



Russian Railways Communication secured by ViPNet VPN technology since 1999

www.eng.mps.ru

Client profile:

The Russian Ministry of Railroads is the largest ministry in Russia. This ministry manages 17 railroads all over Russia. Each railroad operates as an individual enterprise and has own telecom and information networks as part of an entire ministry's network.

Technical challenges:

The top challenges facing the Ministry of railroads were:

- protection of the member enterprises' LANs against outside unauthorized access;
- delimitation of access to both the ministry private network resources and each individual enterprise's LAN server;
- provision of a secure site-to-site connection between the Ministry's head office and remote enterprises;
- access management and protection of sensitive financial and process-related information communicated over the public and private network environments.

To solve these problems, the Ministry's senior management decided to install an integrated security system capable of adequately protecting the control and commercial information transmitted within the corporate LAN and over wide area public networks. The company made studies into the Russian telecom and safety services market and singled out the **ViPNet** system from the many available offerings. **ViPNet** won out as a solution best meeting the requirements above and considering the value-for-money factor.

The ViPNet Security Solution:

Given the specifics of the Ministry of Railroad business placing a stringent flexibility requirement upon the network configuration, the prospect of changes in the number of workstations and in the access right allocation policy, it was decided to install the **ViPNet [CUSTOM]** software package.

The deployed **ViPNet** environment includes to the present day:

Key Center (currently 25 site licenses, further 17 planned for 2003)

Network Control Center (currently 25 site licenses, further 17 planned for 2003)

Coordinators (currently 250, further 150 planned for 2003)

End-user clients (currently 3000, further 1500 planned for 2003)

VPN access profile:

Transport companies (client-server)

Ticket sales office (client-server-mainframe)

Travel agencies (client-server-mainframe)

Banks (client-server-mainframe, net-to-net (extranet))

Pension fund Russia (net-to-net (extranet))

The "client-server" scheme means that users can connect to a corporate server by ViPNet VPN. The "client-server-mainframe" scheme means that users with ViPNet[Client] software can connect to a corporate mainframe by ViPNet VPN through a ViPNet[Coordinator] server, which provides a secure VPN tunnel between user and server. Internally, each user/client with ViPNet[Client] software installed can securely connect to any other user/client with ViPNet[Client] software installed if it is allowed by the administrator. This is a substantial difference to the great majority of existing VPN solutions, where a VPN client can only connect to a server, not to other clients.

Network profile:

The overall network secured by ViPNet VPN technology consists of the following components:

17 independent networks, one for each railroad

8 sales networks covering all sales and billing activities

17 independent internal communication networks, one for each railroad

Results of the ViPNet Corporate Installation:

- The corporate network is now completely secured, and can be re-configured according to current needs.
- It integrates closed segments, and access can be controlled both at the segment level and for the whole system.
- The use of a combination of symmetric and asymmetric encryption algorithms ensures a high reliability of information encoding.
- A preinstalled digitally-signed e-mail appliance allows secure transmission and archiving of financial reports, commercial and process-related data. Being encoded using the encryption algorithms, such information is unreadable to third parties, even if intercepted.
- The network is protected against attacks from the Internet and has intrusion detection/logging/tracing capabilities.
- Also, it enables transparent secure connections with enterprise remote offices and mobile users, file encryption and delivery control based on digital signatures, and holding of audio- and video-conferences.
- The pilot network connecting ticket offices and travel agencies to the mainframe has been successfully deployed. The ticket machine is a PC with either Linux OS or Windows . These PCs have specially programmed applications for billing and ticket reservations OS. All transactions between the client and the mainframe are protected by ViPNet.
- The top managers of the railroads communicate through their internal communication network GSM communications secured by ViPNet technology while traveling over enormous distances in Russia.

General remarks on the ViPNet VPN software solution deployed:

All corporate database clusters and information servers are protected by ViPNet in such a way that any client trying to connect, can do this only if he has

- a) ViPNet client software installed
- b) corresponding connection links
- c) a key set.

If they are connecting from a network, ViPNet gateway software has to be installed.

Further cost savings factors:

The ViPNet [Business mail] features not only a digitally signed off-line information exchange, but, in addition, it provides also file autoprocessing to automate mail exchange. The ViPNet [Business mail] is an isolated mail system isolated from the public e-mail area and operates over existing ViPNet servers. These servers do not require an installation of an e-mail system like MS Exchange (~\$100 per client, total for 3000 users would be about \$300.000) and others. The isolation of the ViPNet[Business Mail] environment is not only a savings factor for larger corporate customers, but also excludes all external and internal SPAM issues for the entire corporation . No antiSPAM software (~\$5 per client-month subscription; total for 3000 users would be about \$15000 per month) is necessary.