REDES VIRTUAIS PRIVADAS

VPN

Universidade Católica do Salvador
Curso de Bacharelado em Informática
Disciplina: Redes de Computadores
Professor: Marco Antônio Câmara
Aluna: Patricia Abreu

VPN – VIRTUAL PRIVATE NETWORK

1. INTRODUÇÃO

Rede Privada Virtual (VPN – Virtual Private Network) é uma rede privada construída sobre a infra-estrutura de uma rede pública já existente, normalmente a Internet, onde o acesso e a troca de dados só são permitidos a pessoas que estejam autorizadas.

Para entendermos melhor esse conceito falaremos mais um pouco sobre algumas características importantes:

As redes públicas não são confiáveis, pois os dados que trafegam nelas podem ser interceptados e capturados, mas, por outro lado, tem um custo de utilização inferior aos necessários para o estabelecimento de redes privadas, pois esta envolve a contratação de links dedicados e muitos outros equipamentos.

Com o grande crescimento da internet, o aumento da sua área de abrangência, a expectativa de uma rápida melhoria na qualidade dos meios de comunicação e o aumento das velocidades de acesso, aquela passou a ser vista como um meio conveniente para as comunicações corporativas. Contudo, o tráfego de informações confidenciais pela internet só é possível com o uso de alguma tecnologia que torne esse meio inseguro em um meio confiável.

Veremos mais na frente quais as tecnologias empregadas para tornar o meio público confiável.

1.1 TUNELAMENTO

A VPN é uma rede privada simulada onde os links dedicados existentes em uma rede privada convencional são simulados por um túnel, através da técnica de tunelamento. Essa técnica, é o encapsulamento ponto-a-ponto das transmissões dentro de pacotes IP. O tunelamento permite:

- ✓ tráfego de dados de várias fontes para diversos destinos em uma mesma infra-estrutura;
- ✓ tráfego de diferentes protocolos em uma mesma infra-estrutura a partir de encapsulamento;
- ✓ tratamento de QoS (Quality of Service), direcionado e priorizando o tráfego de dados para destinos específicos.

Um ponto importante que deve ser observado é que na estrutura de redes privadas convencionais, as conexões são mantidas por links permanentes entre dois pontos da rede. Já nas redes virtuais privadas, as

conexões são dinâmicas, pois elas são criadas no momento em que se tornam necessárias e são desativadas quando não são mais necessárias, fazendo com que a banda esteja disponível para outros usuários.

Os túneis podem consistir de dois tipos de pontos finais, que podem ser: uma LAN ou um usuário remoto tentando acessar a LAN corporativa.

No caso de túneis entre duas LAN's, chamado de Tunelamento LAN-to-LAN, pode haver um gateway seguro (roteador ou firewall) em cada ponto, servindo de interface entre o túnel e a LAN privada.

No caso de túneis entre um usuário remoto e a LAN corporativa temos o tunelamento Client-to-LAN, onde o usuário remoto deve possuir instalado em sua máquina um software que possibilite transpor o gateway que protege a LAN de destino.

Abaixo temos algumas figuras que demonstram como é feita a comunicação através de túneis VPN LAN-to-LAN (Figura 1) e Client-to-LAN (Figura 2):

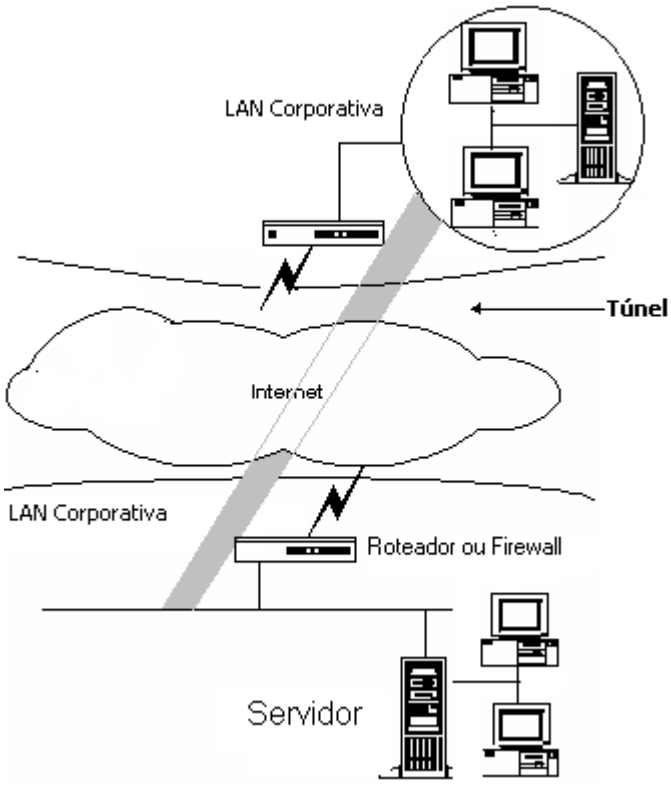

Figura 1: Rede VPN – Tunelamento LAN-to-LAN

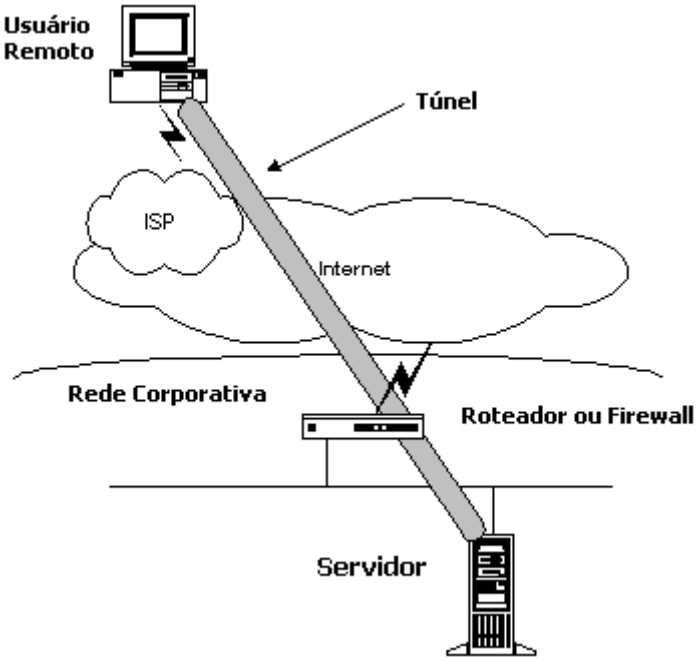

Figura 2: Rede VPN – Tunelamento Client-to-LAN

2. MOTIVAÇÕES

Uma das principais motivações do uso da VPN em detrimento do uso das redes privadas convencionais é a redução de custos. Podemos citar, também, como uma vantagem da VPN a sua grande abrangência (acesso de qualquer rede pública) e o fato de serem facilmente escaláveis.

2.1 REDUÇÃO DE CUSTOS

As redes tradicionais são baseadas em diversos links dedicados acarretando altos custos mensais fixos, principalmente quando se leva em consideração redes WAN que envolvem longas distâncias.

Já utilização de VPN acarreta em uma redução desses custos, já que utilizam um único link com banda menor, com custo variável, necessitando de somente um roteador no lado do cliente reunindo todos os serviços (Internet e WAN) em um só, provendo acesso remoto através de um provedor de Internet que detêm os provedores de acesso e as linhas telefônicas e acarreta uma diminuição nos custos com suporte e manutenção.

2.2 ACESSO DE QUALQUER REDE PÚBLICA

A VPN provê acesso de qualquer rede pública, pois com apenas um software de acesso remoto é possível conectar-se a ela. Hoje em dia, a Internet possibilita interligação com quase todo o mundo.

2.3 FACILMENTE ESCALÁVEIS

As VPN's são facilmente escaláveis, pois para se interconectar mais um escritório à rede basta contatar o provedor de serviços para a instalação do link local e respectiva configuração dos poucos equipamentos nas instalações do cliente. Da mesma forma, no momento em que a utilização da rede esbarrar na banda disponível no link local alugado do provedor, basta requisitar um aumento desta banda para se determinar uma melhora considerável no desempenho da rede.

É importante ressaltar que a questão da escalabilidade deve levar em consideração a especificação dos equipamentos quanto à quantidade de endereços MAC conectáveis e o número máximo de túneis. Desde que exista folga nestes parâmetros, é fácil escalar.

3. SEGURANÇA

A segurança é um aspecto primordial que deve ser levado em consideração para o desenvolvimento de VPN's sobre a infra-estrutura da rede já existente.

Os protocolos TCP/IP (Transmission Control Protocol /Internet Protocol) e a própria Internet não foram originalmente projetados tendo a segurança como prioridade, pois o número de usuários e os tipos de aplicações não exigiam a garantia da mesma. Mas as VPN's exigem para sua implementação um rigoroso cuidado com a segurança, já que elas são substitutas das linhas dedicadas e para tanto devem atender essa premissa. Por esse motivo, houve a necessidade de acrescentar tecnologias que possibilitam a criação de um meio seguro de comunicação dentro da internet.

Essas tecnologias devem assegurar que a comunicação esteja protegida de escutas clandestinas, que os dados não sofrerão alterações e que a rede esteja protegida contra intrusos.

Abaixo segue a maneira de como implementar essas premissas:

3.1 CONTROLE DE ACESSO

O controle de acesso basicamente dita os direitos de cada usuário na rede, visando negar acesso a um usuário que não está autorizado a acessar a rede como um todo, ou simplesmente restringir o acesso de

usuários. Por exemplo, se uma empresa possui áreas como administrativa-financeira e desenvolvimento de produtos é correto imaginar que um funcionário de uma divisão não deva acessar e, possivelmente, obter dados da rede da outra divisão. Ele também faz o controle e "log" de todos os acessos dos usuários na rede.

3.2 AUTENTICAÇÃO

A autenticação permite a entrada do usuário na rede virtual privada. Isto é feito, geralmente, através de uma senha. Porém, já se implementa em algumas redes uma autenticação denominada "dois fatores". Além de uma senha o usuário precisa ter algo em seu poder como, por exemplo, um cartão magnético. Isso reduz a probabilidade de uma pessoa ter sucesso ao tentar se passar por outra pessoa. Além disso, a autenticação dos usuários permite ao sistema enxergar se a origem dos dados faz parte da comunidade que pode exercer acesso à rede.

3.3 PRIVACIDADE e INTEGRIDADE

A idéia da criptografia é embaralhar os dados e associar a esses dados uma chave. Apenas quem possuir essa chave poderá desembaralhar esses dados. Com isso garante-se a **privacidade** dos dados, isto é, garante-se que ninguém mexerá nos dados que trafegam protegidos, assim como também se garante a **integridade** dos dados, ou seja, que ninguém irá alterar as informações contidas no pacote.

4. ETAPAS DA CONEXÃO

4.1 AUTENTICAÇÃO

Primeiramente é feita a autenticação entre os dois pontos. Essa autenticação permite ao sistema enxergar se a origem dos dados faz parte da comunidade que pode exercer acesso à rede.

4.2 AUTORIZAÇÃO

Em seguida, o servidor VPN verifica quais serviços que o usuário tem permissão para acessar, monitorando assim o subseqüente tráfego de dados. Este passo é chamado de autorização e visa negar acesso a um usuário que não está autorizado a acessar a rede como um todo, ou simplesmente restringir o acesso de usuários.

4.3 CRIPTOGRAFIA E ENCAPSULAMENTO

Uma vez formado o túnel seu ponto de partida adiciona cabeçalhos especiais aos pacotes que serão endereçados ao outro ponto do túnel, para em seguida, criptografar e encapsular toda a informação na forma de novos pacotes IPs. Os cabeçalhos internos permitirão então a autenticação da informação e serão capazes de detectar qualquer alteração dos dados enviados.

5. TIPOS

Existem vários tipos de implementação de VPN's. Cada implementação apresenta especificações próprias, assim como características que devem ter uma atenção especial na hora de implementar.

Entre os tipos de VPN, destacam-se três principais:

5.1 INTRANET VPN

Em uma Intranet VPN, que pode, por exemplo, facilitar a comunicação entre departamentos de uma empresa, um dos requisitos básicos a considerar é a necessidade de uma criptografia rápida para não sobrecarregar a rede (que deve ser rápida).

Outro requisito essencial é a confiabilidade a fim de garantir a prioridade de aplicações críticas, como por exemplo, sistemas financeiros e banco de dados. E por último, é importante a facilidade de gerenciamento, já que numa rede interna tem-se constantes mudanças de usuários, seus direitos, etc.

5.2 ACESSO REMOTO VPN

Uma VPN de acesso remoto conecta uma empresa a empregados que estejam distantes fisicamente da rede. Neste caso, torna-se necessário um software cliente de acesso remoto.

Quanto aos requisitos básicos, o mais importante é o tratamento de QoS (Quality of Service), isto porque, geralmente quando se acessa remotamente de um laptop você está limitado à velocidade do modem. Outro item, não menos importante, é uma autenticação rápida e eficiente, que garanta a identidade do usuário remoto. E ainda tem-se a necessidade de um gerenciamento centralizado desta rede, já que ao mesmo tempo pode-se ter muitos usuários remotos logados, o que torna necessário que todas as informações sobre os usuários, para efeitos de autenticação, por exemplo, estejam centralizadas num único lugar.

5.3 EXTRANET VPN

Extranet VPN é implementada para conectar uma empresa à seus sócios, fornecedores, clientes entre outros. Para isso é necessária uma

solução aberta, para garantir a interoperabilidade com as várias soluções que as empresas envolvidas possam ter em suas redes privadas. Outro ponto essencial é o controle de tráfego, que minimiza os efeitos dos gargalos existentes em possíveis nós entre as redes e, ainda, garante uma resposta rápida para aplicações críticas.

6. SOLUÇÕES

6.1 HARDWARE ESPECÍFICO

O encapsulamento aumenta o tamanho dos pacotes, consequentemente, os roteadores poderão achar que os pacotes estão grandes e fragmentá-los, degradando assim a performance da rede. A fragmentação de pacotes e a criptografia poderão reduzir a performance de sistemas discados a níveis inaceitáveis, mas a compressão de dados poderá solucionar este problema. No entanto, a combinação de compressão com encapsulamento irá requerer um poder computacional mais robusto para atender às necessidades de segurança. Por isso, uma VPN implementada através de hardware, graças a seu poder computacional, irá alcançar uma melhor performance. Este tipo de implementação também fornece uma melhor segurança - física e lógica - para a rede, além de permitir um volume de tráfego maior. A desvantagem desta implementação é um custo mais alto e o uso de hardware especializado.

6.2 APENAS SOFTWARE

Já uma VPN implementada através de software terá critérios menos rígidos de segurança e um custo menor, mas se encaixa perfeitamente para atender as necessidades de conexão, onde o volume de dados trafegados é pequeno e onde não exista necessidade de grandes requisitos de segurança.

6.3 SOFTWARE AUXILIADO POR HARDWARE

Quanto a performance de VPN's implementadas por software assistido por hardware, esta dependerá da performance dos equipamentos aos quais o software está relacionado.

A tabela a seguir resume os aspectos a serem considerados para a escolha do tipo de solução para a implementação de uma VPN.

Solução	Apenas software	Software assistido por Hardware	Hardware especializado
Performance	baixa	média-baixa	alta
Segurança	plataforma fisicamente e logicamente insegura	plataforma fisicamente e logicamente insegura	fisicamente e logicamente seguro
Produtos	Firewalls, Softwares de VPNS	Cartões de criptografia para roteadores, PCs (Personal Communication Services)	Hardware especializado

7. PROTOCOLOS

7.1 PPTP (Point-to-Point Tunneling Protocol)

O protocolo PPTP é um modelo "voluntário" de tunelamento, uma vez que permite que o próprio sistema do usuário final configure e estabeleça conexões sem a intermediação do provedor de acesso, fazendo o encapsulamento dos pacotes em um túnel fim a fim.

O protocolo PPTP é capaz de lidar com outros tipos de pacotes, além do IP, como o IPX (Internet Packet Exchange) e o NetBEUI (Network Basic Input/Output System Extended User Interface), pois é um protocolo baseado na camada 2 do modelo OSI (enlace).

7.2 GRE (Generic Routing Protocol)

Túneis GRE são geralmente configurados entre roteadores fonte e roteadores destino (pacotes ponto-a-ponto). Os pacotes designados para serem enviados através do túnel (já encapsulados com um cabeçalho de um protocolo como, por exemplo, o IP) são encapsulados por um novo cabeçalho (cabeçalho GRE) e colocados no túnel com o endereço de destino do final do túnel. Ao chegar a este final os pacotes são desencapsulados (retira-se o cabeçalho GRE) e continuarão seu caminho para o destino determinado pelo cabeçalho original.

7.3 L2F (Layer-2 Forwarding)

O LF2 foi um dos primeiros protocolos utilizados por VPN’s. Ele foi projetado como um protocolo de tunelamento entre usuários remotos e corporações e é capaz de transportar pacotes por diferentes meios como FRAME RELAY ou ATM, além de suportar mais de uma conexão.

O L2F também permite tratar de outros pacotes diferentes de IP, como o IPX e o NetBEUI por ser um protocolo baseado na camada 2 do modelo OSI.

7.4 L2TP (Layer 2 Tunneling Protocol)

Este protocolo foi criado pela IETF (Internet Engennering Task Force) para resolver as falhas do PPTP e do L2F. Ele utiliza os mesmo conceitos do L2F e assim como este foi desenvolvido para transportar pacotes por diferentes meios, como X.25, frame-relay e ATM e também é capaz de tratar outros pacotes diferentes do IP, como o IPX e o NetBEUI (protocolo baseado na camada 2 do modelo OSI).

O L2TP é, porém, um modelo de tunelamento "compulsório", ou seja, criado pelo provedor de acesso, não permitindo ao usuário qualquer participação na formação do túnel.

7.5 IPSec (Internet protocol security protocol)

O protocolo IPSec foi desenvolvido também pela IETF (Internet Engennering Task Force). Ele permite ao usuário ou ao gateway seguro autenticar e/ou criptografar cada pacote IP e por isso é considerado uma ótima solução para ambientes IP, mas ao contrário dos protocolos PPTP e L2TP, o IPSec não foi desenvolvido para suportar outros pacotes além do IP.

8. CONCLUSÃO

Em resumo, podemos dizer que as VPN's constituem-se numa alternativa segura para a transmissão de dados através de redes públicas ou privadas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança, possibilitando eliminar os links dedicados de longa distância e de altos custos na conexão de WANs.

Porém, a decisão de implementar, ou não, redes privadas virtuais, requer uma análise criteriosa dos requisitos, principalmente, aqueles relacionados a segurança, custos, qualidade de serviço e facilidade de uso que variam de acordo com o negócio de cada organização.

9. REFERÊNCIAS

- ✓ http://www.isaserver.org/shinder/tutorials/gateway_to_gateway_part1.htm
- ✓ http://www.cisco.com/go/vpn-7100/
- ✓ http://www.abusar.org.br/
- ✓ http://www.teltecnetworks.com.br/vpn.htm