

# VPN - Virtual Private Network

## (Rede Privada Virtual)

GPr Sistemas/ASP Systems - Agosto/2000  
Marco Antonio G. Rossi  
Oswaldo Franzin

### Introdução

O conceito de VPN surgiu da necessidade de se utilizar redes de comunicação não confiáveis para trafegar informações de forma segura. As redes públicas são consideradas não confiáveis, tendo em vista que os dados que nelas trafegam estão sujeitos a interceptação e captura. Em contrapartida, estas tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.

Com o explosivo crescimento da Internet, o constante aumento de sua área de abrangência, e a expectativa de uma rápida melhoria na qualidade dos meios de comunicação associado a um grande aumento nas velocidades de acesso e backbone, esta passou a ser vista como um meio conveniente para as comunicações corporativas. No entanto, a passagem de dados sensíveis pela Internet somente se torna possível com o uso de alguma tecnologia que torne esse meio altamente inseguro em um meio confiável. Com essa abordagem, o uso de VPN sobre a Internet parece ser uma alternativa viável e adequada. No entanto, veremos que não é apenas em acessos públicos que a tecnologia de VPN pode e deve ser empregada.

Aplicativos desenvolvidos para operar com o suporte de uma rede privativa não utilizam recursos para garantir a privacidade em uma rede pública. A migração de tais aplicações é sempre possível, no entanto, certamente incorreria em atividades dispendiosas e exigiriam muito tempo de desenvolvimento e testes. A implantação de VPN pressupõe que não haja necessidade de modificações nos sistemas utilizados pelas corporações, sendo que todas as necessidades de privacidade que passam a ser exigidas sejam supridas pelos recursos adicionais que sejam disponibilizados nos sistemas de comunicação.

## **Funções Básicas**

A utilização de redes públicas tende a apresentar custos muito menores que os obtidos com a implantação de redes privadas, sendo este, justamente o grande estímulo para o uso de VPNs. No entanto, para que esta abordagem se torne efetiva, a VPN deve prover um conjunto de funções que garanta *Confidencialidade, Integridade e Autenticidade*.

### **Confidencialidade**

Tendo em vista que estarão sendo utilizados meios públicos de comunicação, a tarefa de interceptar uma seqüência de dados é relativamente simples. É imprescindível que os dados que trafeguem sejam absolutamente privados, de forma que, mesmo que sejam capturados, não possam ser entendidos.

### **Integridade**

Na eventualidade dos dados serem capturados, é necessário garantir que estes não sejam adulterados e re-encaminhados, de tal forma que quaisquer tentativas nesse sentido não tenham sucesso, permitindo que somente dados válidos sejam recebidos pelas aplicações suportadas pela VPN.

### **Autenticidade**

Somente usuários e equipamentos que tenham sido autorizados a fazer parte de uma determinada VPN é que podem trocar dados entre si; ou seja, um elemento de uma VPN somente reconhecerá dados originados em por um segundo elemento que seguramente tenha autorização para fazer parte da VPN.

Dependendo da técnica utilizada na implementação da VPN, a privacidade das informações poderá ser garantida apenas para os dados, ou para todo o pacote (cabeçalho e dados). Quatro técnicas podem ser usadas para a implementação de soluções VPN:

### **Modo Transmissão**

Somente os dados são criptografados, não havendo mudança no tamanho dos pacotes. Geralmente são soluções proprietárias, desenvolvidas por fabricantes.

### **Modo Transporte**

Somente os dados são criptografados, podendo haver mudança no tamanho dos pacotes. É uma solução de segurança adequada, para

implementações onde os dados trafegam somente entre dois nós da comunicação.

### **Modo Túnel Criptografado**

Tanto os dados quanto o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e de destino.

### **Modo Túnel Não Criptografado**

Tanto os dados quanto o cabeçalho são empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino. No entanto, cabeçalho e dados são mantidos tal como gerados na origem, não garantindo a privacidade.

Para disponibilizar as funcionalidades descritas anteriormente, a implementação de VPN lança mão dos conceitos e recursos de *criptografia*, *autenticação* e *controle de acesso*.

## **Criptografia**

A criptografia é implementada por um conjunto de métodos de tratamento e transformação dos dados que serão transmitidos pela rede pública. Um conjunto de regras é aplicado sobre os dados, empregando uma seqüência de bits (*chave*) como padrão a ser utilizado na criptografia. Partindo dos dados que serão transmitidos, o objetivo é criar uma seqüência de dados que não possa ser entendida por terceiros, que não façam parte da VPN, sendo que apenas o verdadeiro destinatário dos dados deve ser capaz de recuperar os dados originais fazendo uso de uma *chave*.

São chamadas de *Chave Simétrica* e de *Chave Assimétrica* as tecnologias utilizadas para criptografar dados.

### *Chave Simétrica ou Chave Privada*

É a técnica de criptografia onde é utilizada a mesma *chave* para criptografar e decriptografar os dados. Sendo assim, a manutenção da *chave* em segredo é fundamental para a eficiência do processo.

### *Chave Assimétrica ou Chave Pública*

É a técnica de criptografia onde as *chaves* utilizadas para criptografar e decriptografar são diferentes, sendo, no entanto relacionadas. A *chave* utilizada para criptografar os dados é formada por duas partes, sendo uma pública e outra privada, da mesma forma que a *chave* utilizada para decriptografar.

## **Algoritmos para Criptografia**

### *DES - Data Encryption Standard*

É um padrão de criptografia simétrica, adotada pelo governo dos EUA em 1977.

### *Triple-DES*

O *Triple-DES* é uma variação do algoritmo *DES*, sendo que o processo tem três fases: A seqüência é criptografada, sendo em seguida descriptografada com uma *chave* errada, e é novamente criptografada.

### *RSA - Rivest Shamir Adleman*

É um padrão criado por Ron Rivest, Adi Shamir e Leonard Adleman em 1977 e utiliza chave pública de criptografia, tirando vantagem do fato de ser extremamente difícil fatorar o produto de números primos muito grandes.

### *Diffie-Hellman*

Foi desenvolvido por Diffie e Hellman em 1976. Este algoritmo permite a troca de *chaves* secretas entre dois usuários. A *chave* utilizada é formada pelo processamento de duas outras *chaves* uma pública e outra secreta.

## **Integridade**

A garantia de integridade dos dados trocados em uma VPN pode ser fornecida pelo uso de algoritmos que geram, a partir dos dados originais, códigos binários que sejam praticamente impossíveis de serem conseguidos, caso estes dados sofram qualquer tipo de adulteração. Ao chegarem no destinatário, este executa o mesmo algoritmo e compara o resultado obtido com a seqüência de bits que acompanha a mensagem, fazendo assim a verificação.

## **Algoritmos para Integridade**

### *SHA-1 - Secure Hash Algorithm One*

É um algoritmo de hash que gera mensagens de 160 bits, a partir de uma seqüência de até  $2^{64}$  bits.

### *MD5 - Message Digest Algorithm 5*

É um algoritmo de hash que gera mensagens de 128 bits, a partir de uma seqüência de qualquer tamanho.

## Autenticação

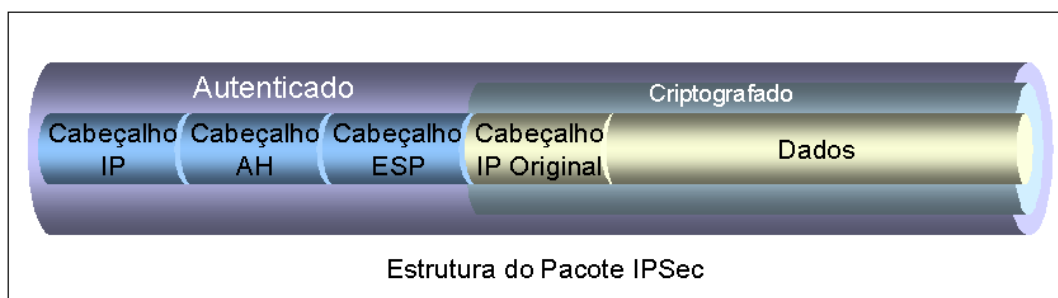
A Autenticação é importante para garantir que o originador dos dados que trafeguem na VPN seja, realmente, quem diz ser. Um usuário deve ser identificado no seu ponto de acesso à VPN, de forma que, somente o tráfego de usuários autenticados transite pela rede. Tal ponto de acesso fica responsável por rejeitar as conexões que não sejam adequadamente identificadas. Para realizar o processo de autenticação, podem ser utilizados sistemas de identificação/senha, senhas geradas dinamicamente, autenticação por RADIUS (Remote Authentication Dial-In User Service) ou um código duplo.

A definição exata do grau de liberdade que cada usuário tem dentro do sistema, tendo como consequência o controle dos acessos permitidos, é mais uma necessidade que justifica a importância da autenticação, pois é a partir da garantia da identificação precisa do usuário que poderá ser selecionado o perfil de acesso permitido para ele.

## Protocolos para VPN

### IPSec

IPSec é um conjunto de padrões e protocolos para segurança relacionada com VPN sobre uma rede IP, e foi definido pelo grupo de trabalho denominado IP Security (IPSec) do IETF (Internet Engineering Task Force). O IPSec especifica os cabeçalhos AH (Authentication Header) e ESP (Encapsulated Security Payload), que podem ser utilizados independentemente ou em conjunto, de forma que um pacote IPSec poderá apresentar somente um dos cabeçalhos (AH ou ESP) ou os dois cabeçalhos.



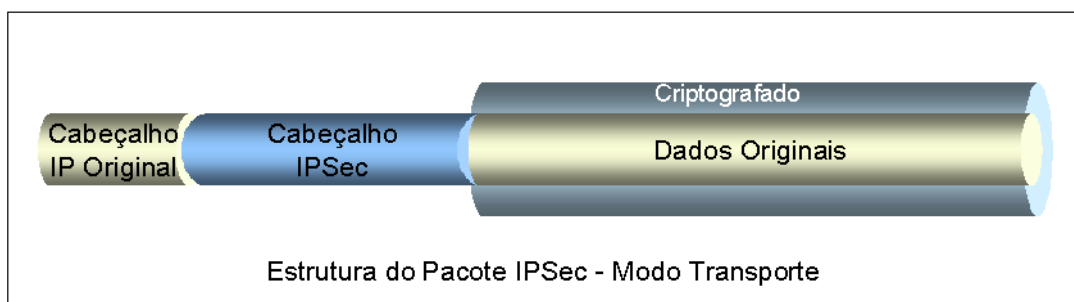
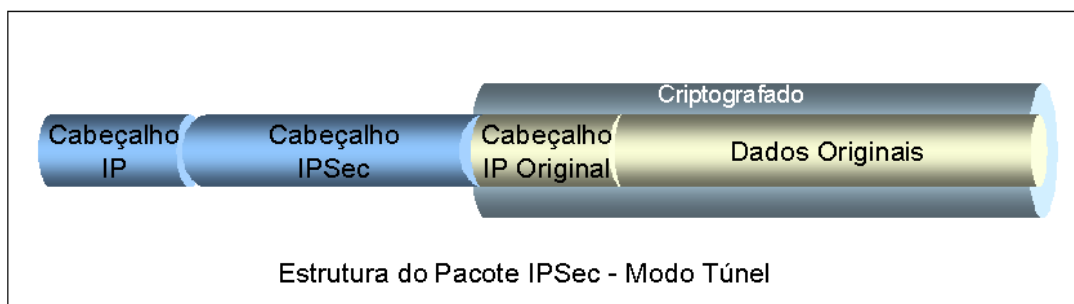
### Authentication Header (AH)

Utilizado para prover integridade e autenticidade dos dados presentes no pacote, incluindo a parte invariante do cabeçalho, no entanto, não provê confidencialidade.

### *Encapsulated Security Payload (ESP)*

Provê integridade, autenticidade e criptografia à área de dados do pacote.

A implementação do IPSec pode ser feita tanto em *Modo Transporte* como em *Modo Túnel*.



### ***PPTP - Point to Point Tunneling Protocol***

O PPTP é uma variação do protocolo PPP, que encapsula os pacotes em um túnel IP fim a fim.

### ***L2TP - Level 2 Tunneling Protocol***

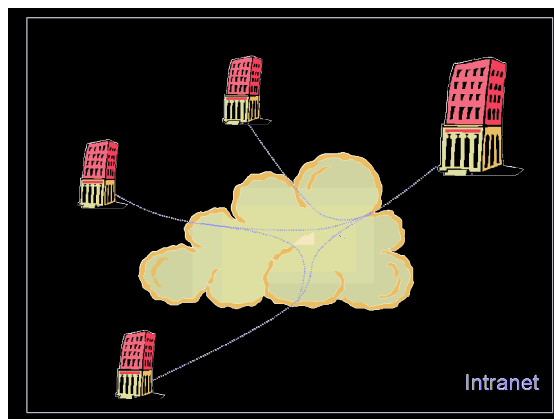
É um protocolo que faz o tunelamento de PPP utilizando vários protocolos de rede (ex: IP, ATM, etc) sendo utilizado para prover acesso discado a múltiplos protocolos.

### ***SOCKS v5***

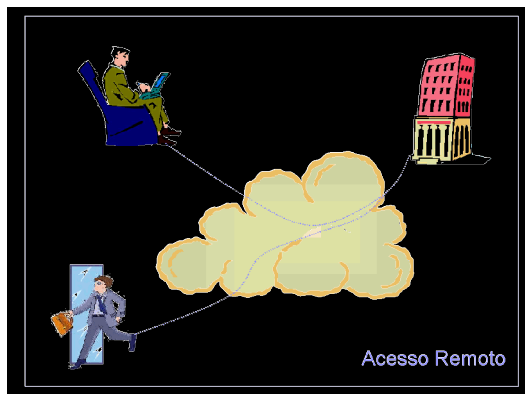
É um protocolo especificado pelo IETF e define como uma aplicação cliente - servidor usando IP e UDP estabelece comunicação através de um servidor proxy.

## VPN para Intranet

Uma Intranet é utilizada para conectar sites que geralmente possuem uma infraestrutura completa de rede local, podendo, ou não, ter seus próprios servidores e aplicativos locais. Tais sites têm em comum a necessidade de compartilhar recursos que estejam distribuídos, como bases de dados e aplicativos, ou mesmo de troca de informações, como no caso de e-mail. A Intranet pode ser entendida como um conjunto de redes locais de uma corporação, geograficamente distribuídas e interconectadas através de uma rede pública de comunicação. Esse tipo de conexão também pode ser chamado de *LAN-to-LAN* ou *Site-to-Site*.



## VPN para Acesso Remoto

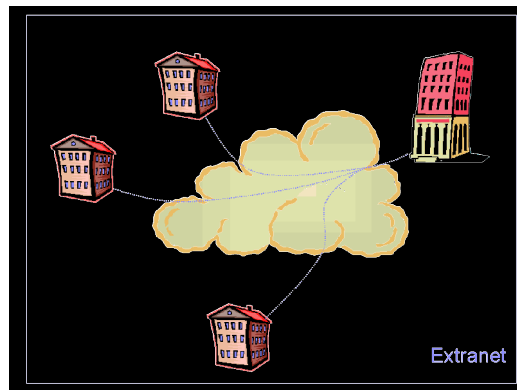


É chamado de acesso remoto aquele realizado por usuários móveis que se utilizam de um computador para conexão com a rede corporativa, partindo de suas residências ou hotéis. Esse tipo de conexão, que também é denominado *Point-to-Site*, está se tornando cada vez mais utilizada. Aplicações típicas do acesso remoto são:

- Acesso de vendedores para encaminhamento de pedidos, verificação de processos ou estoques;
- Acesso de gerentes e diretores em viagens, mantendo atualizadas suas comunicações com sua base de operação, tanto para pesquisas na rede corporativa como acompanhamento de seu correio eletrônico;
- Equipe técnica em campo, para acesso a sistemas de suporte e documentação, bem como a atualização do estado dos atendimentos.

## VPN para Extranet

Em uma Extranet, tem-se a disponibilidade para o acesso de parceiros, representantes, clientes e fornecedores ao ambiente da rede corporativa. Esta comunicação é permitida com o objetivo de agilizar o processo de troca de informações entre as partes, estreitando o relacionamento, e tornando mais dinâmica e efetiva a interação. Esse tipo de conexão também pode ser chamado de *LAN-to-LAN* ou *Site-to-Site*.



## Nível de Segurança

A especificação da VPN a ser implantada deve tomar por base o grau de segurança que se necessita, ou seja, avaliando o tipo de dado que deverá trafegar pela rede e se são dados sensíveis ou não. Dessa definição depende a escolha do protocolo de comunicação, dos algoritmos de criptografia e de Integridade, assim como as políticas e técnicas a serem adotadas para o controle de acesso. Tendo em vista que todos esses fatores terão um impacto direto sobre a complexidade e requisitos dos sistemas que serão utilizados, quanto mais seguro for o sistema, mais sofisticados e com capacidades de processamento terão de ser os equipamentos, principalmente, no que se refere a complexidade e requisitos exigidos pelos algoritmos de criptografia e integridade.