Intelligent Traffic Manager ©

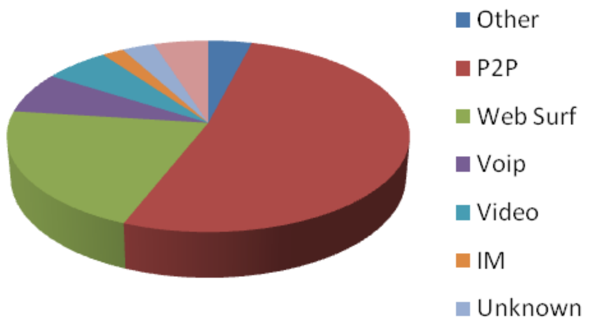
PROTECT YOUR NETWORK AGAINST THE RISK AND THE COST OF UNDESIRABLE INTERNET AND P2P TRAFFIC

Unauthorized or otherwise undesirable Internet traffic can degrade the performance of your network, expose it to the internet security threats, undermine employee productivity, and even leave your organization vulnerable to serious legal liabilities. Our traffic management and filtering solution helps secure your network and maximize its capacity by completely blocking such traffic – without interfering with the legitimate Internet access required to run your business applications.

P2P (peer-to-peer) **Networks**are mainly used to distribute copyright-protected content, what may lead to legal consequences for the Internet service providers, network operators and corporate users. Many file sharing sites offer one-click file hosting services providing so-called DDL (direct download links). Thus, the Internet operators, corporate and educational networks suffer from a small percentage of heavy downloaders consuming a large part of the available bandwidth.

Uncontrolled and unmanaged availability of P2P (eMule, BitTorrent), IP-telephony (VoIP, Skype), IM (ICQ, G-Talk) and Video Streaming applications pose serious security threats and degrade staff efficiency due to the non-work-related nature of these applications. Most of the traditional Internet traffic gateways, intelligent routers and firewalls fail to detect these applications, as they use stealth techniques like protocol obfuscation and data encryption to avoid detection. Such systems often become overloaded by the large number of parallel connections opened by such applications.

Bandwidth-hungry applications such as peer-to-peer file sharing use a very high amount of network recourses. This may dramatically increase communications and infrastructure costs degrading the quality of the critical business applications such as CRM, ERP, corporate video-conferencing, business



Skype Threats:

Hacker-like operation:

- Skype uses stealth techniques to bypass Firewall systems
- Web browser configuration is secretly used in order to use the corporate proxy for tunneling packets to the Internet. The program uses inside-out hacking attack patterns.
- Skype hides its internal modules on the workstations
- Skype can be installed with minimal user privileges
- Skype is the most heavily encrypted and obfuscated application on Earth, which prevents its debugging, reverse engineering and analysis
- Vulnerabilities in Skype and VoIP are a brilliant tool to hide backdoors and Trojans for carrying out different kinds of attacks like intrusions into internal networks and workstations

Connections encrypted by obfuscated secret algorithms:

- It is not possible to inspect Skype traffic
- Files can be secretly transferred in and out of an organization without any authorization
- No virus scanning of the file transfers is possible
- Usage of unapproved encryption algorithms is forbidden by many states – the state legislation may be violated

Obfuscated software – complete black box:

- Blocking Skype is not trivial. Skype company gives no recommendations in this regard.
- Administrators have no possibility to configure the Skype client to adhere to the corporate security policies
- Skype executable and communication protocol are completely encrypted, obfuscated and closed making it impossible to confirm their security or to enforce regulatory mandates

Unverified Identities:

- Every Skype client trusts other Skype clients
- Any user can register with any name even already existent in the system

RRX offers you a sophisticated content filtering and management solution – Intelligent Traffic Manager (ITM) ©

RRX ITM is a hardware based solution that performs traffic monitoring, network access control and Internet protocols analysis. ITM filter functions allow administrators to block any Internet Protocol including Skype, Gizmo, IM, Video streaming, etc, as well as customer-defined protocols.

ITM statistics and logging modules let dedicated administrators collect and

RRX ITM detection mechanism is based on a combination of the layer-7 deep packet inspection and traffic behaviour analysis.

RRX ITM supports all the major protocols including P2P, instant messaging (IM), media streaming, VoIP, tunneling, online gaming analyze statistical data of the network utilization and log or monitor any IP session of a network user.

RRX ITM comes with variety of options and can be easily integrated into a complex network to enforce filtering policies for the local systems as well as the mobile or corporate users.

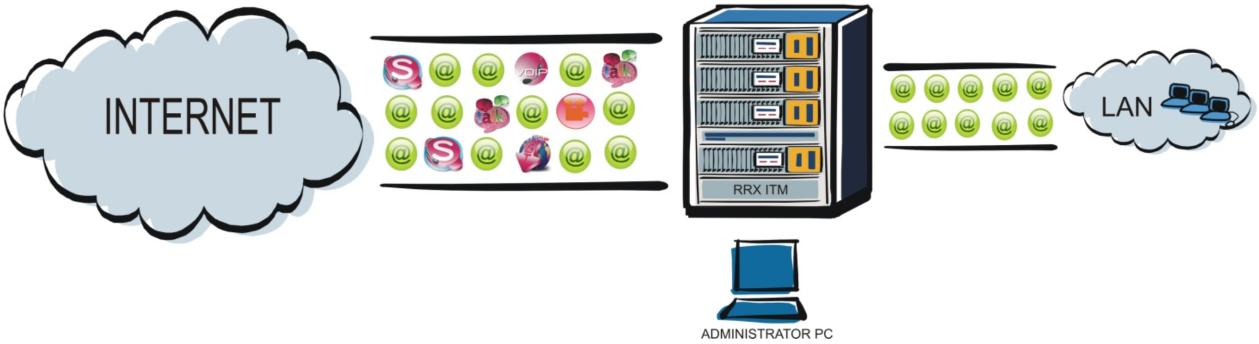
It is a highly scalable solution that can serve the network of a small organization as well as a multinational corporation or a telecom operator.

RRX ITM is a competitive and comprehensive solution that enables operators with monitoring and control of the network traffic per net application or per user.

Custom protocols can also be managed based on the user-defined criteria.

The Integrated QoS management module provides classified traffic prioritization, shaping or blocking functions. Enhanced features provide comprehensive network and user visibility.

RRX ITM solution provides a complete range of network tools to meet every aspect of the internet access control maximizing performance and security of your IT infrastructure.



Key features

- Layer-7 protocol detection with DPI and behavioural analysis
- VoIP, P2P, IM, media streaming, tunnel, Web, e-mail protocol support
- Detects encrypted protocols such as Skype, BitTorrent, eDonkey/eMule, Winny, VPN
- Application and User-Level bandwidth and policy control
- Supports 10 Gigabit and faster links
- Over 600,000 packets per second
- Over 20 millions of concurrent connections
- Over 500,000 new connections per second
- Legal file sharing authorization and illegal file transfer blocking
- Fast integration as a passive or a transparent bridge
- Integrated bypass and hot standby switchover
- Web GUI or CLI for flexible administration
- Signature-based blocking subscription
- Customized modes of operation

Ultimate Performance

RRX ITM is optimized to meet the performance requirements of the most demanding network environments. Performance scales up to fully loaded Gigabit links. Packet queuing yielding latency below 0.1 millisecond on an average loaded link and below 1 millisecond on a highly loaded link.

RRX ITM supports several network links per system and is able to handle asymmetric network traffic.

Statistics, Logging and Accounting

The Administration console provides graphical usage statistics per link, per user group, per application, per application class, per protocol and per adjustable time periods ranging from one hour to one year. A number of

VoIP and Skype

All the major VoIP protocols are supported including SIP, H.323, and Skype (all versions). Accessibility of appropriate VoIP services can be tuned per user, per application or per provider.

Integrated **RRX ITM** QoS functionality allows one to prioritize and guarantee the necessary bandwidth or to degrade quality for these applications if required.

RRX ITM provides a detailed audit of the non-essential bandwidth usage such as Skype or other VoIP activities. All the sessions can be logged and analyzed later.

High Availability

The built-in bypass maintains network connectivity during updates or in case of system failure. Two **RRX ITM** systems can be configured to work in active standby mode. The standby system maintains all the state information and automatically takes over if the primary system fails.

Simple installation and ease of use

RRX ITM operates as a transparent bridge for the seamless integration into the existing network structure. Web console contains a simple configuration panel.

SNMP support gives possibility of ITM integration into the existing traffic control and management systems.

RRX ITM Software an be installed on dedicated hardware as well as integrated into the network routers.

Support

Flexible support options include regular signature updates, e-mail, phone support. 24x7 support with a maximum 3-hour response time.

preconfigured reports help to take control over your network, viewing its utilization from different perspectives. All the statistical data can be automatically delivered to the different aggregation levels for later processing. In addition, all the logging data can be transferred to the external logging system.

Each system can be produced according to the customer-specific requirements. Integration into the existing network and deployment are performed as soon as the customer approves all the necessary design features and configuration.

RRX ITM can immediately improve your network performance, reduce costs and will pay long-term dividends in your dramatically increased network and employee efficiency.

RRX Ltd.
114, Dzerzhinsky str. Stavropol
355000, Russian Federation
tel./fax +7(865)2942002
rrx@rrx.ru , www.rrx.ru