VPN – Virtual Private Network

Luiz Arthur

A VPN (Virtual Private Network ou simplesmente Rede Privada Virtual) cria "**túneis virtuais**" de comunicação entre redes ou hosts, fazendo com que os dados trafeguem de forma segura usando métodos criptográficos que visam aumentar a segurança na transferência de dados.

No âmbito das redes de computadores, **uma rede considerada privada é formada de dois ou mais computadores** interligados via hubs ou switches, formando uma rede local (**LAN**) de dados ou informações entre os equipamentos. Normalmente este tipo de rede troca inúmeras informações tal como arquivos, programas, serviços, impressoras, etc.

Já uma **rede** dita **pública** é normalmente uma **rede de grande porte**, geralmente formada por **MANs** e **WANs**, tais redes devido a este grande porte não podem ser sustentadas por uma única empresa por exemplo, assim redes como a Internet é um ambiente formado por inúmeras empresas (telecomunicações, informática, governos, etc) formando uma rede dita pública (**não tem** um único **dono**).

Com o mundo atual globalizado as **empresas estão em expansão**, ou seja, uma empresas que tem **sede** em uma cidade rapidamente pode necessitar de uma **filial em outro bairro** desta mesma cidade. Porém, essa empresa vai necessitar trocar informações entre si, unindo a rede local da empresa sede com a nova filial, ampliando desta forma sua rede privada.

Para fazer a **ampliação da rede local** desta empresa será necessário por exemplo contratar alguma empresa que forneça infraestrutura de rede entre os bairros para **ligar a sede e a filial**, por exemplo, uma rede sem fio (WiFi).

Bem agora imagine que a empresa continuá crescendo e precise abrir **filiais em outras cidades**, estados ou ainda países. É fato que a solução utilizando redes sem fio (WiFi) não vai poder ser mantida para um ambiente grande como este, a empresa certamente precisaria contratar links de dados tal como, **Fame Relay**, **ATM**, etc, para continuar com seu ambiente corporativo interligado via rede.

Então, ao invés de **manter** uma **rede privada** tal como uma **LAN**, a empresa terá uma **rede** ainda **privada** só que como uma **MAN** ou **WAN** e o custo para manter uma rede empresarial deste porte vai se tornar rapidamente muito dispendioso (caro).

Uma **solução** para o cenário descrito anteriormente é ligar as filiais e sede através de uma rede pública, tal como a **Internet**, já que o custo de um link ADSL, por exemplo, é insignificante para uma empresa. Desta forma, podemos ligar a empresa através da Internet, **mas surge um outro problema** agora trafegamos todos os dados da empresa não mas por um ambiente privado mas sim por um ambiente público, no qual as **informações da empresa podem ser capturadas por pessoas não autorizadas**, comprometendo a confidencialidade dos dados.

É justamente neste cenário que surge a tecnologia de Redes Privadas Virtuais – VPN.

Outra questão importante: suponha que a empresa tenha **vendedores que viajam a trabalho para fechar negócios**, que precisam se conectar à rede da empresa no decorrer de uma reunião ou no hotel, para compartilhar o andamento de um negócio.

Esses vendedores, poderiam por exemplo, fazer uma **conexão discada para dentro de um serviço de discagem na empresa** e pagar o custo da ligação interurbana, o que seria também caro para empresa pois normalmente exige discagens interurbanas. Neste caso manter um link ATM, Frame Relay, etc, torna-se impossível devido a mobilidade do usuário, mais uma vez a melhor **solução é a Internet**, o que exige a passagem de dados em uma rede pública e a solução é a **VPN**.

Outro problema tratado por VPNs é que a Internet trabalha com os protocolos TCP/IP, mas **algumas redes privadas não trabalham com TCP/IP**, através de algumas técnicas de VPN, como **encapsulamento**, é possível ligar redes que não usam protocolos TCP/IP na Internet.

Então com os problemas das redes privadas e das redes públicas, surgio um paradigma novo:

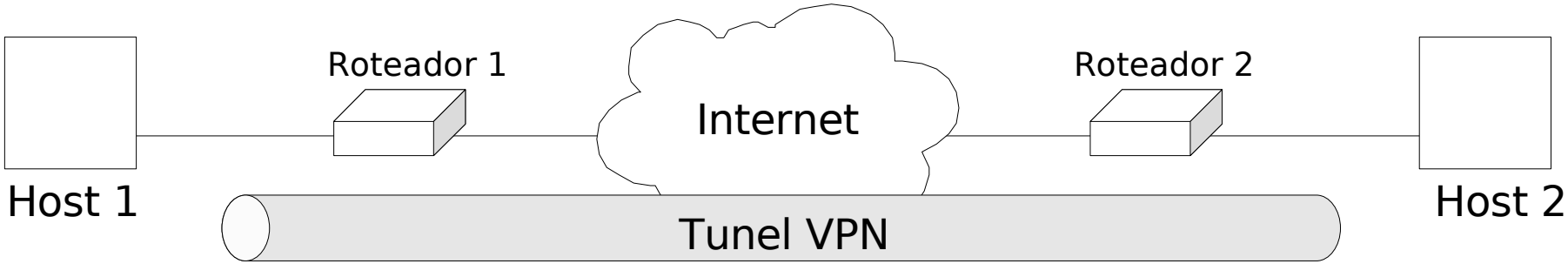
"Usar a rede pública como se fosse uma rede privada com segurança, criando-se, assim, a Virtual Private Network ou Rede Privada Virtual".

VPN – Virtual Private Network

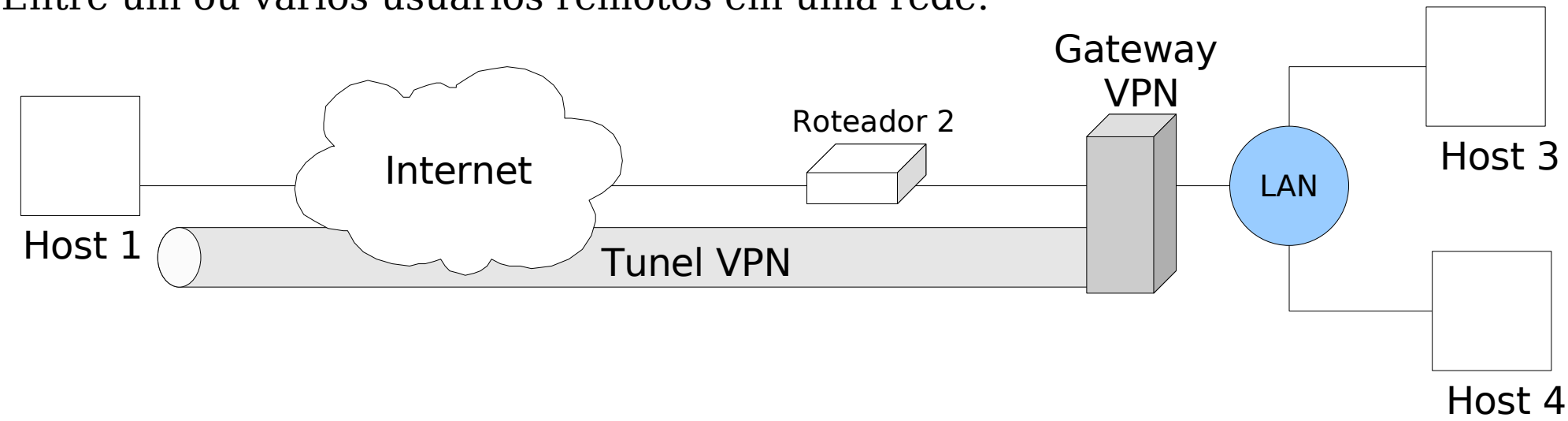
Luiz Arthur

O termo Virtual entra, porque depende de uma **conexão virtual, temporária, sem presença física no meio**. Essa conexão virtual consiste em troca de pacotes, sendo roteados entre vários equipamentos. Tais conexões podem ser feitas das seguintes formas:

- Entre duas máquinas, servidor ou estações, interligadas via Internet:

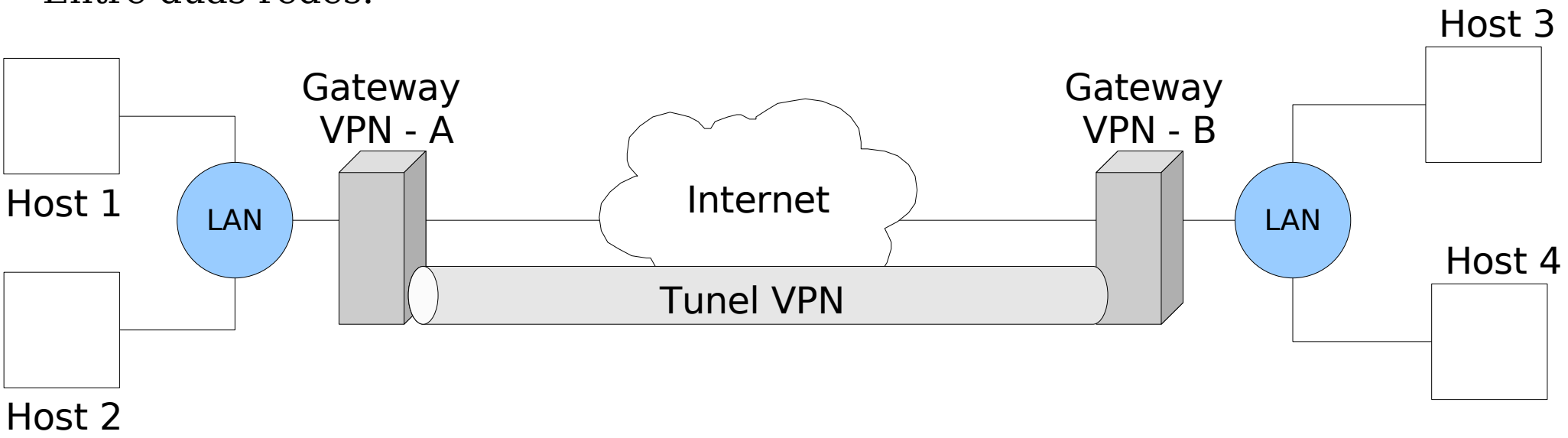


- Entre um ou vários usuários remotos em uma rede:



No procedimento entre vários usários remotos usando a rede, o usuário deve estabelecer conexão com a Internet (via discada, ADSL, etc). E depois por meio deste canal estabelecer uma VPN entre o usuário remoto e o gateway da VPN. Este procedimento normalmente **não é transparente** ao usuário, porque é necessária uma fase de estabelecimento da conexão.

- Entre duas redes:



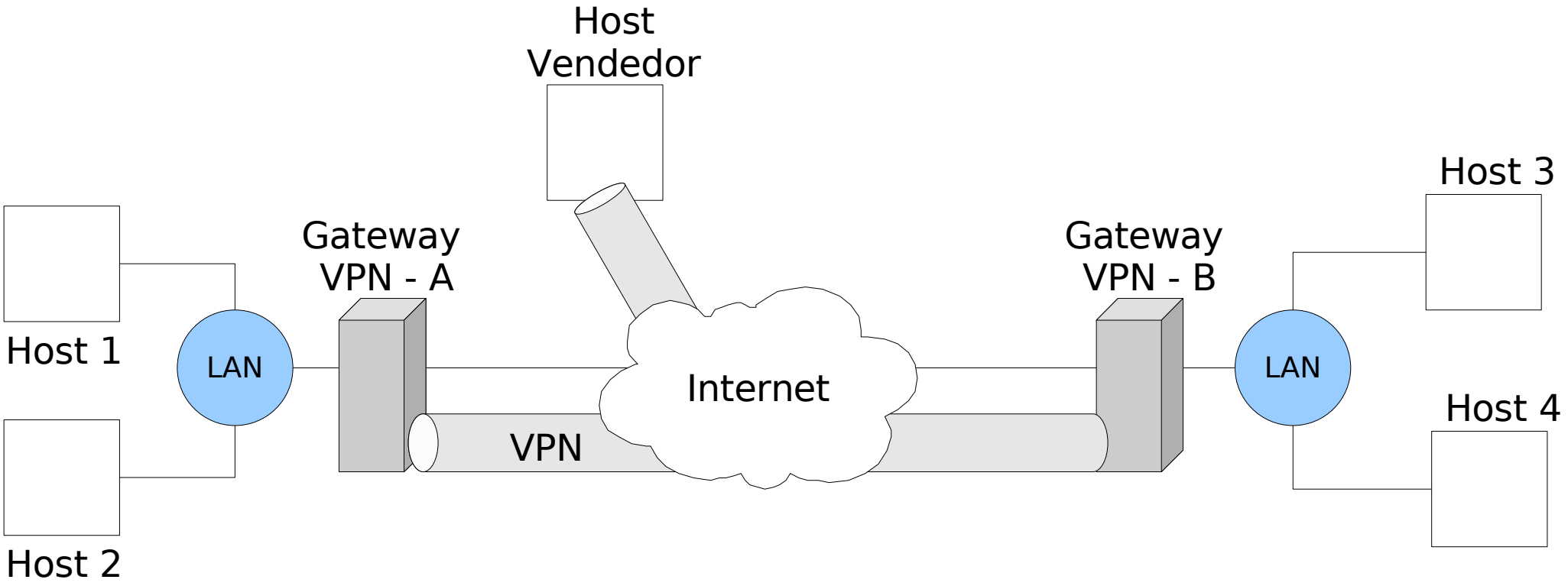
Este é o típico caso de ligação entre filias e sede, formando uma **extranet**. Cabe ao **gateway da VPN** definir quais usuários irão trafegar pela Internet e, dentre estes, quais irão usar o túnel VPN. Neste caso **a VPN é totalmente transparente para os usuários** da rede.

É válido ressaltar que neste cenário os **dados criptografados só ocorre entre os gateways e não dentro das redes locais**.

VPN – Virtual Private Network

Luiz Arthur

-Entre duas redes com acesso remoto:



Este é um cenário híbrido no qual temos hosts de acesso isolado (não permanentes) aos gateways da VPN, e outra conexão permanente entre os gateways VPN.

Cabe a algum elemento da rede decidir que se depois dos hosts não permanentes, por exemplo, um vendedores acessarem o gateway VPN se este pode acessar o outro gateway ou não, normalmente esta configuração fica a cargo do próprio gateway VPN.

Segurança na VPN

As VPNs normalmente **tentam manter a privacidade, integridade e autenticidade** da informação que trafega através das redes públicas.

Para **garantir** uma **rede** virtual **privada** é necessário que ninguém, nem nenhum equipamento não autorizado rede pública, consiga ler as informações da rede virtual. Para obter este nível de segurança podemos optar por **duas alternativas**:

- Adquirir uma **infra-estrutura física** de rede fornecida por uma empresa de comunicação de dados que garanta a privacidade na linha de dados em questão;

- Usar a **criptografia** para impossibilitar a compreensão das informações por pessoas não autorizadas, de forma que esta não consiga utilizá-la.

Empresas que administram a **infra-estrutura da Internet**, no caso dos backbones e provedores de acesso à Internet, podem oferecer redes privadas como é o caso do **MPLS (Multiprotocol Label Switching)** que adiciona um rótulo (label) no início de cada pacote e direciona os pacotes baseado nas informações desses rótulos, com isto, é permitido a criação de VPNs garantindo um isolamento completo do tráfego com a criação de tabelas de rótulos, usadas para roteamento, exclusivas de cada VPN.

Outros exemplos são ATM, Frame Relay e links dedicados. Este tipo de **VPN** é possível por que o tráfego da informação é **controlado nos cirtuitos e roteadores**, sendo garantida a privacidade na comunicação isolando o tráfego de cada empresa.

Porém atualmente existe uma tendência de se utilizar VPNs juntamente com criptografia ao invés de se utilizar links dedicados, para redução de custos.

Criptografia

A privacidade no mundo virtual está geralmente ligada as técnicas de criptografia utilizadas, diferente da privacidade "física" que os roteadores e switches tentam implementar, além do que esta privacidade física é difícil de se manter se não impossível. O que torna a criptografia uma ótima alternativa.
É claro que juntar as duas soluções (links dedicados e criptografia) vai ser uma boa opção mas normalmente muito cara.

Criptrografia é o estudo de códigos e crifras, cujo nome vem do grego `kryptos`, que significa oculto, e `graphem`, que significa escrever. Já a palavra **cifra** vem do hebraico `saphar`, que significa dar números.

Os espartanos foram os primeiros a utilizar um sistema de criptografia militar, por volta do século V a.C.

O imperador Julio César, há mais de 2000 anos, inventou o método de **criptografia por subistituição**, enviando mensagens trocando letras do alfabeto por três letras subseqüentes (`A->D, B->E`, etc...)

Neste tipo de criptografia milenar já surge um conceito fundamental para os dias atuais, **o segredo**, que é quantas letras do alfabeto eu devo contar para substituir as palavras, no exemplo anterior é 3, mas se alguém descobri-se este segredo é só mudá-lo. Tal segredo também é chamado de **chave de criptografia**.

Chamamos de **plaintext o texto original** e **ciphertext o texto embaralhado** ou criptografado.

Ao longo dos anos, inúmeras formas de criptografia foram usadas e junto vieram várias maneiras de descobrir como elas foram embaralhadas.

Atualmente o segredo da criptografia não esta no algoritmo empregado, e sim na chave criptográfica.

Os melhores sistemas criptográficos são aqueles de **domínio público**, podendo ser extensamente analisados pelos cientistas (hackers) e validados quanto a possíveis falhas ou fraquezas, sendo posteriormente revistos num processo permanente de melhoria (open source).

Chaves simétricas

Na chave simétrica **um mesmo segredo é compartilhado por todos**, ou seja, o destinatário sabe qual é a chave que é utilizada para voltar a informação à sua forma original.

O segredo reside na chave e o **problema** é conseguir fazer com que o emissor e o destinatário **escondam esta chave** de outras pessoas, de forma que, a segurança não seja quebrada. Mas a criptografia e descriptografia usando chaves simétricas **apresenta um ótimo desempenho** em relação a outras técnicas.

O conceito de chave simétrica surgiu em 1972 pela IBM com a aplido de Lucifer Cipher e foi revisto em 1977 pelo ANSI X9.32, já com o nome de Data Encryption Standard ou simplesmente **DES**. O DES trabalha com chave de comprimento de 64 bits, sendo 56 bits para a chave e 8 bits para paridade. O tempo para **descobrir o segredo** deste tipo de chave é **seria de 228 milhões de anos**.

Mas uma máquina chamada DES Cracker, criada para quebra do DES **quebrou uma chave DES em 3 dias**, posteriormente está máquina usando micros da Internet (100 mil) em **paralelo**, usando força bruta, ou seja, tentando resolver todas as combinações possíveis do algoritmo, quebraram a chave DES em **22 horas e 15 minutos**. Na época, estimou-se o tempo de processamento em torno de 256 bilhões de chaves por segundo.

A quebra do DES gerou desconfiança com o algoritmo e outras variantes do DES foram lançados, o **Duplo DES**, que usa 112 bits para o tamanho da chave, e o **Triplo DES**, ou 3-DES, que usa três chaves DES, combinadas entre si, para embaralhar a informação.

Mas o DES é muito seguro visto que esta quebra é muito difícil e não qualquer pessoa que tem um supercomputador para quebra-lo ainda mais se for com 3-DES.

Existem **vários outros algoritmos** para chaves simétricas, tais como: Blowfish, CAST-64, CAST-80, CAST-128, RC2, RC4, RC5, IDEA, etc, que podem ser usados, uma vez que com os recursos de hardware disponíveis atualmente, uma **quebra** por força bruta nessas variantes **ainda não é visualizada a curto prazo**.

Durante muito tempo cientistas da computação e matemáticos do munto todo **disputaram entre si a publicação de um algoritmo de criptografia** dito seguro: e depois de muitos testes e discussões o algoritmo eleito foi apresentado em 2 de dezembro de 2001, e o algoritmo selecionado foi o **Rijndael**.

Esta nova geração de criptografado agrega fatores como combinação de segurança, desempenho, eficiência, facilidade de implementação e flexibilidade em diversas plataformas.

Chaves assimétricas

As chaves assimétricas são chamadas também de **chaves públicas**.

Este conceito é bem mais amplo que o de chave simétrica.

Basicamente a chave é dividida em duas chaves:

- Uma **privada e unica** para o usuário que não pode ser compartilhada com ninguém;
- Outra de **domínio público** e disseminada para qualquer pessoa que queira enviar dados criptografados.

Normalmente a **chave privada** fica armazenada usando-se um algoritmo de chave simétrica como o DES ou **3-DES**.

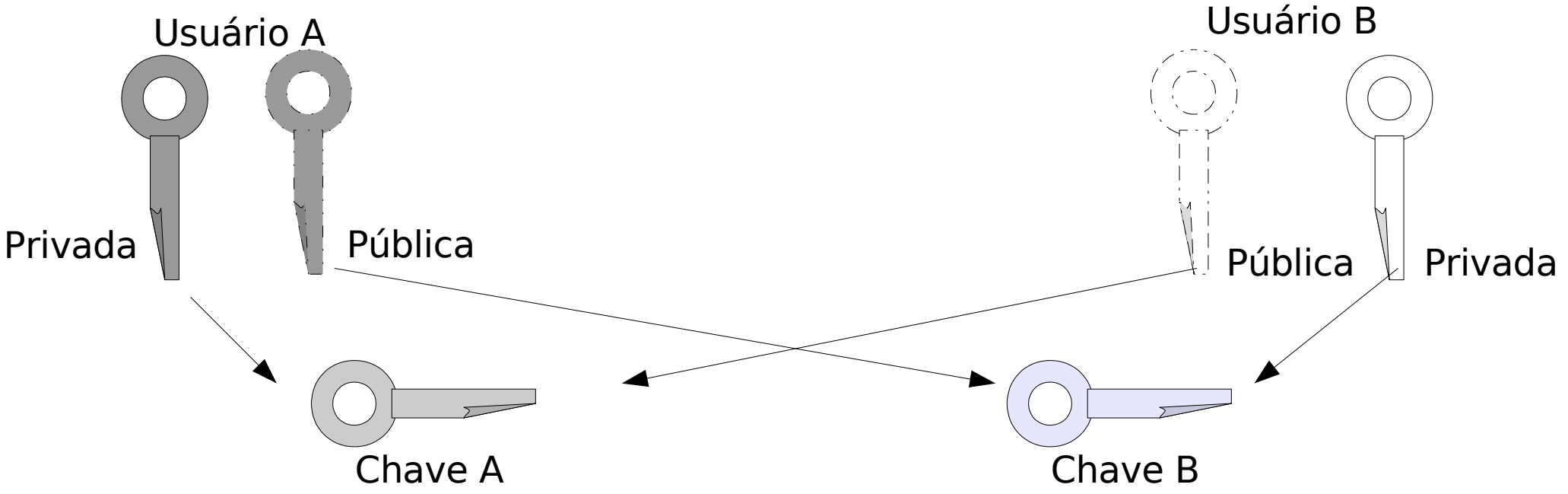
Quando queremos enviar uma informação criptografada para alguém, usamos a chave pública do nosso destinatário para criptografar e enviarmos o dado. Nosso destinatário utilizará a chave privada para descriptografar a mensagem e retorná-la à forma original. Caso ele queira enviar algo para nós, irá criptografas com nossa chave pública e enviar pela Internet, onde iremos usar nossa chave privada para descriptografar.

Existem basicamente dois algoritmos que implementão o uso de chaves assimétricas, sendo eles:

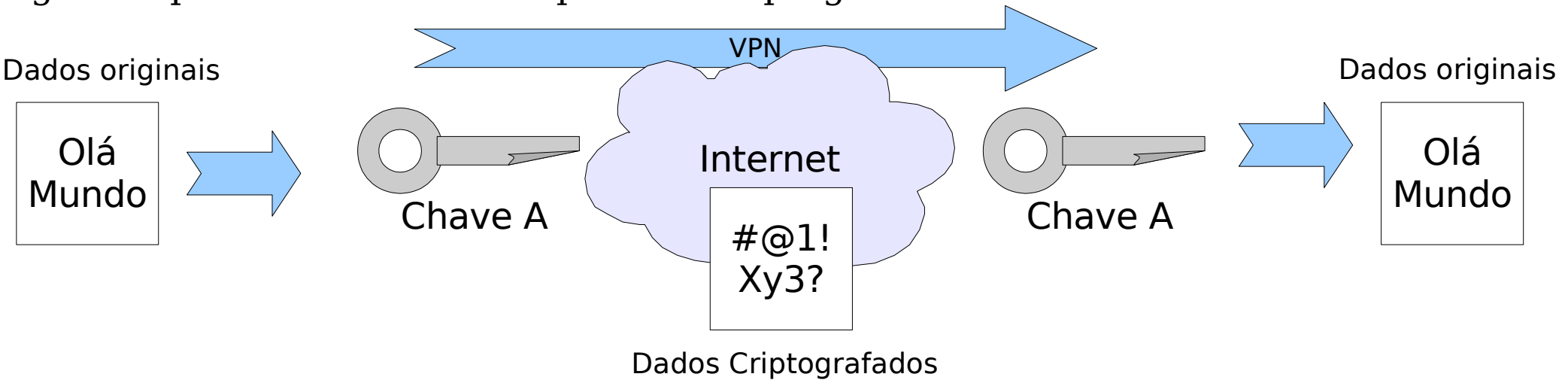
Diffie-Hellman

A Diffie-Helman **não tem por objetivo criptografar os dados** nem prover assinatura digital. **O objetivo do algoritmo é prover uma maneira rápida e eficiente de troca de chaves de criptografia**, entre dois sistemas, baseada nas duas partes da chave (pública e privada) de cada interlocutor.

O usuário A gera uma chave composta da chave privada dele e a chave pública do usuário B. O usuário B faz o inverso, ou seja, gera uma chave composta da chave privada dele mais a chave publica do usuário.



Por meio de um processo matemático, a chave gerada pelo usuário A serve para criptografar os dados a serem enviados ao usuário B e a chave gerada pelo usuário B serve para descriptografar, inversamente, a chave gerada pelo usuário B serve para criptografar os dados a serem enviados ao usuário A, e a chave gerada pelo usuário A serve para descriptografar.



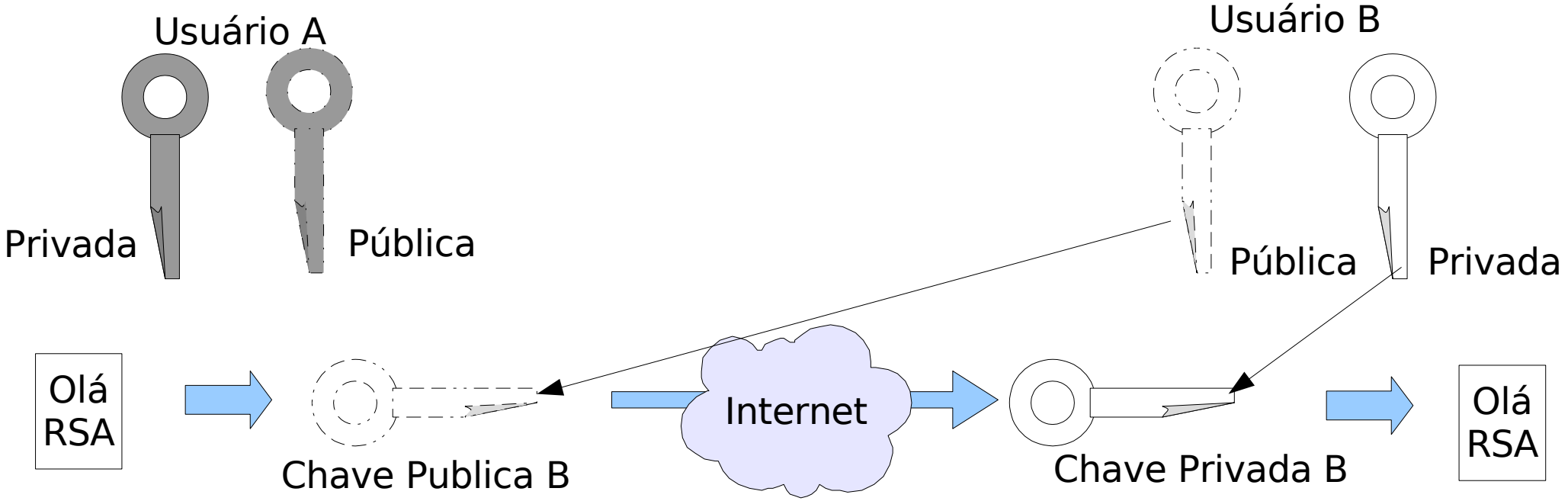
A grande **desvantagem** deste algoritmo, na verdade de todos os algoritmos de criptografia, está no momento de **pegar a chave pública do outro usuário**, sendo feita **de forma insegura**, outro usuário pode responder ao pedido se fazendo passar pelo usuário ao qual queremos enviar dados seguros.

Esta deficiência nos **algoritmos de criptografia se deve ao fato deles estarem preocupados com a criptografia e não com a autenticação**. Não é do escopo deles suportar um meio de distribuição seguro ou um meio de certificação de chaves.

RSA

O RSA está embutido nos navegadores Internet Explorer e outras centenas de produtos na Internet. Esse algoritmo **não faz a geração da chave**, mas usa as chaves previamente geradas por meio da infra-estrutura da chave pública, criptografando e descriptografando com o par de chaves de cada usuário.

Então no RSA existe dois conceitos em questão, a distribuição de chaves que não faz parte do algoritmo de criptografia e o algoritmo em questão.



No exemplo, o usuário A quer enviar alguma informação para o usuário B, neste caso, ele pega a chave pública do usuário B, criptografa a informação e envia pela Internet. O usuário B, que recebe a informação, usa sua chave privada para descriptografar a informação e retorná-la à sua forma original. O contrário é feito do outro lado quando B quer enviar algo para A.

As chaves públicas ficam disponíveis na rede por órgãos certificadores ou Certificate Authority – CA.

O método **RSA**, embora totalmente transparente ao usuário, pode ser de 100 a 10 mil vezes mais **lento** em função da complexidade do algoritmo e comprimento das chaves.

Encapsulamento e protocolos para VPN

Encapsulamento é um conceito muito utilizado nas VPN, para entender o que é encapsulamento, podemos comparar com uma carta, com conteúdo, remetente e destinatário, porém essa carta não está dentro de um padrão do correio, ou seja, não tem um formada de carta de correio comum. É, por exemplo, um papel que tem no início as informações necessárias para que a carta chegue ao destino, mas fora do padrão. A saída seria colocar essa carta dentro de um envelope, ou seja, pegá-la e colocar dentro de outra carta mas com o formato reconhecido pelo correio.

Então quando falamos de redes de computadores, podemos pegar uma **rede que não utilize o protocolo IP**, e fazer com que esta trafegue na Internet **colocando o pacote de uma rede não IP dentro de um pacote IP**. Este método é utilizado até mesmo pelo próprio protocolo IP, neste caso, o objetivo é esconder o endereço IP de origem, que pode ser um IP não válido para tráfego na Internet por um IP válido da Internet.

Um pacote IP é composto de cabeçalho (ou header) e os dados (ou payload).

"O encapsulamento consiste em gerar um novo cabeçalho com o datagrama original como payload".

Já os protocolos servem para definir como os pacotes serão encapsulados, como a chave de criptografia será compartilhada e outros métodos de autenticação.

Há dois conjuntos de protocolos:

- Os **orientados a pacotes**, que trabalham nas camadas de Enlace, Rede e Transporte do modelo OSI;
- Os **protocolos orientados à aplicação** que operam nas camadas de Sessão, Apresentação e Aplicação do modelo OSI.

Existe muita confusão em relação aos protocolos de tunelamento que podem ser utilizados para VPN, tomaremos que VPN é uma rede que visa privacidade, ou seja, somente pessoas autorizadas podem acessar tal rede.

Partindo dessa premissa de garantir **privacidade** na comunicação, **ou utilizamos a segmentação de rede**, tal como Frame Relay, ATM, MPLS, etc. **Ou** utilizamos **tuneis criptográficos** para tornar o canal de comunicação privado. Mas é claro que existem outras premissas de segurança que uma VPN pode abordar tal como: autenticação, integridade, etc, mas que não são relevantes a protocolos de tunelamento.

Alguns protocolos fazem exclusivamente o tunelamento, outros agregam criptografia e outras premissas da VPN, tal como:

7. Aplicação	SSH/SSL/TSL
6. Apresentação	
5. Sessão	SOCK v.5
4. Transporte	SunNET/TCP
3. Rede	IPSec/IP/SKIP/OpenSWAN
2. Enlace	PPTP/L2TP/L2F
1. Física	

PPTP (Point-to-Point Tunneling Protocol)

O PPTP foi desenvolvido por várias empresas tal como **Microsoft**, Lucent, US Robotics, etc. O PPTP tem o objetivo de facilitar o acesso remoto de **computadores em uma rede privada** através da Internet. O protocolo está incorporado ao Windows 95/98 e NT inclusive em versões mais recentes do Windows por compatibilidade, já que deve ser substituído pelo protocolo IPSec.

O **PPTP encapsula pacotes PPP** utilizando uma versão modificada do protocolo de Encapsulamento Genérico de Roteamento (GRE), que dá ao PPTP a flexibilidade de lidar com outros tipos de protocolos diferentes do IP, como o IPX e o NetBEUI.

Os pacotes a serem enviados pelo **túnel são encapsulados em um pacote GRE**, no qual existe o endereço do gateway de destino. Ao chegarem ao gateway destino, os pacotes são desencapsulados, ou seja, é retirado o cabeçalho GRE, e os pacotes seguem seu caminho determinado pelo endereço do cabeçalho original.

O protocolo **PPTP não inclui privacidade e gerência de chaves de criptografia**, o que é um problema quando falamos de VPN.

A autenticação do usuário no PPTP, fica por canta do próprio RAS que suporta Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) e Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

É possível usar um servidor **RADIUS** (Remote Authentication Dial-In User Service) ou **TACACS** (Terminal Access Controler Access Control System) para **autenticar usuários**. O TACACS+ utiliza ainda criptografia na autenticação.

A **comunicação segura** criada pelo PPTP tipicamente **envolve três processos**, cada um deles exigindo que os anteriores sejam satisfeitos, eles são:

- **Conexão e comunicação PPP**: O cliente PPTP usa o PPP para se conectar ao ISP, utilizando uma linha telefônica. O PPP é utilizado aqui para estabelecer a conexão e criptografar os dados;

- **Conexão de controle PPTP**: Utilizando a conexão estabelecida pelo PPP, o PPTP cria um controle de conexão desde o cliente até o servidor PPTP na Internet. Essa conexão **utiliza o TCP** e é chamada de túnel PPTP;

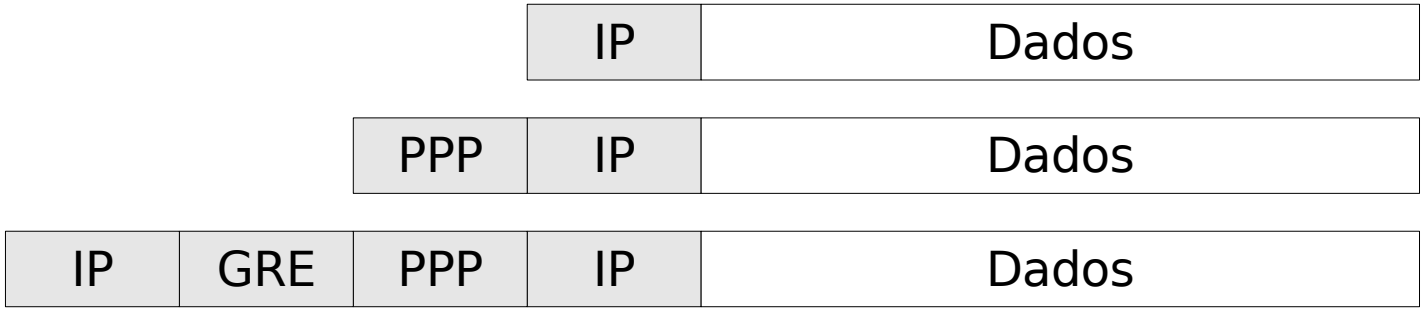
- **Tunelamento de dados PPTP**: O PPTP cria os datagramas IP contendo os pacotes PPP criptografados e os envia através do túnel até o servidor PPTP. Nesse servidor, os datagramas são então demostrados e os pacotes PPP descriptografados, para que finalmente sejam enviados até a rede privada corporativa.

VPN – Virtual Private Network

Partindo da premissa que toda conexão e túnel foram estabelecidos e o usuário remoto tem um datagrama IP para ser enviado a um equipamento dentro da rede local.

1. Datagrama IP original;
2. Datagrama IP dentro de um frame PPP;
3. Frame PPP encapsulado usando Encapsulamento de Roteamento Genérico (GRE), com cabeçalho IP;
4. Frame PPP com todo o pacote construído. Esse frame PPP é enviado do NAS para primeira conexão PPP encontrada.
5. Retirado o cabeçalho PPP, o pacote é enviado através da Internet para o servidor PPTP utilizando o túnel PPTP criado anteriormente;
6. O cabeçalho IP e o GRE são removidos e o servidor PPTP recebe o frame PPP;
7. Servidor PPTP retira o cabeçalho PPP e coloca o datagrama IP dentro da rede interna, que encontrará o caminho até o equipamento de destino.

PPTP não tem funções de segurança para os dados, porém utiliza os serviços de autenticação do protocolo PPP.



L2F (Layer Two Forwarding Protocol)

Na mesmo época de desenvolvimento do PPTP, a **Cisco** e algumas outras empresas proporam o **L2F**, que tinha como missão permitir que provedores de acesso ou empresas de telecomunicações oferecessem ao mercado acesso remoto discado para redes privadas; desta forma, as empresas não precisariam adquirir modens ou equipamentos de acesso.

O L2F usa qualquer protocolo orientado a pacote que pode prover conexão ponto-a-ponto, sendo então permitido os protocolos UDP, X.25, ATM e Frame Relay. A grande diferença entre o PPTP e o **L2F** é a terminação do túnel no L2F que **assume que a rede privada do cliente sempre estará atrás de um gateway**.

A grande desvantagem do L2F é a mesma que do PPTP, ou seja, não define criptografia.

L2TP (Layer Two Tunneling Protocol)

O protocolo **PPTP** tem o respaldo da Microsoft, no qual o túnel é construído com **computadores remotos**; desta forma são chamados de **túnel voluntários**.

Já o **L2F** tem o respaldo da Cisco, no qual o **túnel é formado do provedor de acesso** e não do computador remoto; desta forma são chamados de **túneis involuntários ou compulsórios**.

Tanto o PPTP e o L2F foram submetidos ao IETF com o propósito de virar um padrão a ser utilizado no mercado, porém isto não ocorreu e a **IETF lançou sua proposta que é o protocolo L2TP**.

Os desenvolvedores do PPTP continuaram sozinhos e os do L2F decidiram para o desenvolvimento desse protocolo e assumir a proposta L2TP.

O L2TP é muito similar ao PPTP, mas não utiliza controle TCP separado para o Controle do Canal. **O L2TP foi desenvolvido para suportar os dois modos de tunelamento, voluntário e compulsório**. Sendo que, o túnel voluntário é iniciado pelo computador remoto, sendo mais flexível para usuários em trânsito que podem discar para qualquer provedor de acesso.

O túnel compulsório é automaticamente criado, sendo iniciados provedor de acesso à Internet sob a conexão discada. Isto implica que o provedor deve ser pré-configurado para saber a terminação de cada túnel baseado nas informações de autenticação dos usuários remotos que estão estabelecendo a conexão. Isto é feito sem nenhuma intervenção do usuário remoto e não há necessidade de software nos computadores remotos, sendo o **processo de tunelamento completamente transparente ao usuário final**.

O protocolo de tunelamento L2TP, bem como PPTP e L2F, sofre da **falta de mecanismos sólidos de proteção ao túnel**. O L2TP encapsula frames PPP, logo ele herdou os mecanismos de segurança, incluindo autenticação e serviços de criptografia, mas não fornece mecanismo de gerência de chaves para criptografia e autenticação. Então o IPSec se faz necessário.

IPSec

O objetivo da camada de Rede do modelo OSI é fornecer **endereçamento e roteamento ao pacote de rede**. Os serviços do nível de rede OSI relativos à interconexão de redes distintas são implementados na arquitetura TCP/IP pelo **protocolo IP**, ou seja, só existe uma opção de protocolo e serviço para esta camada, pelo menos se esperamos usar a Internet.

Infelizmente o protocolo **IP versão 4 não tem mecanismos de segurança próprios** (segurança em termos de privacidade, confidencialidade, autenticação, etc), desta forma, é necessário adicionar protocolos e procedimentos para garantir a segurança das informações dentro do datagrama IP.

Assim, o **IPSec é um conjunto de protocolos** que define a arquitetura e as especificações **para prover serviços de segurança dentro do protocolo IP**. O IPSec foi padronizado para garantir interoperabilidade, mecanismo de criptografia para o IPv4 e IPv6. O IPSec também define um conjunto de serviços de segurança, incluindo **integridade** dos dados, **autenticação**, **confidencialidade** e **limite de fluxo de tráfego**.

IPSec oferece este serviços independente do algoritmo de criptografia usado, ou seja, o IPSec possui **arquitetura aberta** e assim, **possibilita o uso de vários algoritmos de autenticação e criptografia**.

Protocolos do IPSec

Os serviços de **segurança do IPSec são oferecidos por meio de dois protocolos** de segurança o **Authentication Header** (Autenticação de Cabeçalho ou AH) e o **Encapsulation Security Payload** (Encapsulamento Seguro de Dado ou ESP).

Atualmente a lista de protocolos disponíveis, não necessariamente implementados por todos os fornecedores de IPSec, inclui:

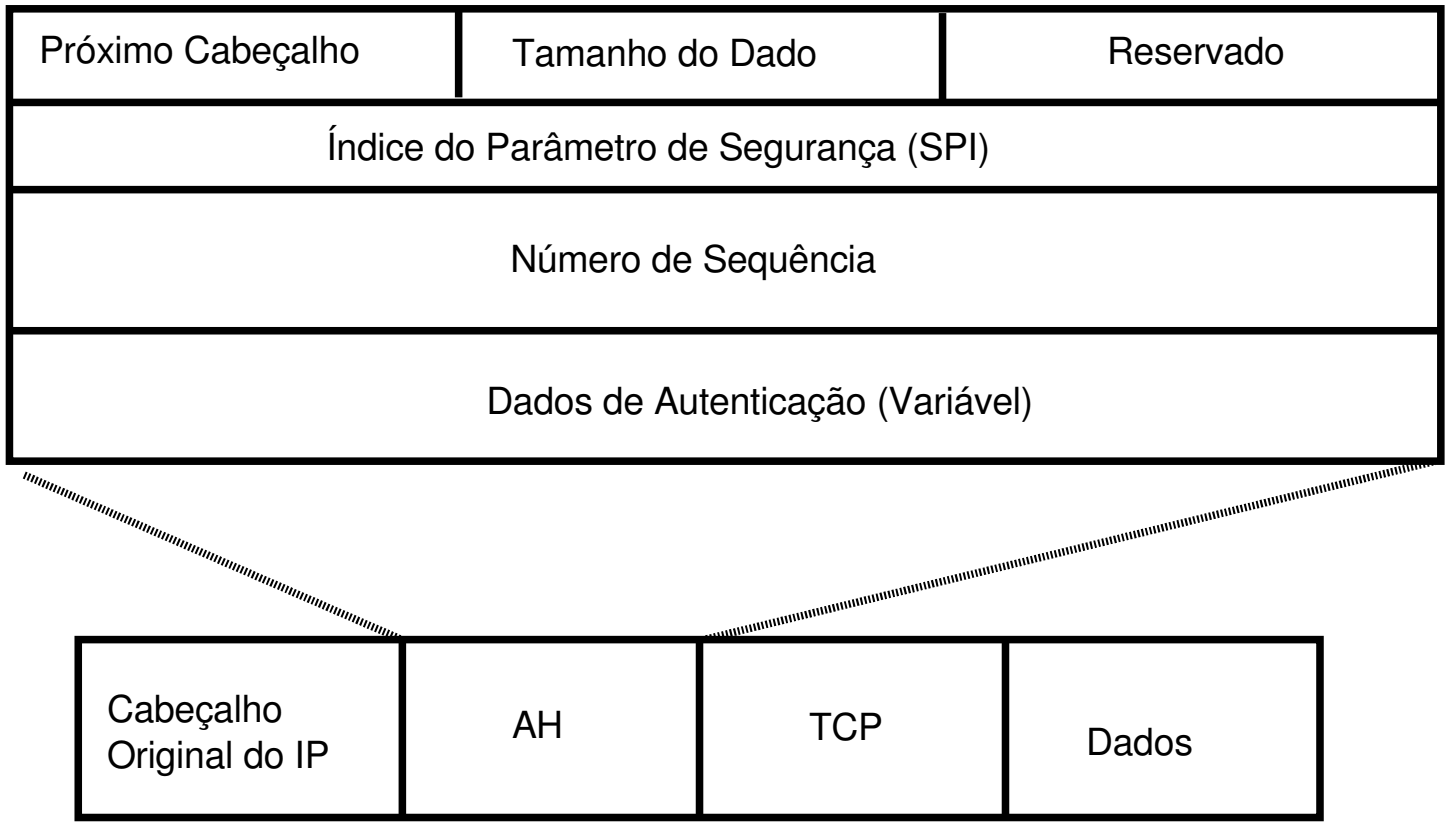
Criptografia: DES, Blowfish, 3-DES, CAST, AES, SERPENT, TWOFISH, etc.
Autenticação: HMAC, MD5, SHA1, SHA2, etc.

É claro que estes protocolos podem não estar mais na lista do IPSec, ou existirem outros, isto se dá devido a evolução dos protocolos e dos hackers.

Authentication Header

O protocolo **AH adiciona autenticação e integridade ao pacote IP**, ou seja, garante a autenticidade do pacote e também que este não foi alterado durante a transmissão. O AH pode ser usado em modo transporte e em modo túnel.

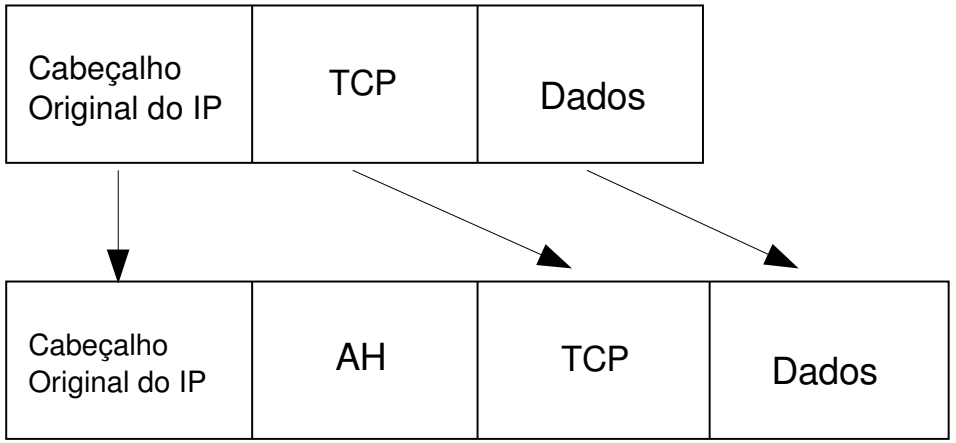
O protocolo AH previne ataques do tipo Replay, ou seja, quando uma pessoa mal intencionada captura pacotes válidos e autenticados que pertencem a uma conexão, replica-os e os reenvia, como se fosse a entidade que iniciou a conexão. Também previne ataques do tipo spoofing, ou seja, quando um invasor assume o papel de uma entidade confiável para o destino e dessa forma, ganha privilégios na comunicação. E por último, previne contra ataques do tipo connection hijacking, ou seja, quando o invasor intercepta um pacote no contexto de uma conexão e passa a participar da comunicação.



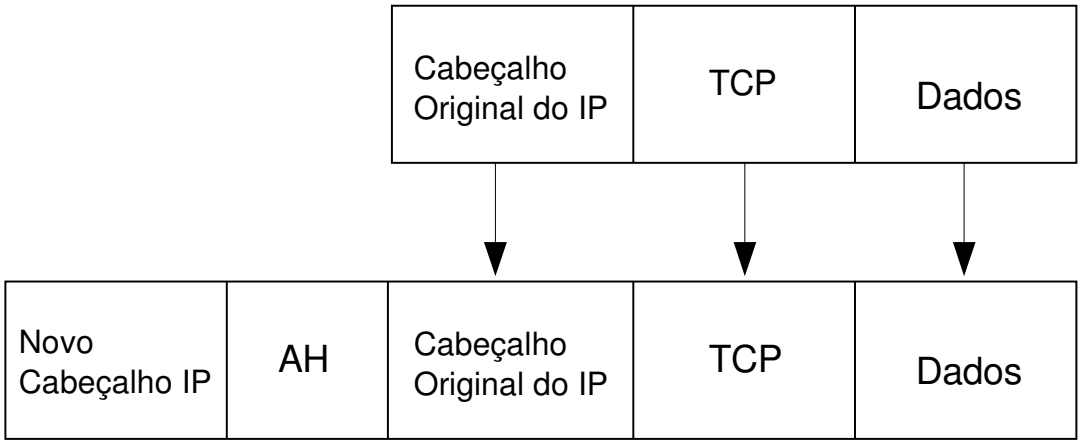
Embora a autenticação aconteça no pacote IP, nem todos os campos vão ser autenticados, por que alguns campos do cabeçalho serão alterados no decorrer da transmissão.

O mecanismo de autenticação é feito utilizando a função hash, utilizando a chave negociada durante o processo de estabelecimento da conexão IPSec.

O protocolo AH adiciona um cabeçalho de autenticação depois do cabeçalho original do pacote ou depois de um novo cabeçalho construído. No modo transporte é usado o mesmo cabeçalho original e troca-se somente o campo Protocolo. Já no modo túnel, é gerado um novo cabeçalho, contendo o cabeçalho original encapsulado, seguido pelo cabeçalho de autenticação



Modo transporte

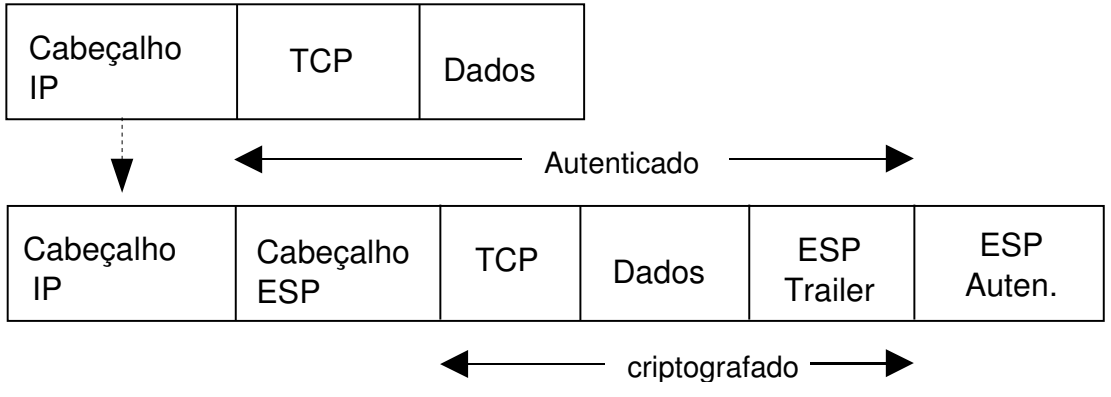


Modo túnel

Encapsulation Security Payload

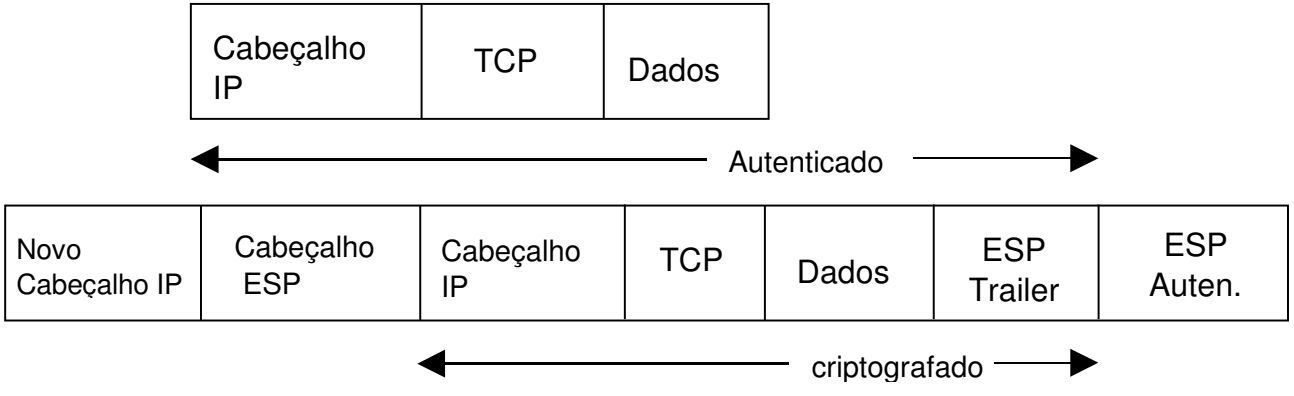
O protocolo de Encapsulamento Seguro do dado (ESP), oferece **confidencialidade**, **integridade** dos dados, e uma opção de **autenticação** da origem dos dados e serviços anti-replay.

Como o pacote IP é um datagrama, cada pacote deve conter informações necessárias para estabelecer o sincronismo da criptografia, permitindo que a descriptografia ocorra na entidade de destino. Se nenhum algoritmo de criptografia for utilizado, o que é uma situação possível no padrão, o protocolo ESP só oferecerá o serviço de autenticação.



Modo Transporte ESP

Modo Túnel ESP



fim