Tech Overview : P2P Management Now Supported

The majority of businesses already have sufficiently large WAN bandwidth to conduct their normal business operations. However, when the network is subject to misuse, such as P2P file transfers, it has a significant detrimental impact. P2P activity not only slows down the network but also introduces further problems such as the leakage of confidential information, virus infections, etc.

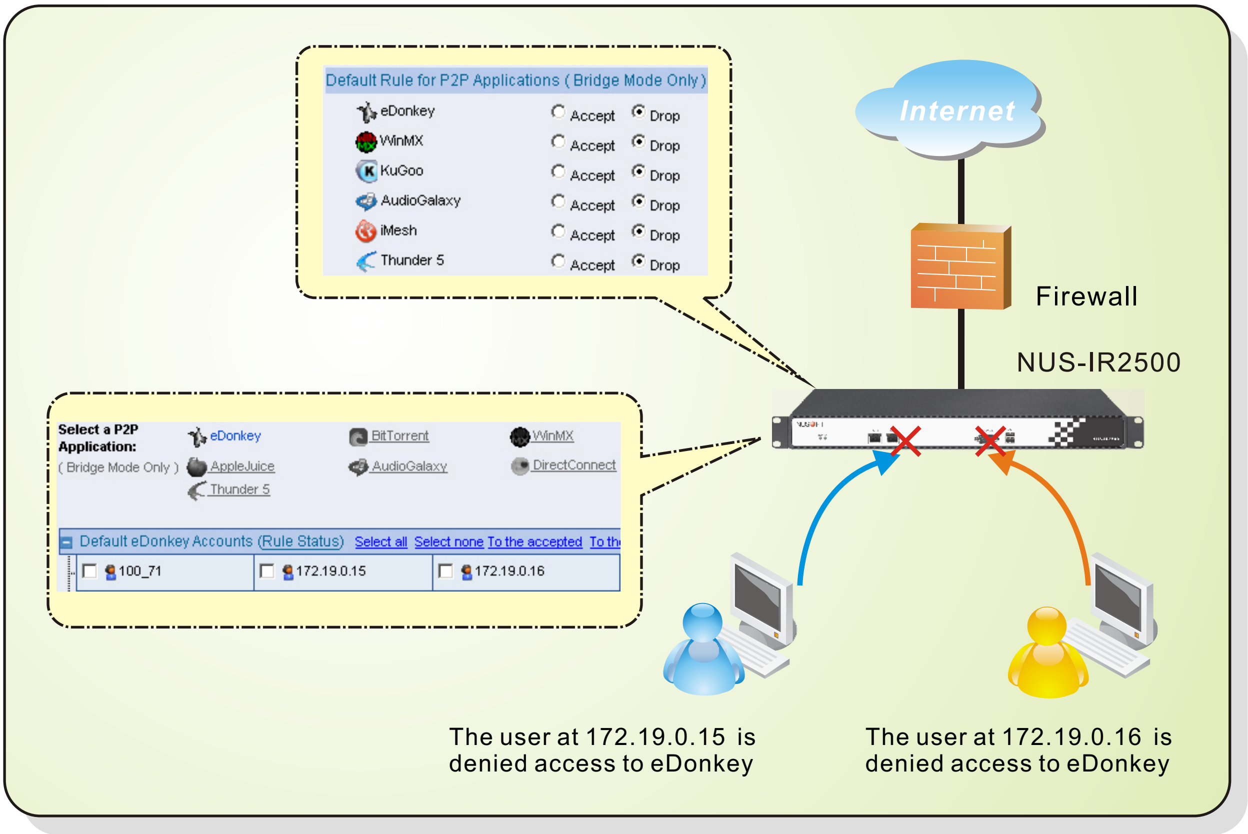
Firewalls can provide QoS by allocating the network bandwidth equally to each group or department. However, if one user in the group uses P2P software, others in the same group will be unfairly affected.

These days, many firewall devices on the market feature P2P blocking in order to meet the demand of businesses. But those devices block P2P activities based on the port number. Thus, it will be ineffective when the user modifies the connection port number with the aim of avoiding detection.

A few firewall devices on the market block P2P activities successfully because they can detect application layer packets. However, the disadvantage of those devices is that, the IT administrator needs to spend more time managing network utilization. When users intentionally changes the IP address or uses other PCs, the IT administrator constantly needs to reconfigure the "Policy" in order to ensure its ongoing effectiveness.

In order to make up for the shortcoming of P2P management, Nusoft Internet Recorder can manage the P2P activity completely.（By utilizing Bridge Mode）

Taking the NUS-IR2500 as an example, the device manages P2P software by analyzing transmitted packets. Thus, under the deployment of bridge mode, any device accessing the Internet through the NUS-IR2500 cannot use P2P software, no matter what settings they change.



Default Rule for P2P Applications (Bridge Mode Only)

eDonkey	○ Accept	● Drop
WinMX	○ Accept	● Drop
KuGoo	○ Accept	● Drop
AudioGalaxy	○ Accept	● Drop
iMesh	○ Accept	● Drop
Thunder 5	○ Accept	● Drop

Select a P2P Application:
(Bridge Mode Only)
eDonkey BitTorrent WinMX
AppleJuice AudioGalaxy DirectConnect
Thunder 5

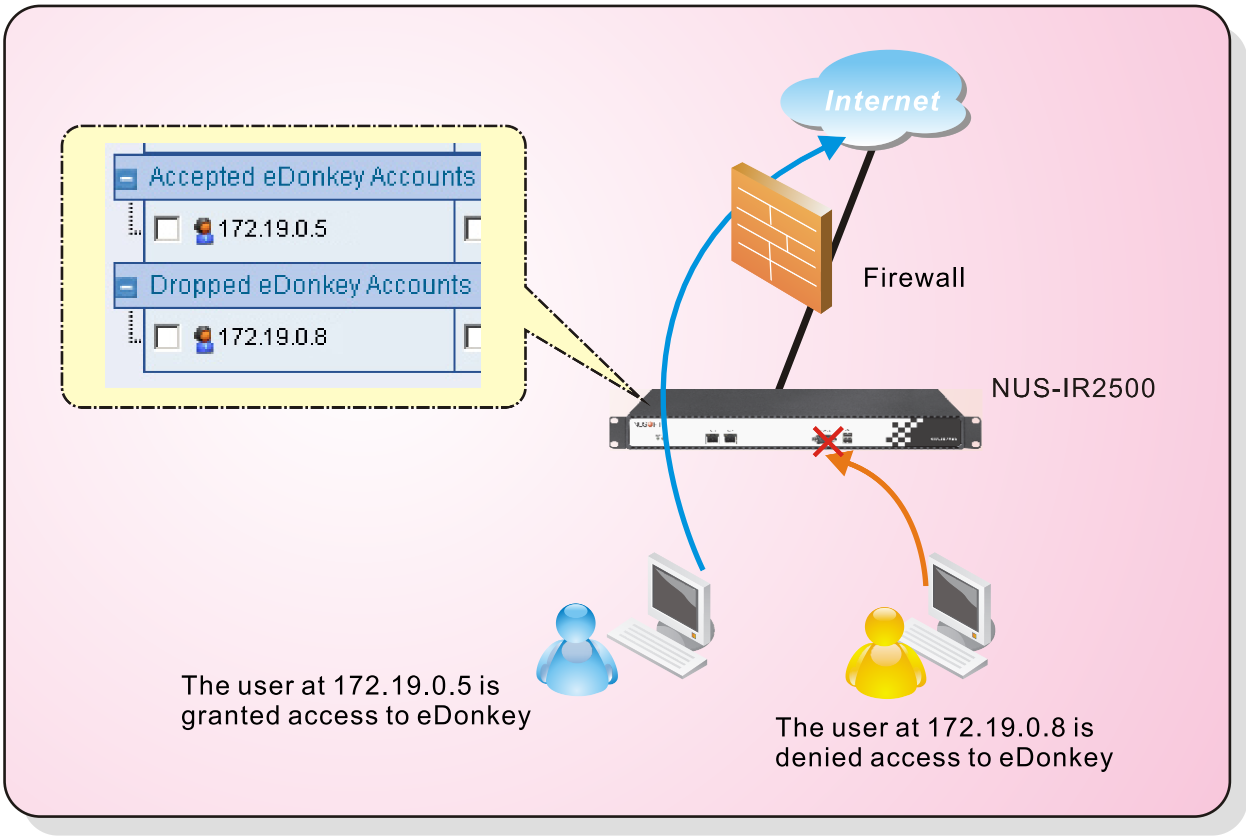
Default eDonkey Accounts (Rule Status) Select all Select none To the accepted To th

□ 100_71	□ 172.19.0.15	□ 172.19.0.16

The user at 172.19.0.15 is
denied access to eDonkey

The user at 172.19.0.16 is
denied access to eDonkey

Moreover, NUS-IR2500 provides you with a more flexible management of P2P software. Settings for individual users can be customized. （Shown in the figure below）



The user at 172.19.0.5 is granted access to eDonkey

The user at 172.19.0.8 is denied access to eDonkey

The following table shows the comparison between the Nusoft Internet Recorder and third-party firewall devices.

	Nusoft Internet Recorder	Third-Party Firewall Devices
Prerequisite	The device should be deployed using Bridge mode.	The settings should be applied to a policy.
Managing Basis	P2P packets	IP addresses
Configuration Procedure	Configure the settings for individual users.	The configuration should be applied to the policy.
P2P User Management	All PCs under enterprise network are subject to the management.	Management becomes ineffective when a user changes the IP address intentionally.

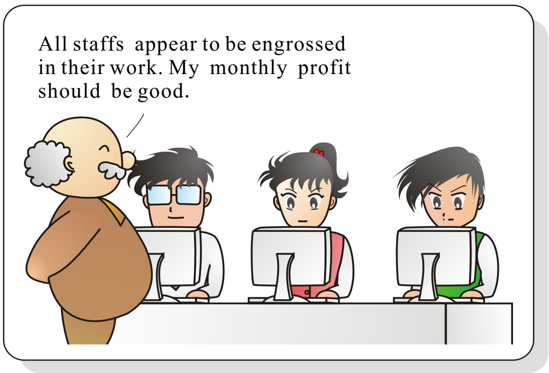
Product News : The Benefits of Nusoft Internet Recorder for Businesses

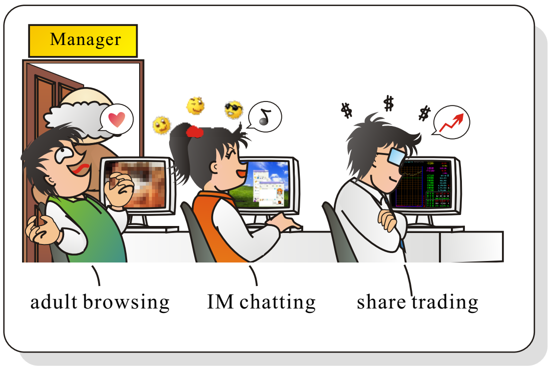
The Internet is firmly established as a necessity for a majority of businesses. New avenues for its integration into businesses are also constantly being paved. Despite the various benefits, the Internet's negative influence on employees' efficiency as they misuse the service for non-ork related Internet activities, is of major concern for managers. The leakage of confidential business information is another. Businesses currently face the dilemma of choosing whether to completely ban or allow all Internet services.

Statistics revealed that during working hours approximately 40% of employees utilize their business's network bandwidth for their own personal use. They may use the Internet to read the news, make online purchases, play games, write emails to friends, etc. The difficulty facing employers is that cyberslacking is difficult to detect due to employees appearing to be using their computers to conduct their normal business duties. If the problem is left unaddressed, employee's working efficiency is dramatically reduced.

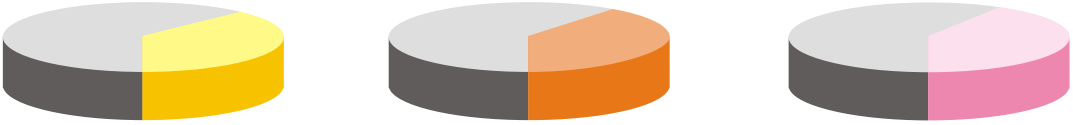
Preventing Employees from Misusing Internet Services through Comprehensive Recording

The Nusoft Internet Recorder is capable of comprehensively recording the eight commonly used Internet services, including HTTP (web pages), email (both web-based and regular), instant messaging (MSN Messenger, Yahoo Messenger, QQ, ICQ), etc. It paints the exact picture behind employees' Internet use, effectively halting employees' non-work related online activities.


All staffs appear to be engrossed in their work. My monthly profit should be good.



Employees' Cyberslacking Activities



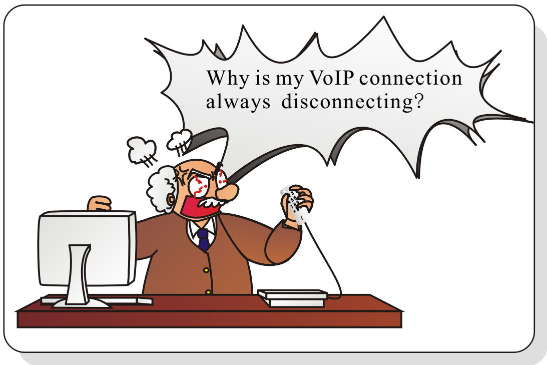
Protecting Important Reordered Data with Remote Backup

The Nusoft Internet Recorder, in addition to saving all the comprehensive recordings on its storage disk, can also utilize a remote backup server (NAS, file server or similar device with NetBIOS support). IT administrators can conveniently access the backup records via the management interface. Due to the importance of retrieving records such as email correspondence, businesses see this as an invaluable tool.

Protecting the Network by Unmasking the Culprits behind Its Misuse

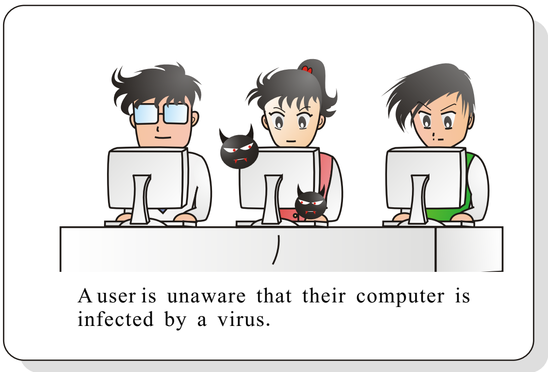
Aside from plain cyberslacking, employees also misuse the businesses' network to download large files such as MP3, movies, etc. placing a major drain on the business' s limited bandwidth.

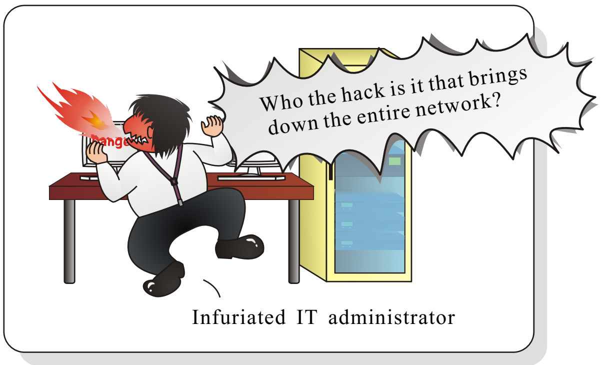
Employees' downloading files and wishing to evade detection commonly change their application' s port number or limit the downloading speed. This approach will be in vain when the Nusoft Internet Recorder is used. Its packet analyzing capabilities distinguishes the service being used, such as P2P software, instant messaging file transfers, etc. The device' s management interface also provides various charts and statistics clearly identifying the business' s exact network utilization and the associated users.



Identifying and Resolving Virus Infections Promptly

Not only can employees' misuse of the Internet degrade the network' s bandwidth, virus-infected internal PCs can cause even greater damage. Once an internal computer exhibits denial-of-service attack characteristics, in order to protect the internal network and prevent it from infecting other PCs, the device' s anomaly flow detection will block the attacking packets. In addition, the infected PC user and the IT administrator will also be alerted. This promptly resolves the issue, allowing the network to remain in operation. There is no longer the need for the IT administrator to inspect all internal PCs individually.


A user is unaware that their computer is infected by a virus.


Who the hack is it that brings down the entire network?
Danger
Infuriated IT administrator