1 - O que é uma VPN?

R.: VPN ou Virtual Private Network é uma rede de comunicação privada que controla a comunicação
de forma segura entre 2 hosts

2 - Quais as 3 garantias no uso da VPN?

R.: As garantias são
Integridade: A VPN deve garantir que os dados capturados não sejam acessados
Autencidade: garantir que os dados de fora do túnel não entrem
Confidencialidade: garantir o conteúdo da informação.

Esses características vimos em aula. Abaixo segue mais alguns itens pesquisados:

* Autenticação de Usuários
Verificação da identidade do usuário, restringindo o acesso às pessoas autorizadas. Deve dispor
de mecanismos de auditoria, provendo informações referentes aos acessos efetuados – quem acessou , o quê e quando foi acessado.

* Gerenciamento de Endereço
O endereço do cliente na sua rede privada não deve ser divulgado, devendo-se adotar endereços fictícios para o tráfego externo.

* Criptografia de Dados
Os dados devem trafegar na rede pública ou privada num formato cifrado e, caso sejam interceptados por usuários não autorizados, não deverão ser decodificados, garantindo a privacidade da informação. O reconhecimento do conteúdo das mensagens deve ser exclusivo dos usuários autorizados.

* Gerenciamento de Chaves
O uso de chaves que garantem a segurança das mensagens criptografadas deve funcionar como um segredo compartilhado exclusivamente entre as partes envolvidas. O gerenciamento de chaves deve garantir a troca periódica das mesmas, visando manter a comunicação de forma segura.

* Suporte a Múltiplos Protocolos
Com a diversidade de protocolos existentes, torna-se bastante desejável que uma VPN suporte protocolos padrão de fato usadas nas redes públicas, tais como IP (Internet Protocol), IPX (Internetwork Packet Exchange), etc.

3 - Em que casos as VPN são mais utilizadas?

R.: A VPN ganhou popularidade á medida que os custos em banda larga foram diminuindo popularizando o acesso a internet. Nesse contexto é muito utilizada para:
* trafegar dados em redes não seguras (rede publica);
* tornar um meio inseguro em um meio seguro (rede publica);
* Empresas usam VPN para comunicar hosts de fora da sua rede com sua rede interna.

4 - Como pode ser garantida a confidencialidade?

R.: Confidencialidade é a propriedade da comunicação que permite que apenas usuários autorizados entendam o conteúdo transportado. Desta forma, os usuários não autorizados, mesmo tendo capturado o pacote,

não poderão ter acesso às informações nele contidas. O mecanismo mais usado para prover esta propriedade é chamado de criptografia.
O serviço que garante a "confidencialidade" no IPSec é o ESP - Encapsulating Security Payload. O ESP também provê a autenticação da origem dos dados, integridade da conexão e serviço anti-reply. A "confidencialidade" independe dos demais serviços e pode ser implementada de 2 modos - transporte e túnel. No primeiro modo, o pacote da camada de transporte é encapsulado dentro do ESP, e, no túnel, o datagrama IP é encapsulado inteiro dentro do cabeçalho do ESP.

5 - Como pode ser garantida a integridade?

R.: Integridade significa que os dados transmitidos chegam ao seu destino íntegros, eliminando a possibilidade de terem sido modificados no caminho sem que isto pudesse ser detectado.
O AH é um mecanismo que provê integridade e autenticação dos datagramas IP. A segurança é garantida através da inclusão de informação para autenticação no pacote a qual é obtida através de algoritmo aplicado sobre o conteúdo dos campos do datagrama IP, excluindo-se aqueles que sofrem mudanças durante o transporte. Estes campos abrangem não só o cabeçalho IP como todos os outros cabeçalhos e dados do usuário. No IPv6, o campo hop-count e o time-to-live (TTL) do IPv4 não são utilizados, pois são modificados ao longo da transferência.
Para alguns usuários o uso da autenticação pode ser suficiente não sendo necessária a "confidencialidade".
No IPV6, o AH normalmente é posicionado após os cabeçalhos de fragmentação e End-to-End, e antes do ESP e dos cabeçalhos da camada de transporte (TCP ou UDP, por exemplo).

6 - O que é IPSEC?

R.: O IPSec é um protocolo padrão de camada 3 projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada. Essencialmente, ele pega pacotes IP privados, realiza funções de segurança de dados como criptografia, autenticação e integridade, e então encapsula esses pacotes protegidos em outros pacotes IP para serem transmitidos. As funções de gerenciamento de chaves também fazem parte das funções do IPSec.
Tal como os protocolos de nível 2, o IPSec trabalha como uma solução para interligação de redes e conexões via linha discada. Ele foi projetado para suportar múltiplos protocolos de criptografia possibilitando que cada usuário escolha o nível de segurança desejado.

7 - O que é AH?

R.: Authentication Header (AH). Este cabeçalho, ao ser adicionado a um datagrama IP, garante a integridade e autenticidade dos dados, incluindo os campos do cabeçalho original que não são alterados entre a origem e o destino; no entanto, não fornece confidencialidade. É utilizada uma função hash com chave, ao invés de assinatura digital, pois o mecanismo de assinatura digital é bem mais lento e poderia reduzir a capacidade da rede.

8 - O que é ESP?

R.: Encapsulating Security Payload (ESP). Este cabeçalho protege a confidencialidade, integridade e autenticidade da informação. Se o ESP

for usado para validar a integridade, ele não inclui os campos invariantes do cabeçalho IP.