



INTERPOL Russia uses ViPNet-VPN technology since 1999. The Russian INTERPOL office is closely cooperating with the Ministry of Interior of the Russian Federation.

Daily work requires mutual access to the data banks of both organizations. INTERPOL Russia has to permit the Ministry of Interior access to its data bank, but at the same time has the problem of safeguarding such access from non-authorized users from within their own structures.

Because of the high probability of an abuse of access to the internal networks due to corruption and the influence of organized criminality it has become necessary to protect not only the INTERPOL servers but also the INTERPOL terminals of all users as well.

On the basis of an internal threat analysis and security audits ViPNet was the solution selected meeting the prescribed criteria, especially the protection against INTERNAL data abuse.

- ViPNet [Client] Software offers, in a flexible way, the possibility of establishing coded communication between mobile users, stationary workstations and servers and, simultaneously, to deny internal abuse and unauthorized access by means of a multiple system of authentication and verification.
- The integrated firewall of the ViPNet [Client] software filters and blocks not only data traffic between a VPN client and an external network subject, but also in the case of a trusted connection the traffic between from VPN client to VPN client.
- In addition to the key system with public keys ViPNet uses a key and authentication system based on symmetric (preshared) codes by which an interference in the authentication process by unauthorized individuals is prevented. By these means attacks of the type “Man in the middle”, session hijacking and others will be thwarted. The system of symmetric (preshared) keys is automatic; it results in saving additional costs for complicated key systems, authentications and certificates.

INTERPOL Russia is regularly provided with updates and makes use especially of additionally secured sensible data for selected terminals by means of the virtual encrypted hard disk ViPNet [Safe Disk]. Sensibility of data inherent in this case study prevent us from disclosing further technical details.