E00 – Março de 1999

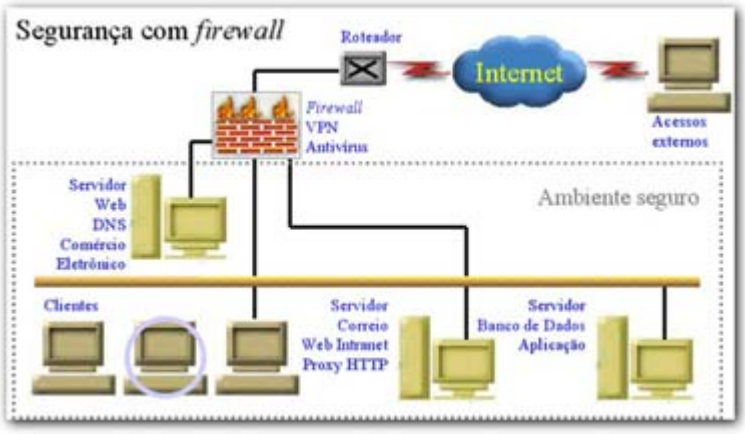
# O que tem a ver Camisa de Vênus com Firewall Pessoal ?

Neste exato momento, milhares de computadores estão conectados a uma enorme malha de comunicação, espalhados por todo o planeta e trocando informações incessantemente. Muitas delas sem valor. Mas uma boa quantidade potencialmente poderosa, circulando livremente. Pois bem, cheguei onde queria: A segurança.

Um dos grandes problemas no ambiente de rede sempre foi a segurança de acesso aos dados. Com a expansão da Internet, da Intranet e do acesso remoto, os sistemas passaram a ficar vulneráveis aos ataques externos.

**Vulnerabilidades**
Existem alguns pontos nevrálgicos e passíveis de invasão em uma conexão entre computadores. Em primeiro lugar, vem o servidor, que está sendo acessado e que disponibiliza alguma informação aos computadores clientes. Em seguida, devemos lembrar do meio por onde trafegam as informações e, por fim, do computador cliente.

**Cenário Corporativo**




Exemplo corporativo com ambiente Intranet e acesso à Internet.

O cenário mostra o papel do *firewall* tradicional protegendo a rede interna de acessos externos indevidos. O meio de transporte é representado pelo raio por onde devem trafegar informações devidamente criptografadas, e por fim, vê-se um computador cliente com um círculo. Este é o foco do *firewall* pessoal, o computador em rede na sua individualidade.

**Soluções**
A criptografia veio solucionar o problema da segurança de dados durante a trajetória até o computador de destino. Algoritmos matemáticos complexos são utilizados para codificar a informação, de forma a permitir somente que o verdadeiro destinatário possa compreendê-las. Existem diversos algoritmos criptográficos, cada um com sua peculiaridade, complexidade e nível de segurança.

**Algoritmo criptográfico IDEA 128-bit**

"IDEA - (International Data Encryption Algorithm - Algoritmo de criptografia de dados internacionais) é o nome do novo algoritmo de criptografia de dados em bloco aplicável universalmente, que permite a proteção eficaz de dados transmitidos e armazenados contra acesso não autorizado de terceiros. Os critérios fundamentais para o desenvolvimento do

> IDEA foram os requisitos mais elevados de segurança e implementação facilitada de hardware e de software. O algoritmo, que fica disponível de imediato, é predestinado para ser utilizado em grande número de aplicativos comerciais."
>
> Adotado pela Módulo Security Solutions S.A.

O *firewall*, tradicional na interligação entre LANs e WANs e na proteção de acesso aos servidores com a separação da rede interna da externa, vem cumprindo – quando bem configurado - seu papel inicial. Mas se o acesso externo está em parte equacionado por esta solução, não se pode dizer o mesmo dos acessos a dados externos pelos usuários da rede interna. Chegamos então à outra ponta da conexão.

Em virtude da complexidade dos sistemas, do crescente poder de ação das informações contidas nos computadores (exemplo: senhas para transações financeiras) e do potencial de destruição e invasão dos atuais "vírus" como os Trojans (Cavalo de Tróia), há uma exigência maior de níveis de segurança e controle de acessos diferentes, o que mostra a tendência do *firewall* em se tornar uma solução mais fragmentada para proteger cada área da empresa de forma específica ou até mesmo cada estação da rede. Surge então o conceito de *firewall* pessoal.

> **Trojan Horses**
>
> "Cavalo de Tróia em português, são programas que ocultam os seus reais objetivos sob uma camuflagem de programas úteis ou inofensivos. Destruição de dados e quebra de segurança de sistemas são apenas alguns exemplos do que trojan horses costumam visar.
>
> Uma vez instalado na máquina da vítima, o trojan permite que o cliente (atacante) tenha perigosas permissões como: executar e fechar programas, apagar, renomear, criar e copiar arquivos, tocar sons, encerrar a conexão, travar o teclado e o micro, abrir e fechar a porta do cdrom, capturar as senhas do usuário e até mesmo capturar telas e todas as teclas pressionadas."
>
> Cartilha Trojans Horses
> Marcos Sêmola

O ***firewall* pessoal** veio trazer também um conceito de *firewall* ao inverso. Quando utilizado nas estações de uma rede corporativa, dá-se a elas o controle e a privacidade sobre as informações armazenadas (exemplo: senhas e documentos) e aos administradores da rede, o controle dos acessos realizados por elas à informações externas. Portanto, com uma só ferramenta, garantimos a privacidade dos dados da corporação e controlamos os acessos externos evitando a possível queda de produtividade por mau uso (exemplo: acesso à sites pornográficos).

Sem esquecer o usuário doméstico com seu acesso discado ao provedor – que pode conter uma estrutura semelhante à do cenário acima – fica fácil perceber que ele também pode se beneficiar com o uso do *firewall* pessoal no que se refere à proteção das informações.

**Nova tecnologia**
Uma opção de segurança cada vez mais popular é o conceito de VPNs (Virtual Private Networks), que incorporam a criptografia entre as extremidades de uma conexão (criptografia fim a fim). Dessa forma, é possível ter uma conexão segura entre dois computadores distintos. Atualmente, essa tecnologia está sendo implementada em *firewall*, permitindo que as organizações criem "túneis" seguros ao longo da Internet.

No entanto, cada vez mais fornecedores estão anunciando a utilização de recursos de VPNs fim a fim, permitindo que as organizações criem um *firewall* "pessoal". Este recurso possibilitará controles de acesso

mais eficientes e maior proteção para a confidencialidade de cada conexão, mostrando se superior ao *firewall* tradicional.

**Conselho**
Com o foco no bem mais valioso a ser protegido: **a informação**, costumo dizer que o melhor comportamento é se proteger individualmente. Aproveito para fazer uma analogia ao vírus HIV, cujo cenário inicial da doença gerava conselhos do tipo: "evite manter relações com pessoas do grupo de risco, assim você estará seguro".

Como na vida real, os conceitos no meio digital mudam, portanto, o conselho de não se executar programas vindos de pessoas desconhecidas está totalmente furado. Muitas vezes, pessoas conhecidas e confiáveis estão sendo vítimas também de um programa de computador contaminado. Assim, tanto na vida real quanto na virtual, a palavra de ordem é: proteja-se. E...que tal com um *firewall* pessoal ?