**Tunelamento através da Camada de Enlace**

Nos protocolos de tunelamento através da **camada 2 (de Enlace)**, os pacotes da camada 3 (como IP) são encapsulados em quadros PPP (Point-to-Point Protocol) para serem transportados através da Internet.

* **PPTP** - Desenvolvido por um consórcio de empresas formado por Microsoft, 3Com, Ascend, US Robotics e ECI Telematics, o PPTP (Point-to-Point Tunneling Protocol) é uma extensão do PPP. Desde o Windows 95, todas as versões do Microsoft Windows incluem um cliente PPTP.
* **L2F** - O L2F (Layer 2 Forwarding), da Cisco Systems, permite a criação de VPNs discadas.
* **L2TP -** O L2TP resulta de uma combinação de funcionalidades do PPTP e do L2F e permite que uma estação de trabalho PPP e um dispositivo a operar ao nível da ligação de dados residam em redes distintas, interligadas por uma rede de comutação de pacotes. Uma ligação L2TP envolve dois componentes – o L2TP Access Concentrator (LAC), instalado no cliente, e o L2TP Network Server (LNS), no lado do servidor. Tal como no PPTP, recorre a um canal de controle não exige uma ligação TCP autônoma. O túnel L2TP, tal como no L2F, é construído sobre UDP.

**Tunelamento através da Camada de Rede** **IPSec** **(camada 3)**

* **IPSec -** É um protocolo definido pelo IETF utilizado para transferir dados de maneira segura na Camada de Rede. Ele é uma extensão do protocolo de internet IP, proporcionando segurança, garantindo a privacidade e integridade dos dados enviados.

Existem 2 "arquiteturas" distintas para se implantar uma VPN. Ou por **criptografia** de dados ou por **isolamento** de trafego. Na criptografia, os dados são trafegados entre os envolvidos criptografados, garantindo a confiabilidade, autenticidade e integridade. Já no isolamento de trafego, são adicionados rótulos nos pacotes e o fluxo de dados é baseado nestes rótulos. Por isso se diz que VPN com isolamento de trafego não é "verdadeiramente" uma VPN, já que não possui todas as seguranças necessárias:  
Como exemplo de VPN com isolamento de trafego podemos citar o protocolo **MPLS**, já VPNs com criptografia temos o **SSL/TLS, IPSec, SSH, SHTTP**.

**IPsec**é uma abreviação de Internet Protocol Security. O IPsec é um protocolo de VPN usado para proteger a comunicação de Internet através de uma rede IP. Um túnel que está configurado em um site remoto permite o acesso ao seu site central. Um IPsec funciona para proteger a comunicação do protocolo de Internet verificando cada sessão e criptografando individualmente os pacotes de dados em toda a conexão. Uma VPN IPsec tem dois modos de operação. Os dois modos são: **modo de transporte e modo de tunelamento.** Ambos os modos servem para proteger a transferência de dados entre duas redes diferentes. Durante o modo de transporte, a mensagem no pacote de dados é criptografada. No modo de tunelamento, o pacote de dados completo é criptografado. Uma vantagem de se utilizar uma VPN IPsec é que ela também pode ser utilizada em adição a

outros protocolos de segurança para proporcionar um sistema de segurança mais forte.

*O IPSec permite ao remetente (ou um gateway de segurança, atuando em seu lugar) autenticar ou encriptar cada pacote IP ou aplicar ambas as operações a um mesmo pacote. A separação entre autenticação e encriptação criou duas formas de utilização do IPSec, conhecidas como modo de transporte e modo de tunelamento.*

*Em****modo de transporte****, utilizado para comunicação segura host-a-host, os pacotes recebem encriptação e/ou autenticação, enquanto****os cabeçalhos são mantidos (quase) intactos****.****Os endereços originais do cabeçalho são mantidos, apenas alguns campos são adicionados****para identificar o pacote IPSec.*

*No****modo de tunelamento****, cria-se um túnel IPSec entre os dois pontos conectados à rede pública (Internet). O tunelamento IPSec é transparente à rede, portanto, os hosts comunicam-se utilizando endereços locais, como se estivessem na mesma rede.****O pacote IP original é encapsulado em um pacote IPSec****, que tem um cabeçalho IP próprio, utilizado para o roteamento na rede pública. O modo de tunelamento do IPSec é a forma preferida para a implementação de VPNs.*

***Protocolos***

Os principais protocolos de segurança utilizados nos serviços requisitados, como autenticação básica, integridade e encriptação de dados, são: autenticação de cabeçalho (Authentication Header, AH) e encapsulamento para a segurança da mensagem (Encapsulated Security Payload, ESP).  
  
**Autenticação de Cabeçalho:** O protocolo AH, como o próprio nome já diz, autentica. Ele não altera a mensagem e sim, adiciona um cabeçalho do tipo AH ao pacote IP contendo um hash de dados e uma sequência numérica. Com isso pode ser verificada a integridade dos dados e a autenticidade do emissor do pacote.  
  
**Encapsulamento para segurança da mensagem (Encapsulated Security Payload, ESP):** O protocolo ESP utiliza algoritmos de encriptação para dar confidencialidade aos dados além de autenticar a fonte e garantir a integridade dos dados. Dessa forma o protocolo de ESP precisa ser utilizado de forma equivalente em ambos os lados da comunicação, ou seja, o algoritmo de encriptação necessariamente precisa ser o mesmo. O ESP tem suporte para operar num modo onde há apenas encriptação ou num modo onde há apenas autenticação.

RESUMO IPSec:

* **AH** -------------------------------> Integridade + autenticidade
* **ESP**------------------------------> confidencialidade + integridade + autenticidade
* **Modo Transporte**----------> não gera novo cabeçalho
* **Modo Túnel**-----------------> gera novo cabeçalho (garante a privacidade)

Existem vários meios de implementar uma VPN, cada um com suas características e dentro de sua possibilidade.

**PPTP e L2TP** na camada 2.  
**MPLS** na camada "2.5"  
**IPSEC** na camada 3  
**SSL/TLS**na camada de API/socket. (entre a camada de transporte e de aplicação no modelo TCP/IP).

***Localização da VPN/Firewall***

Em Frente ao Firewall

* - Representa um ponto único de falha.
* - Impossibilidade de verificar o comprometimento do Gateway VPN, pois Firewall Aceita os pacotes vindos do Dispositivo.
* \*Caso a VPN seja comprometida, Firewall deixara passar todos os Pacotes.

Atrás Do Firewall

* - Também se Constitui um Ponto único de falha
* - Agravante, obriga que o firewall deixe passa todo trafego cifrado.
* - Dessa forma, a política de segurança deixa de ser efetivamente cumprida em relação às regras de filtragem.
* - Atacantes realizariam ataques através de pacotes cifrados.

No firewall

* - Administração e gerenciamento simplificado.
* - Continua sendo ponto único de falha.
* - Falhas na implementação da VPN pode significar o controle do dispositivo ao atacante, possibilitando a alteração de regras de firewall e todas as conexões.

Paralelo ao Firewall

* - A VPN deixa de ser um ponto único de falha.
* - Mas ele fica passível de ataques oriundos da internet.
* - Viabilizando um caminho alternativo ao atacante.
* - Não haverá regras de filtragem atribuídas as conexões de VPN.

Na Interface do Firewall

* - Configuração mais indicada
* - O firewall realiza a proteção do dispositivo VPN
* - Todo o pacote é filtrado pelas regras de Firewall.
* \*Funcionamento - Pacotes IPSec são enviados diretamente ao dispositivo VPN.
* - Eles são decifrados e enviados de volta ao Firewall para filtragem segundo suas Regras

VPN’s podem ser divididas em quatro tipos básicos de comunicação:

* **Linha Virtual Alugada** (Virtual Leased Line,VLL) - Utiliza o Espinha Dorsal IP (backbone IP) como entidade de enlace e transporte fim-a-fim, conectando dois usuários por um túnel IP que emula um circuito físico ou linha privada, podendo começar e terminar em uma mesma estação.
* **Rede Privada Virtual Roteada** (Virtual Private Routed Network, VPRN) - Atua na terceira camada estabelecendo conexões entre os roteadores e construindo tabelas de roteamento para os clientes se conectarem com o servidor e também pode ser usado no controle de tráfego. Devido à sua complexa implementação, ele é mais usado no meio empresarial e centros de processamento de dados.
* **Rede Privada Virtual Discada** (Virtual Private Dial Network, VPDN) - Permite ao usuário remoto se conectar por demanda através de um túnel para outro site. O usuário é conectado a um IP público e seus pacotes são enviados pelo túnel através da rede pública para o site desejado dando a impressão de uma conexão direta. A característica chave dessa conexão é necessidade de uma autenticação do usuário.
* **Segmento de Rede Virtual Privada Local** (Virtual Private LAN Segment, VPLS) - Permite que sites distantes entre si compartilhem uma conexão através de pseudo-fios. Oferece suporte a broadcast e multicast.

**SSL -** Secure Sockets Layer e **TLS** - Transport Layer Security. Elas funcionam como um protocolo. Ambas são usadas para construir uma conexão VPN. Está é uma conexão VPN na qual o navegador Web serve como cliente e o acesso de usuário é restrito a aplicativos específicos em vez de uma rede inteira. O protocolo SSL e TLS é utilizado principalmente por sites de compras online e prestadores de serviços. Uma VPN SSL e TLS fornece a você uma sessão segura a partir de seu navegador de PC para o servidor de aplicativos. Isso ocorre porque os navegadores Web mudam para SSL facilmente e não exigem praticamente nenhuma ação do usuário. Os navegadores Web já vêm integrados com SSL e TLS. As conexões SSL tem https no início da URL em vez de http.

**MPLS -** Multi-Protocol Label Switching ou VPNs MPLS são melhores para o uso do tipo de conexões Site a Site. Isto ocorre principalmente devido ao fato de que as MPLS são a opção mais flexível e adaptável. A MPLS é um recurso baseado em padrões que é usado para acelerar a distribuição de pacotes de rede através de vários protocolos. As VPNs MPLS são sistemas que são VPNs sintonizadas com ISP. Uma VPN sintonizada com ISP é quando dois ou mais sites estão conectados para formar uma VPN usando o mesmo ISP. No entanto, a maior desvantagem de usar uma VPN MPLS é o fato de a rede não ser tão fácil de montar comparativamente a outras VPN. Além disso, não é fácil de fazer modificações. Portanto, VPNs MPLS são tipicamente mais caras.

 http://www.hardware.com.br/tutoriais/vmware-server2/