



Ensaio e Ciências

UNIVERSIDADE PARA O DESENVOLVIMENTO DO ESTADO E DA REGIÃO DO PANTANA

editora@uniderp.br

ISSN: 1517-9141

BRASIL

2000

Luiz Alberto de Oliveira Azevedo

ESQUEMA DE SEGURANÇA PARA TRÁFEGO DE DADOS NA INTERNET

Ensaio e Ciência, Abril, año/vol. 4, número 001

Universidade para o Desenvolvimento do Estado e da Região do Pantanal

Campo Grande, Brasil

pp.59-74



ESQUEMA DE SEGURANÇA PARA TRÁFEGO DE DADOS NA INTERNET

Luiz Alberto de Oliveira Azevedo

Professor Mestre, CCPD, Universidade para o Desenvolvimento do Estado e da Região do
Pantanal.

Rua Antônio Carlos Martins, 73, Vila Planalto. CEP 79009-090. Campo Grande - MS.
luizalberto.azevedo@bol.com.br

RESUMO

Esta é uma pesquisa introdutória que mostra como disponibilizar informações seguras na Internet, que está se tornando cada vez mais presente em nossas vidas. São elencados os problemas enfrentados para a disponibilização de dados para efetuar o comércio eletrônico na Internet, os tipos de ataques e mecanismos que estão sendo implementados para solucionar tais problemas. O desenvolvimento de mecanismos mais seguros, fará com que a utilização da Internet como meio de comunicação e comércio eletrônico se torne indispensáveis no dia-a-dia em nossas vidas.

Palavras-chave:

Firewal,
protocolos de segurança,
criptografia,
comércio eletrônico.

ABSTRACT

This is an introductory research that indicates how to provide safe information through the Internet, since the Internet is getting more and more present in our lives. This paper lists the problems faced when making data available to perform electronic commerce through the Internet, the types of attacks and the mechanisms that are being implemented to solve such problems. The development of safer mechanisms will make the usage of the Internet as a mean of communication and electronic commerce essential in our daily lives.

Key-words:

Firewall,
secure protocols,
encryption,
electronic business.

1 INTRODUÇÃO

A segurança no acesso às redes corporativas sempre foi tema de longas discussões, para o ambiente informatizado das empresas tem criado diversas opções para diferentes tipos de crimes por computador. Na década de 70, o principal criminoso era técnico de informática; na década de 80, tanto técnicos de informática quanto os funcionários de instituições financeiras eram os principais criminosos. Atualmente, qualquer pessoa pode praticar crimes por computador, pelas inúmeras oportunidades que as novas tecnologias e os novos ambientes organizacionais proporcionam.

Com o advento da globalização do mercado mundial, surgiu a necessidade de as empresas disponibilizarem suas redes corporativas no mercado global, já que essa disponibilização faz com que as empresas se tornem mais competitivas.

Com o surgimento da Internet e sua posterior utilização para fins comerciais, as empresas começaram a correr para disponibilizar seus dados corporativos através dessa rede, pois ela atinge grande parte do mercado mundial (estima-se que mais de 247 países estão conectados à Internet).

Com o intuito de disponibilizar as redes corporativas através da Internet, os empreendedores que desejam aproveitar as oportunidades criadas devem tratar o assunto utilizando a razão; implementar garantias e controles de segurança adequados para evitar que os *hackers* possam acessar as redes sem autorização.

As empresas disponibilizam *home pages* na Internet para publicar anúncios e para divulgar ofertas de produtos, uma vez que, com um investimento relativamente pequeno, elas conseguem atingir um grande número de pessoas. Isto significa que a Internet é predominantemente utilizada como veículo para comunicação simples, marketing e propaganda, mas os recursos de comércio eletrônico estão crescendo muito rapidamente.

O problema que as empresas enfrentam atualmente é como efetuar transações comerciais utilizando ferramentas disponíveis para a Internet, já

que os protocolos básicos de comunicação (TCP/IP) dessa rede não são seguros e a preocupação com segurança virou uma paranóia, ao ponto de impedir empresas sérias de usarem a Internet, pois alega-se que os *hackers* estão por toda a rede tentando se infiltrar e piratear informações, criando dessa forma um medo generalizado.

A atual tecnologia de encriptação e de “filtragem” está bem desenvolvida, o que dificulta extremamente a ação de pessoas não autorizadas (*hackers*) que tentam acessar as redes corporativas através da Internet. O que tem ocorrido é a quebra de segurança pelo mau uso dos sistemas de segurança, por exemplo: sistemas de proteção de alta qualidade são burlados, pois pessoas utilizam senha que é o nome do filho ou a data de aniversário. Mas as principais vulnerabilidades encontradas costumam ser relativas a erros, acidentes ou desconhecimento dos usuários autorizados que, inadvertidamente, alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência ou mesmo contaminam seus arquivos e programas com vírus.

O desenvolvimento do comércio eletrônico, o intercâmbio de dados financeiros ou o trabalho cooperado entre empresas, já pode ser implementado, pois existem recursos disponíveis. Quanto vale uma informação na empresa? Esta é a primeira dúvida que surge quando se inicia um processo de segurança, de forma a considerar o impacto no negócio nos casos de possíveis perdas e, com isto, dimensionar adequadamente os investimentos necessários para a proteção e controle. Deve-se, então, fazer uma análise técnica (custos, treinamentos) e uma análise da situação (o que esperar da rede, os perigos, quais recursos utilizar para impedir acessos indevidos). Segurança a qualquer custo é um extremo freqüente que deve ser evitado, pois segurança é sempre relativa.

A utilização dos firewalls (“muros de fogo”) impedem que pessoas não autorizadas acessem as redes corporativas quando essas estão conectadas à Internet. A escolha em utilizar ferramentas já existentes ou implementar as próprias, depende do nível de segurança que se deseja obter.

A Internet pode oferecer uma grande economia de custos e excelentes ganhos de produtividade, além de oportunidades significativas para a geração de receita. Mas para obter esses benefícios, as empresas devem expor suas redes a ameaças à segurança potencialmente sérias. As ameaças podem vir tanto da Internet quanto da rede interna, em sua maioria. Mas em nosso caso, iremos tratar dos problemas vindos através da Internet e possíveis soluções.

2 CONEXÃO À INTERNET

A Internet oferece muitos serviços que podem ser disponibilizados na rede corporativa da empresa. O primeiro destes serviços, pode ser o correio eletrônico. A rede corporativa é conectada à Internet de modo que os funcionários possam fazer o seguinte: trocar mensagens de correio eletrônico com seus parceiros nos negócios, pesquisar informações sobre produtos, obter assistência técnica, participar em discussões setoriais ou participar de qualquer uma das inúmeras oportunidades disponíveis (listas de discussões, comunicações em tempo real, recuperação de informações, transferência de arquivos, terminal virtual, anúncios publicitários, serviços bancários e financeiros).

Fazer negócio na Internet é atualmente o ponto crucial de muitas organizações, por isso aproveitar o potencial da Internet é uma tarefa que deveria envolver todas as áreas da organização. Recursos e mercados virtuais, juntamente com canais de distribuição global, traduzem-se em infinitas novas possibilidades comerciais. A Internet funciona como um “possibilitador” de negócios, facilitando objetivos comerciais chave.

A tecnologia da Internet teve um êxito tão grande que as empresas estão começando a utilizá-la internamente. A mesma tecnologia que é usada para anunciar produtos e compartilhar informações mundiais está sendo empregada para disseminar informações internas de uma empresa. As empresas estão começando a reprojeter seus processos comerciais com base na tecnologia da Internet.

Os serviços bancários eletrônicos estão tendo um imenso crescimento potencial através da Internet e as instituições financeiras já oferecem serviços financeiros eletrônicos, entretanto o desafio enfrentado é como oferecer uma matriz de serviços que se beneficie do tamanho e da abrangência da Internet e de sua enorme base de usuários, uma vez que a implementação de transações bancárias através da Internet está revolucionando os serviços bancários.

2.1 PROBLEMAS DE PADRONIZAÇÃO

A falta de padrões técnicos é um dos grandes problemas enfrentados para a disponibilização dos dados na Internet. A Internet Engineering Task Force (IETF) que é uma associação aberta, é quem define as diretrizes de padronizações para a Internet. Mas, à medida que a Internet passou a ser mais comercial, o papel da IETF tornou-se mais indefinido. Cada vez mais os fornecedores estão propondo sua própria versão de padrão sem passar pelo processo tradicional da IETF. Os fornecedores que criam padrões nem sempre fazem isso por motivos altruístas - colocar no mercado um produto baseado em um padrão patenteado traz significativo lucro. Dentre os exemplos desse tipo de comportamento estão as batalhas entre os protocolos de comunicação segura - Secure Hypertext Transfer Protocol (SHTTP), Secure Sockets Layer (SSL), Private Communications Technology (PCT), Secure Transaction Technology (STT), Secure Electronic Payment Protocol (SEPP) e Secure Electronic Transaction (SET).

As propriedades intrínsecas da Internet representam a principal fonte de sua vulnerabilidade a falhas e ataques. A Internet conecta centenas de redes regionais e redes de provedores de serviços regionais espalhados pelo mundo inteiro. Seu enorme tamanho afeta sua confiabilidade, pois, inicialmente, quando projetada, o objetivo era permitir diversas possibilidades de conectividade entre as partes que estivessem interagindo. Portanto, a interoperabilidade, e não a segurança, foi enfatizada. Característica essa que foi aceita por ser inicialmente uma rede de pesquisa (Bernstein, 1996).

Os protocolos que definem as regras para interoperabilidade entre os equipamentos conectados na Internet são deficientes e geram muitos problemas de segurança. Muitos protocolos são usados juntamente com outros e agregados em “conjunto de protocolos”. O conjunto de protocolos mais comum na Internet é o Transport Control Protocol/Internet Protocol (TCP-IP). Infelizmente, os protocolos TCP-IP têm características inatas que os tornam vulneráveis a ataques. O principal problema do TCP-IP é sua inabilidade para confirmar a identidade dos participantes em um processo de comunicação. Qualquer computador pode criar mensagens que parecem ter uma outra origem. Devido a uma característica de um dos protocolos TCP-IP básicos, uma determinada máquina pode monitorar todo o tráfego de uma rede a que está conectada, independentemente de seu destino.

O sistema operacional UNIX é muito utilizado atualmente com o TCP-IP. Mas como o UNIX foi originalmente projetado para compartilhar informações sem qualquer restrição, a maior parte dos sistemas UNIX apresentam algum tipo de ponto vulnerável.

2.2 TIPOS DE ATAQUES PELA INTERNET

Vejamos alguns tipos de ataques pela Internet:

a) **Baseados em senhas** - este tipo de ataque é aquele em que o intruso informa o nome do usuário e a senha repetidas vezes. Essa estratégia de força bruta tem sucesso em muitos tipos de UNIX que não bloqueiam tentativas de *login* após um número de insucessos.

b) **Exploram o acesso confiável** - vários sistemas operacionais têm mecanismos de acesso confiável projetados para facilitar o acesso a outros sistemas e domínios. Esses sistemas permitem o uso de arquivos de *host* confiáveis formados por nomes de *hosts* ou endereços a partir dos quais um usuário pode obter acesso sem utilizar uma senha. O intruso que adivinhar o nome de uma máquina ou de uma combinação *host/nome* do usuário poderá acessar uma máquina que permita acesso confiável.

c) **Spoofing do IP** - este tipo de ataque envolve o fornecimento de

informações falsas sobre uma pessoa ou sobre a identidade de um *host* para obter acesso não-autorizado a sistemas e/ou aos sistemas que eles fornecem. O *spoofing* identifica as máquinas de destino (endereços e os números de seqüência que as duas máquinas utilizam ao estabelecerem a conexão) e interfere na forma como um cliente e um servidor estabelecem uma conexão, já que para o estabelecimento da conexão TCP-IP as máquinas trocam informações entre si. Apesar de ser uma estratégia desajeitada e entediante, existem ferramentas capazes de executar um ataque de *spoofing* em menos de 20 segundos.

d) **Seqüestro de sessão** - aqui o intruso procura por uma conexão já existente entre dois *hosts* e tenta ter o controle sobre ela. Após obter o controle sobre a máquina através da qual a conexão é estabelecida, ou de outra máquina da mesma LAN, o intruso monitora a conexão que está sendo efetuada. Dessa forma, ele consegue determinar os números de seqüência utilizados por ambos os lados da conexão. Após ver a conexão, o intruso pode gerar um tráfego que parece vir de um dos dois *hosts*, simplesmente “roubando” a sessão de uma das duas pessoas envolvidas no processo.

e) **Rastreamento de Pacote** - como na Internet os pacotes são transmitidos de todas as partes da rede à medida que trafegam dos pontos de origem para os de destino, as redes de meios físicos compartilhados impõem um tipo especial de risco de segurança, pois os pacotes podem ser interceptados em qualquer ponto dessas redes. O rastreamento da rede é uma das mais sérias ameaças a empresas, mesmo que suas redes não se conectem à Internet.

2.3 SEGURANÇA DA CONEXÃO À INTERNET

O primeiro passo a ser tomado, é reforçar o perímetro da rede. Mas, para que isso possa ocorrer, devem-se identificar dois domínios separados (interno e externo) e seus perímetros. Após essas definições, o próximo passo a ser tomado será a identificação dos pontos de entrada na rede: modems de discagem, conexões dedicadas com parceiros que são conectados a

Internet e microcomputadores que ficam ligados em *stand-by* para receberem mensagens de fax.

As políticas de segurança de rede deverão incluir procedimentos para o controle do tráfego entre todos esses pontos de entrada. Até mesmo a defesa de perímetro mais rígida pode se mostrar inútil, diante do ataque de um modem de discagem sem controle que está conectado à rede.

Para fazer uma conexão à Internet, deve-se considerar inúmeros fatores: o tipo de conexão à Internet mais adequado para a empresa, o esquema de endereçamento que a rede utilizará e outros serviços oferecidos pelo provedor Internet.

É possível falsificar um endereço de um site, mas há formas de dificultar enormemente isso, utilizando, por exemplo, a certificação digital e o software de segurança fora do browser. Isso foi usado pela Receita Federal na entrega do Imposto de Renda via Internet. A certificação digital acontece, quando um cartório eletrônico garante a autenticidade e há um terceiro que serve para dar autenticidade à operação. Tal técnica aumenta o nível de segurança algumas vezes, pois é como multiplicar o poder de segurança na Internet (Nery, 1997).

A linguagem Java não é exceção quando se fala de segurança, pois ela também apresenta problemas. Quando as novas versões de browsers são atualizadas, fica-se seguro contra ataques conhecidos, entretanto, não contra ataques que não foram descobertos ainda. Então, para aumentar o nível de segurança, deve-se sempre atualizar os browsers para as últimas versões.

2.3.1 Criptografia

A técnica de criptografia, são funções matemáticas e métodos computacionais (algoritmo) capazes de tornar indecifráveis os dados que trafegam por um meio que não está livre de ataques intrusos, tornando-os legíveis (descriptografia), apenas quando atingem seu destino. A grande força desse esquema é a chave de criptografia, pois os algoritmos utilizados, em

sua maioria, são públicos. É justamente sobre o tamanho da chave que se fala, quando são mencionados algoritmos de criptografia, por exemplo, 40, 56, 128 bits. Assim, uma chave de 40 bits poderia assumir 2^{40} valores (1.099.511.627.776 tentativas). Então, quanto maior a chave, mais seguro o esquema de criptografia (Mourão & Zabeu, 1998).

Os mecanismos que usam a mesma chave para criptografar e descriptografar são chamados de simétricos ou de chave secreta. Em geral, são mais rápidos, mas têm o problema de como combinar a chave, já que a mesma deve ser trocada periodicamente. Uma solução é a chamada criptografia assimétrica que usa chaves diferentes para criptografar e descriptografar. Cada parte envolvida na comunicação possui um par de chaves, uma pública e outra privada, de modo que, por questões matemáticas, apenas a chave privada será capaz de descriptografar a mensagem criptografada com a chave pública.

O uso apenas da criptografia de chave secreta na troca de mensagens entre um grande grupo de correspondentes previamente desconhecidos sobre uma rede pública é impraticável, já que cada par de usuários precisaria de uma chave distinta compartilhada em um canal de segurança fora da Internet para estabelecer uma comunicação segura. Já o método de chave pública assimétrica poderia trocar mensagens seguramente em uma rede pública, pois cada um cria um par de chaves, transmite ao outro um componente de seu par de chaves, designado chave pública, e mantém secreto o outro componente, designado chave privada. As chaves públicas podem ser transmitidas sobre uma rede insegura, porque mensagens criptografadas com chave pública podem apenas ser descriptografadas usando a chave privada correspondente.

O problema do método de criptografia assimétrico é que as chaves são da ordem de milhar, já as chaves do outro método são da ordem de dezenas e centenas e, também, os algoritmos são mais complexos, tornando-os mais lentos no processo de codificação e decodificação.

Segundo Specialski (1997), uma forma de contornar o segundo

problema é usar métodos assimétricos para codificar uma chave de método simétrico, e usar o método simétrico para codificar o texto.

2.3.2 SSL (Secure Sockets Layer)

O SSL é um protocolo que fornece uma camada de segurança de dados entre protocolos de aplicação (tal como HTTP, SMTP, FTP) e o TCP/IP, sendo por isso classificado como um protocolo de segurança de transporte usado para garantir a segurança de servidores e clientes Web (Netscape Navigator e MS Internet Explorer) e outras aplicações Internet.

Socket é uma Application Program Interface (API) de comunicação inter processos, que tem como base a camada de transporte. Uma das API's de comunicação mais conhecidas para sistemas Unix são os *Berkeley Sockets* e para os sistemas Windows, os *Winsockets*. Para se estabelecer uma comunicação entre um par de *sockets*, o *socket* cliente precisa estabelecer uma conexão com o *socket* servidor que se encontra em uma porta bem conhecida. Desta forma, uma associação é feita e teoricamente o SSL pode, de maneira transparente tornar seguro qualquer protocolo de aplicação baseado no TCP rodando em qualquer porta (Specialski, 1997).

A política de segurança do protocolo SSL oferece serviços como autenticação dos participantes, confidencialidade e integridade dos dados, garantidos através dos mecanismos de criptografia, assinatura digital e gerenciamento de certificados. Esse protocolo utiliza criptografia de chave secreta (simétrica) e criptografia de chave pública (assimétrica). Este conjunto de protocolos pode ser visto na figura 1.

O SSL foi baseado em um algoritmo de criptografia chamado Rivest Shamir Adleman (RSA) que combina os métodos de criptografia simétrica e criptografia assimétrica, processo esse chamado de envelope digital, em que o tamanho das chaves não é fixo e pode variar entre seis níveis de segurança.

Por causa das leis de exportação americanas para chaves criptográficas, apenas nos Estados Unidos e Canadá pode-se utilizar

qualquer um dos níveis de segurança; nos demais países apenas, os níveis de segurança com tamanho de chave de até 128 bits podem ser utilizados. Depois de sofrer uma pressão por parte das empresas desenvolvedoras de software que alegavam estar perdendo mercado internacional, o governo norte-americano liberou o uso de criptografia com chave de 128 bits para instituições financeiras fora do território dos Estados Unidos. Com esse novo esquema, uma chave só poderia ser quebrada em cerca de 10^{23} anos.

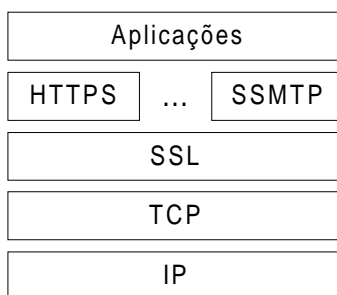


Figura 1 - Arquitetura SSL

2.3.3 Secure Electronic Transaction Protocol (SET)

O SET é um protocolo que fornece uma camada de segurança em nível de aplicação. Segundo (Specialski, 1997), dois aspectos devem ser considerados na escolha do local onde serão implementados os mecanismos de segurança:

a) Implementar nos níveis inferiores pode implicar modificações no código do sistema operacional, onde estão implementados os protocolos de nível de transporte.

b) A implementação de aplicações seguras fica muito mais complexa, se a pilha de protocolos não possuir mecanismos de segurança.

O SET é um protocolo específico para aplicações de pagamento eletrônico na Internet, situado na arquitetura Internet acima do protocolo em nível de aplicação HTTP e dos protocolos TCP/IP, figura 2. O SET está sendo publicado por duas das maiores empresas de cartões de crédito do mundo, a VISA Internacional e a MasterCard como especificações abertas e é objeto

de estudo do IETF. Estas aplicações estão disponíveis para serem aplicadas a qualquer serviço de pagamento com cartão bancário na Internet e podem ser usadas por desenvolvedores de software. A assistência no desenvolvimento destas especificações tem sido fornecida por companhias como a IBM, GTE, Microsoft, Netscape, Terisa e Verisign.

A política de segurança do protocolo SET oferece serviços como autenticação dos participantes, confidencialidade e integridade dos dados, garantidos através dos mecanismos de criptografia, assinatura digital e gerenciamento de certificados como no protocolo SSL. No entanto, a utilização deste serviço é mais rígida, ou seja, não é configurável como no protocolo SSL.

O SET também utiliza o algoritmo RSA, mas com chaves de tamanho fixo. Dependendo de sua funcionalidade, cada chave pode possuir de 512 até 2048 bits.

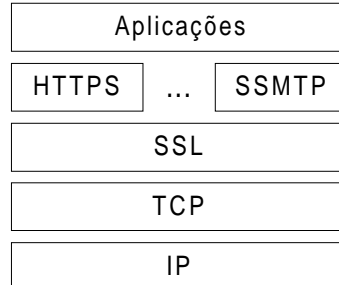


Figura 2 - Arquitetura SET

2.3.4 Firewalls

Firewalls são espécies de barreiras de proteção constituídas de um conjunto de hardware e software muito utilizados para aumentar a segurança de redes ligadas à Internet. Uma ferramenta extremamente avançada que oferece segurança na rede, o *firewall* representa uma eficiente estratégia para implementar a política de acesso à Internet em uma organização. Os *firewalls* podem oferecer proteção contra ataques a protocolos ou aplicações individuais e contra ataques de *spoofing* e têm relativa flexibilidade de configuração, ou

seja, oferecem várias restrições para diferentes tipos de tráfego.

Uma das vantagens do *firewall*, é que ele oferece um único ponto de controle para a segurança em uma rede. Portanto, tendem a ser os principais alvos para ataques externos. Por outro lado, eles apresentam um único ponto para uma falha na segurança. Se o *firewall* for comprometido, o perímetro seguro será violado e um intruso terá acesso livre a toda a rede da corporação. Por essa razão, os melhores *firewalls* são compostos de vários “blocos”, cada um dos quais oferece algum reforço e aumenta a segurança do sistema *firewall* (Bernstein et al., 1996).

Os *firewalls* são compostos de filtros e *gateways* e podem ser classificados em três categorias principais:

a) Os *filtros de pacotes* são baseados na tecnologia “store-and-forward” dos roteadores. Um roteador ou um *host* receberá um pacote em uma interface, comparará as informações em seu cabeçalho com um conjunto de filtros e então decidirá se deixa o pacote passar, se o abandona inteiramente ou se o rejeita. A sintaxe do filtro identifica o tráfego pelos endereços IP de origem e de destino, e portas TCP e UDP para tomar as decisões de controle de acesso. O administrador elabora uma lista de máquinas e serviços que estão autorizados a transmitir datagramas nos possíveis sentidos de transmissão, que é então usada para filtrar os datagramas IP que tentam atravessar o *firewall*. A filtragem de pacotes é vulnerável a adulteração de endereços IP e não fornece uma granularidade muito fina de controle de acesso, já que o acesso é controlado com base nas máquinas de origem e de destino dos datagramas.

b) Os *gateways de circuitos* atuam como intermediários de conexões TCP, funcionando como TCP modificado. Para transmitir dados, o usuário origem conecta-se a uma porta TCP no *gateway*, que por sua vez, conecta-se ao usuário destino usando outra conexão TCP. Para que seja estabelecido um circuito, o usuário de origem deve fazer uma solicitação para o *gateway* no *firewall*, passando como parâmetros a máquina e o serviço de destino. O *gateway* então estabelece ou não o circuito.

c) Os *gateways* de aplicação são *firewalls* que atuam no nível de aplicação e utilizam implementações especiais das aplicações desenvolvidas especificamente para funcionar de forma segura. Pela grande flexibilidade desta abordagem, ela é a que pode fornecer maior grau de proteção. Uma aplicação FTP pode ser modificada para limitar a transferência de arquivos da rede interna para a externa ou ainda, um *gateway* FTP pode ser programado para restringir as operações de transferência a arquivos fisicamente localizados em um único *host* de acesso externo (*bastion host*).

Dependendo dos tipos de serviços que se deseja oferecer, a localização do servidor Web pode variar. Se colocar o servidor da Internet dentro de um *firewall*, talvez não seja possível ser oferecidos serviços avançados, como RealAudio, pois o *firewall* pode ser configurado para bloquear esse serviço. Pois se o *firewall* permitir a passagem desses pacotes, torna-se difícil descobrir os intrusos (Bernstein et al., 1996).

De um modo geral, como visto na figura 3, existem três localizações possíveis para o servidor: dentro da rede corporativa, na zona desmilitarizada de um sistema de *firewall* ou em algum outro lugar na Internet (com terceiros).

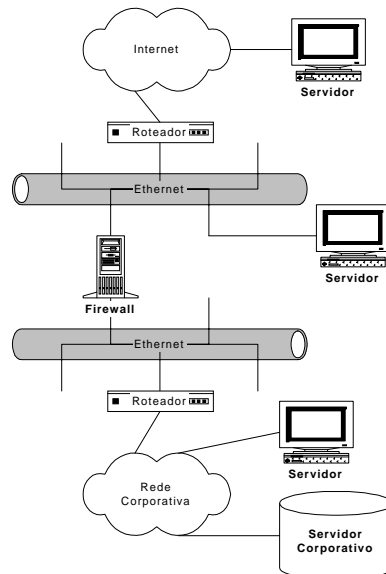


Figura 3 - Localizações do servidor Web

3 CONCLUSÃO

Como muitos dos aspectos vulneráveis da Internet são inerentes ao conjunto de protocolos TCP/IP, que são a base da comunicação na Internet, concluímos que esse ambiente é difícil de ser controlado precisamente e, quando pode ser controlado, o custo em termos de recursos necessários é geralmente alto. As providências específicas que as empresas deverão tomar para conter ataques à Internet deverão ser baseadas nos objetivos das transações e dos serviços a serem oferecidos.

Como resultado desta pesquisa, verificou-se que descrever software seguro é mesmo muito difícil, mas já existem ferramentas e mecanismos seguros - como a criptografia com chave de 128 bits, os protocolos de segurança, SET e SSL, e os *firewalls* - para que se possa disponibilizar redes corporativas e efetuar pagamentos eletronicamente na Internet. Certamente, o comércio eletrônico progredirá mais rapidamente e será uma das mais importantes maneiras de fazer negócio no futuro.

Fica claro que segurança na Internet é um assunto vasto, para o qual não existem soluções universais, apenas soluções relativas a um determinado contexto, mas, cada vez mais, a Internet se tornará presente e indispensável em nossas vidas.

REFERÊNCIAS BIBLIOGRÁFICAS

- BERNSTEIN, Terry et al. **Segurança na Internet**. Tradução do original Internet Security for Business, Rio de Janeiro: Campus, 1997.
- MOURÃO, Liane; ZABEU, Sheila Barcelos. Internet Banking. **PC World**, São Paulo, n. 70, p. 4-12, abr. 1998.
- NERY, Fernando. De Carro Blindado na Rede. **Jornal do Brasil**, São Paulo, 8 dez. 1997. Disponível em: <<http://www.modulo.com.br/noticia>>.
- SPECIALSKI, Elizabeth. **Segurança na Internet**. Disponível em: <<http://pedrao.inf.ufsc.br/cec3604/97mar/segura/segint.htm>>.