



SOUTHERN
TELECOMMUNICATIONS
COMPANY

www.stcompany.ru

Introduction

STC AG is the largest telecommunication company in the southern republic of Russia. The following products are in the STC portfolio:

- fixed telephone networks for local and long-distance calls including international calls,
- data exchange,
- paging,
- channel leasing,
- telemetric services: access to Internet and other communication services.

In total an area of over 500 000 square kilometers is covered with a population of 18.6 millions with a capacity more than 3.2 million telephone lines. With a turnover exceeding 350 million USD STC is the market leader among the seven regional telecommunication companies in Russia.

The decision in favour of ViPNet-technology was based on the following criteria.

- ViPNet offers a flexible protection mechanism for workstations and servers within a LAN as well as for mobile users and protected Websites.
- The Firewall integrated in the ViPNet [Client] filters data traffic and blocks attacks not only when communicating with external lines, but also in the case of “trusted connections” with other ViPNet users.
- In addition to a key system with public key algorithms also symmetric (preshared) keys are used which prevent internal attacks during authentication as well as attacks like ‘man in the middle’, ‘session hijacking’ and so forth. The process of key exchange is fully automatic, saving costs for more complicated systems and eliminating the need for repeated purchase of certificates.

STC Telecommunication: Case Study

- ViPNet incorporates an internal virtual IP-address system, which enables high flexibility and scaling without changes in already existing network structures with all IP-addresses and network applications.
- Excellent compatibility available for all common types of communications (xDSL, ISDN, WiFi, GPRS etc.) This opens users of all kind the possibility of conveniently working with ERP and CRM systems.

The **ViPNet [Coordinator]** fulfills with STC the following functions:

- IP-address Server to provide real-time information about the status of the VPN objects and their current IP addresses;
 - Key Center generates and subsequently updates initial keys and passwords for network objects and users;
 - Proxy Server to handle 'secure connections', e.g. to enable the operation of secured computers within the VPN on behalf of a single workstation;
 - Tunneling Server to tunnel (encrypt) the traffic going between unsecured computers / servers on the LAN to the rest of the VPN (including mobile and remote users) over public communication channels. In the case of mobile and remote VPN users the Tunneling Server acts as a server providing access to LAN resources;
 - Firewall to filter the traffic by specified parameters in accordance with prescribed privacy policy.
 - "Open Internet" Server to filter and tunnel (isolate) untrusted traffic coming to a secured LAN computer from the external network, and virtually isolate this computer during its external communication session from other VPN objects;
- Secure Mail Server to support routing of secured mail packages and control messages.

The **ViPNet [Client]** has been installed in the Server and all workstations of STC and meets the following functions:

- VPN-Client based on Client-Server technology (access to secured network and VPN services;
- Personal Firewall filters the traffic by specified parameters ('white' and 'black' lists of parties seeking connection, ports, protocols, server/application types);
- TCP/IP Traffic Encryption Device: encrypting an decrypting traffic between protected network nodes;
- ViPNet MailClient: supports the digital signature functions and the automated processing of e-documents in accordance with prescribed rules and procedures;
- Automated document processing.

Scope of STC ViPNet installation

10 Coordinators
500 + VPN users
1500 + connected workstations via VPN Tunnel

STC Telecommunication: Case Study

