flow analysis, and are incapable of providing important information. The Nusoft Internet Recorder is capable of analyzing traffic flow across the entire network and for individual users. This can pinpoint the service used and the bandwidth that a specific user occupied. The device can work in combination with company's existing firewall and provide effective network management.

The device's traffic flow analysis can be divided into 3 categories:

Category \ Product	Nusoft Internet Recorder	Third-Party Internet Recording Devices
Flow Statistics	Presents a chart visually showing the network's daily traffic flow rates. IT administrators are able to view what time an anomaly flow occurred.	1. Only provides traffic flow statistics for a fixed period. 2. Can only record from a limited number of services, any packets from an unsupported service will not be identified. 3. Unable to effectively identify users who are misusing the network.
Today Top-10	Provides statistics of the top 10 users, services and groups (or departments) based on the day's network traffic.	
History Top-N	Provides traffic flow statistics similar to the Today Top-10 but based on a past time.	

Table 2 Three Categories of Traffic Flow Analysis

◎ Anomaly Flow Detection

If an internal computer generates an anomaly traffic flow (resulted from a DoS attack), the Internet Recorder will block the traffic flow, preventing any adverse effect on the network or other computers. The device can also work with the core switch to help identify the location of the offending computer. An alert will also be issued to the IT administrator to take further action.

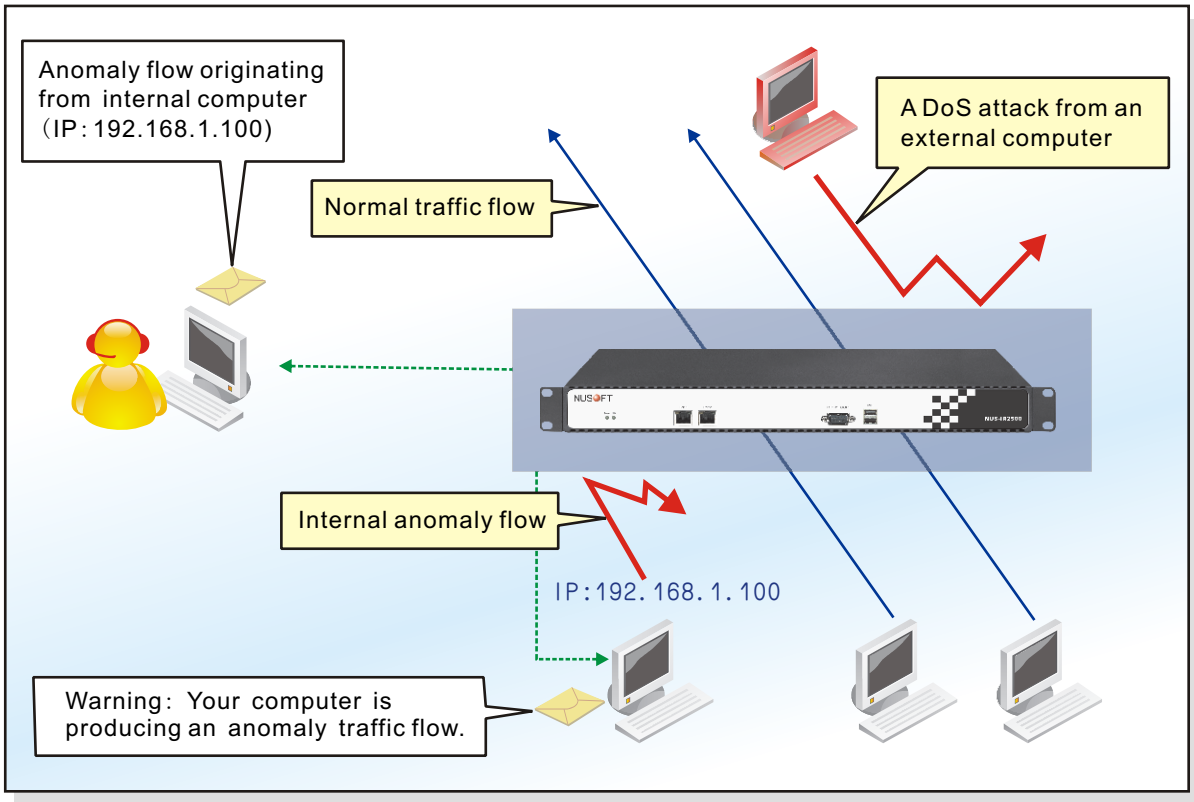

Figure 6 The Device Warns Both IT Administrator and the Victim for Anomaly Flow