

## Rosneft Caso de Sucesso



**ROSNEFT**  
OPEN JOINT STOCK COMPANY  
OIL COMPANY

A **Rosneft** é uma Companhia Russa de Petróleo que possui grandes operações abrangendo territórios muito distantes, e assim, uma gama extensiva de interesses estratégicos.

A informação é altamente estratégica, pois a empresa atua tanto nas regiões ricas em hidrocarboneto, óleo e gás do país. Estão na Sibéria Ocidental e Oriental, na Ilha de Sakhalin e na Província de Timano-Pechorsky, no Sul do país, bem como também no exterior.

A implementação dos projetos estratégicos permitirá à companhia aumentar sua produção de óleo de 3.5 a 4 vezes e sua produção de gás 7 vezes até 2015.

A Empresa de avaliação Degolier and McNoton Company, avaliou os recursos a partir de um de janeiro de 2005 que totalizaram:

- Óleo e gás liquefeito 327.7 milhões de toneladas mínimas, 358.2 milhões prováveis e 465.9 milhões de toneladas possíveis.
- Quanto ao gás, há 77.7 bilhões metros cúbicos mínimos, 1.226,6 bilhões metros cúbicos prováveis e 598.3 bilhões metros cúbicos possíveis .
- Ao término de 2004 a Companhia possuía 268 licenças com o direito para usar recursos minerais subterrâneos, que incluem 217 licenças para extração de hidrocarboneto, 25 licenças combinadas para pesquisa, prospecção e exploração, e 26 licenças de exploração geológica.

### Desafios técnicos:

Os desafios técnicos solicitados por Rosneft foram:

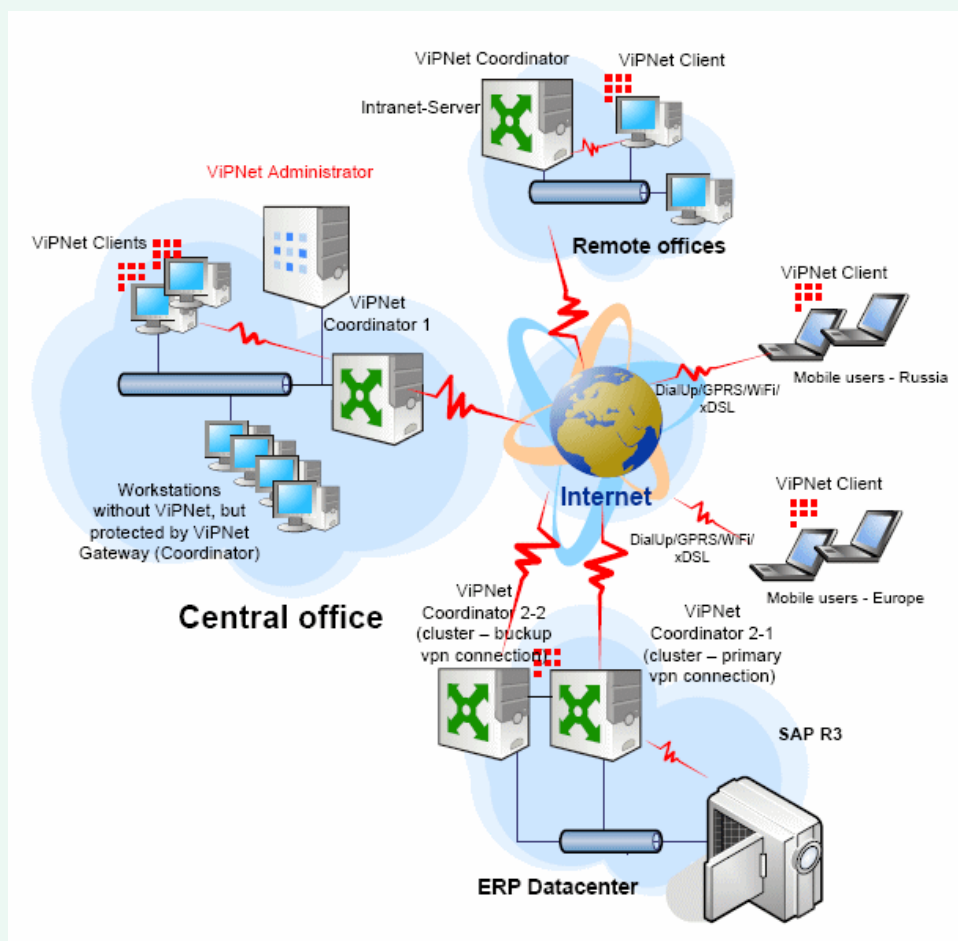
- A. Proteção do sistema de ERP (baseado em SAP R3) para acesso externo não autorizado.
- B. Proteção das LAN contra intrusos internos e externos.
- C. Proteção de toda a informação, não só confidencial que trafega na Intranet ou Internet (redes públicas).
- D. A proteção deveria ser aplicada rapidamente com o mínimo de alterações tanto no sistema ERP como em toda a infra-estrutura de gestão de redes de companhia.
- E. O acesso remoto deveria ter o mesmo nível de segurança da LAN.
- F. O sistema de segurança tem que ter interoperabilidade com os sistemas dos parceiros.

### Decisões:

Para cobrir estes problemas, a alta administração da Companhia decidiu iniciar um Sistema integrado de segurança, capaz de proteger adequadamente o controle e a informações comerciais transmitidas dentro da LAN e na Internet. A empresa fez avaliações no sistema de telecomunicações russo e no mercado de serviços de segurança e elegeu o ViPNet entre todas as propostas recebidas. ViPNet apresentou a solução que atendeu melhor as exigências requeridas e apresentou o menor custo benefício.

## Solução:

Pelas particularidades do negócio com uma exigência de flexibilidade na rede, mudança no número de estações de trabalho e na política de acesso seguro, foi decidido instalar o ViPNet CUSTOM.



## O ambiente de ViPNet inclui:

- Key Center;
- Network Control Center;
- Coordenators (portais) (atualmente 50 e 150 planejados para 2007);
- Clientes (atualmente 500 e 1500 planejados para 2007).

### Perfil de acesso VPN:

- Pessoal de escritório interno;
- Trabalhadores móveis inclusive alta administração, com acesso do mundo inteiro;
- Acionistas, Parceiros e Subcontratados;
- Extranet com parceiro Logístico Russian Railroads;
- Extranet com parceiros financeiros Bancos.

Todos os usuários incorporados podem se conectar ao sistema de ERP por ViPNet-VPN através da integração "cliente-servidor-mainframe". A integração "cliente-servidor-mainframe", significa que os usuários com ViPNet podem se conectar através de um Coordenador server que providencia um tunel seguro entre o usuário e o server. Internamente cada cliente usuário com ViPNet Client é autorizado pelo administrador. Nesta situação ViPNet mantém segurança total pois permite somente a conexão do Cliente ao Server e não a outros clientes.

### Resultados atingidos:

- A rede da corporação esta completamente segura e pode ser reconfigurada de acordo com necessidades atuais.
- A rede da corporação e as informações estão protegidas de ataques via Internet e tem imediata identificação de intrusão: detection/logging/tracking capabilities.
- ViPNet habilita comunicação segura transparente com filiais remotas, usuários móveis, arquivos seguros e e-mail encriptados, bem como controle de entrega baseado em assinaturas digitais e possibilidade de áudio e vídeo conferências encriptadas.
- O mainframe com SAP ERP é protegido por dual-ViPNet Coordenador, com um sistema à prova de falhas. Este é um sistema tolerante a falhas, com um risco muito baixo de perder uma conexão com banco de dados.
- A alta administração se comunica pela rede interna GSM/3G assegurada pela tecnologia de ViPNet quando em viagens internacionais, inclusive no outro lado do mundo.
- A Rosneft entregou uma ViPNet segura com o principal parceiro Russian Railroads abrangendo diversos níveis, incluindo a alta administração.
- A infra-estrutura de TI não mudou com a instalação do ViPNet e opera normalmente.