TECNOLOGIAS QUE VISAM GARANTIR A SEGURANÇA DE INFORMAÇÕES NA INTERNET

Dennys Peixoto Noronha*.

RESUMO: Este trabalho apresenta as principais tecnologias utilizadas para se garantir segurança às informações que trafegam na Internet, tais como a Criptografia e o uso de Firewall, sem deixar de comentar sobre os cuidados mínimos quanto ao aspecto de senhas e conteúdo das informações a serem manipuladas.

No tocante ao aspecto de Criptografia os tópicos abordados são os tipos de criptografia existentes, a diferença entre eles, como criptografar dados e como são utilizadas as informações criptografadas. Na parte de Firewall são abordados os conceitos desta tecnologia assim como a sua utilização na Internet

1. INTRODUÇÃO

Um dos maiores problemas que a industria de computadores enfrenta na atualidade é o da segurança de informações e este problema se agrava quando os computadores estão ligados a uma Rede Mundial que é o caso da Internet.

Com base nesta informação, este artigo tem como finalidade apresentar os principais mecanismos de segurança em Redes de Computadores dando ênfase à Criptografia e ao uso de Firewall, oferecendo então possibilidades para garantir a segurança de informações ao se utilizar a Internet.

2. CUIDADOS BÁSICOS

Ao utilizar um computador ligado em Rede, deve-se tomar inicialmente os cuidados básicos sobre segurança das informações manipuladas.

Para se conectar a uma rede global, como é o caso da Internet, torna-se indispensável uma senha de acesso que deve ser guardada em um local seguro, de preferência na memória do usuário. De que adianta ter uma senha fixada no gabinete de trabalho ? Nada. E uma senha com o data de seu nascimento ? Seria o mais óbvio possível. As senhas devem possuir combinações indecifráveis, de preferência utilizando letras e números em sua formação, dificultando desta forma o trabalho de quem pretende descobri-las.

Ao manipular informações confidenciais via rede, "todo cuidado é pouco", pois o que não falta são Hackers querendo violar informações confidenciais; sendo assim, estas informações devem ser criptografadas (vide seção 4), de tal maneira que possam trafegar com segurança pela rede. Mandar a mensagem em vários pacotes, também ajuda a dificultar a ação de um violador e assim surgem mais uma série de medidas para se obter a segurança de informações via Internet.

Fazer "Backup", guardar arquivos importantes, em locais seguros, também é uma medida de segurança importantíssima, pois garante a existência dos documentos importantes mesmo quando acontece alguma tragédia no computador que guarda tais documentos.

Existem vários mecanismos de segurança em ambientes de rede como a Assinatura Digital, o Controle de Acesso, a Integridade dos Dados, a Autenticação, a Autenticidade, o tráfego Extra, o Controle de Direcionamento e em especial para este a artigo, a Criptografia e o Firewall que são apresentados nos próximos tópicos. A seguir é apresentada uma tabela (**Tab. 2.1**) onde são comparados os diferentes serviços utilizados em rede com os mecanismos de segurança que estes serviços possuem.

*Graduado em Tecnólogo em Processamento de Dados em 1995 pela Universidade da Amazônia e Especialista em redes de Computadores em 1996 pela Universidade Federal do Pará. Atualmente exerce as funções de Professor Assistente I no Departamento de Informática da UNAMA e Professor Adjunto do CESEP. Áreas de Interesse envolvem Redes de Computadores, Inteligência Artificial, Robótica e Engenharia de Software. Departamento de Informática – UNAMA – Universidade da Amazônia. Av. Alcindo Cacela, 287 CEP 66060-000 Belém-PA. Telefone: (091) 210-3086. **dennys@supridad.com.br**

Serviços	Mecanismos							
	Criptografia	Assinatura Digital	Controle de Acesso	Integridade de Dados	Intercâmbio de Autenticação	Mascaramento de Tráfego	Controle de Roteamento	Compromisso de terceiros
Autenticação de Parceiro	✓	✓			✓			
Autenticação da Origem	✓	✓						
Controle de Acesso			✓					
Confidencialidade com conexão	✓						✓	
Confidencialidade sem conexão	✓						✓	
Confidencialidade em campos selecionados	✓							
Confidencialidade do Fluxo de Tráfego	✓					✓	✓	
Integridade com conexão e com recuperação	✓			✓				
Integridade com conexão sem recuperação	✓			✓				
Integridade sem conexão	✓	✓		✓				
Impedimento de Rejeição da Origem		✓		✓				✓
Impedimento de Rejeição do Destino		✓		✓				✓

Tab. 2.1

3. SERVIÇOS, MECANISMOS E AMEAÇAS

Neste tópico são apresentados os serviços, mecanismos e ameaças encontrados na Internet assim como os princípios orientados para a escolha dos mecanismos adotados.

Os mecanismos de segurança devem ser escaláveis, tendo capacidade e potencial para acompanhar o crescimento da comunidade da Internet.

Os mecanismos devem ter sua segurança apoiada na tecnologia que os suporta, por exemplo, em algoritmos e protocolos que sejam seguros, ou seja, que não possuam falhas intrínsecas.

Os mecanismos de segurança não devem restringir a topologia da rede.

Mecanismos de segurança que não sejam sujeitos às restrições de controle de exportação ou patentes devem ter preferência.

É sabido que muitos mecanismos de segurança necessitam de uma infra-estrutura de apoio, o gerenciamento dessa infra-estrutura pode ser tão ou mais complexo que a implementação do mecanismo; sendo assim, deve-se dar preferência a tecnologias de segurança que possam compartilhar uma infra-estrutura de segurança comum.

Algoritmos de criptografia selecionanados para padronização na Internet devem ser amplamente conhecidos, devendo ser dada preferência aos que tiverem sido exaustivamente testados.

3.1 Internet x Serviços de Segurança

A partir de agora são apresentadas algumas aplicações que a Internet disponibiliza com seus respectivos padrões de segurança, ou seja, seus serviços e mecanismos . Ao final deste tópico, após a leitura das aplicações, é apresentado um quadro geral que relaciona as aplicações na Internet com os serviços de segurança.

3.1.1 Correio Eletrônico

Na atualidade, o aplicativo de Correio Eletrônico que a Internet oferece aos seus usuários tem como função uma simples troca de mensagens de textos com a disponibilidade de "atachar" outros arquivos ou figuras em seu envio.

A aplicação de Correio Eletrônico está crescendo muito, paralelamente com o serviço total que a Internet oferece. A troca de mensagens entre usuários vem se tornando um fato comum e já há um grande declínio no tradicional correio via carteiro que em um futuro breve utilizará em baixa escala a troca de cartas e em alta a de pacotes e encomendas como é o caso de uma revista por assinatura que não pode vir pela Internet, é lógico.

É com base neste crescente aumento de tráfego no Correio Eletrônico que deve-se pensar muito na segurança que engloba esse aplicativo.

Os serviços de segurança necessários para o Correio Eletrônico na Internet deverão incluir confidencialidade e integridade em transmissões sem conexão, autenticação da origem das mensagens, e impedimento de rejeição pelo destinatário ou remetente.

Com estes serviços, o Correio Eletrônico torna-se uma ferramenta de profunda utilidade e de grande interesse a qualquer tipo de pessoa independente de classe, profissão ou nível de conhecimento.

3.1.2 Serviço de Diretório

Na Internet existem duas espécies de serviços de diretório que são o DNS - Domain Name Server e o X.500 que possui serviços de segurança bem definidos que são incorporados em seu protocolo através de mecanismos de segurança.

Enquanto o X.500 possui essas definições de segurança, o DNS não consta de nenhuma definição explícita e consequentemente não possui mecanismos de segurança.

Se porventura o DNS for acrescido de recursos de segurança, esses seriam semelhantes ao do X.500 que por sua vez possui os seguintes requisitos: autenticação da origem de dados, controle de integridade em transmissões sem transmissão para proteger as consultas e respostas ao diretório, controle de acesso para permitir o armazenamento dos dados com a garantia de que os dados só possam ser alterados por pessoas previamente autorizadas ou administradores do sistema. Todos estes serviços de segurança são oferecidos pelo X.500 através de mecanismos implementados no protocolo de aplicação.

Além desses serviços ainda podem ser oferecidos outros mecanismos de segurança para garantir a confidencialidade dos dados no diretório e este pode ser fornecido nos níveis de rede ou transporte.

3.1.3 Gerenciamento de Redes

O protocolo de gerenciamento de redes na Internet é o SNMP - Simple Network Management Protocol. Após recentes melhoramentos no SNMP , apareceram com a versão dois do protocolo, um conjunto de requisitos de segurança.

Os serviços de segurança que passaram a ser oferecidos foram: confidencialidade e integridade acoplado com uma proteção contra reenvio postergado ou seja, o replay, na transmissão de datagramas, autenticação da origem de dados e controle de acesso baseado na identidade. Estes serviços são empregados na proteção contra violações no intercâmbio de informações de gerenciamento, e para proteger os objetos gerenciados contra tentativas de manipulação não autorizada.

O nível de aplicação abrange todos os serviços implementados no SNMP incluindo um esquema de distribuição de chaves simétricas.

É interessante que o gerenciamento de redes seja realizado através da versão ampliada do SNMP que já conta com os serviços de segurança ou então uma versão segura do CMIP - Common Management Information Protocol, caso esta venha a ser desenvolvida.

3.1.4 Terminais Virtuais e Transferência de Arquivos

Esta aplicação, Terminal Virtual, da Internet, é oferecida pelo protocolo Telnet que é construído com base em três idéias principais que são o conceito de terminal virtual de rede, o princípio de negociação de opções e o tratamento equivalente de terminais e processos..

Já a Transferência de Arquivos, é suportada pelo protocolo FTP - File Transfer Protocol que é baseado na conexão ente um cliente e um servidor, onde o cliente é o módulo FTP que solicita o acesso a arquivos remotos e o servidor é o módulo FTP que disponibiliza o acessos a esses arquivos que para o servidor, são arquivos locais. Esses arquivos podem ser do tipo texto ou binário, ambos são permissíveis na realização desse protocolo.

Tanto para o Telnet quanto para o FTP, os requisitos de segurança devem incluir integridade e confidencialidade em conexões, autenticação de parceiros e controle de acesso baseado em identidade.

Os serviços de segurança nestes protocolos podem ser implementados diretamente por mecanismos nos próprios protocolos de aplicação, ou através do uso de mecanismos de camadas inferiores como o transporte e rede por exemplo. O TLSP - Transport Layer Security Protocol pode atender a esses requisitos e é um bom exemplo do caso.

Os mecanismos são implementados no nível de aplicação ou inferiores que representam uma modificação nos códigos dos sistemas operacionais onde são implementados os protocolos do nível de rede e de transporte.

3.1.5 Servidores de Arquivos

Os servidores são implementados por sistemas com o NFS - Network File System pertencente a Sun e o AFS - Andrew File System que desta forma se distingue dos protocolos de transferências de arquivos por fornecer um serviço mais aprimorado como por exemplo o acesso randômico a partes de um arquivo.

Os serviços de segurança existentes nesta aplicação são a integridade e a confidencialidade no intercâmbio de datagramas, a autenticação de parceiros e o controle de acesso que desta feita é baseado em identidade.

Os serviços de confidencialidade e integridade podem ser fornecidos por protocolos do nível de rede e de transporte.

Não pode existir uma recomendação para os servidores de arquivos na arquitetura de segurança na Internet visto que ainda não foram definidos padrões para protocolos de segurança que suportam essa aplicação.

3.1.6 Roteamento

O roteamento na Internet é efetuado através de protocolos como o BGP , o EGP e o OSPF.

Todos estes protocolos possuem serviços de segurança semelhantes que são: autenticação de parceiros e integridade no intercâmbio de datagramas carregando informações de roteamento. Caso haja a necessidade de haver uma proteção das informações sobre a topologia de redes, torna-se-ia necessário garantir a confidencialidade dos datagramas.

A grande maioria destes serviços tem a possibilidade de ser fornecidos com a utilização de mecanismos genéricos da camada de rede ou, em uma outra hipótese, podendo também ser construídos especificamente para os protocolos de roteamento.

A diversidade existente entre os protocolos utilizados no roteamento deixa claro os benefícios de se utilizar mecanismos de segurança comuns fornecidos na camada de rede.

O serviço de confidencialidade pode ser realizado no nível físico ou no nível de rede. No nível físico é observado que este serviço pode ser fornecido aos usuários por intermédio de um roteador[1] diretamente. Todavia quando

1 - **Roteador** ↳ São sistemas de processamento de transações, no qual as transações são mensagens de telecomunicações em vez de ordem de compra ou saques em caixas eletrônicos. Permitem conectar redes locais de tipos diferentes, ou interligar redes locais a redes de longa distância

pretende-se garantir tal confidencialidade utilizando pacotes que atravessam vários roteadores em seu caminho, já é necessário a utilização do serviço de confidencialidade através do nível de rede.

Agora que já foram analisados todos os aplicativos com seus respectivos serviços de segurança de forma isolada, na tabela abaixo **(Tab. 3.1)** o leitor encontra um quadro com uma visão geral mostrando um relacionamento entre as aplicações da Internet e os serviços de segurança para que se possa ter uma visão rápida e prática de tudo que foi visto nesse tópico.

	Aplicações						
Serviços	Correio Eletrônico	Serviço de Diretório	Gerencia-mento	Terminal Virtual	Transferência de Arquivos	Servidores de Arquivos	Rotea-mento
Autenticação de Parceiro				👍	👍	👍	👍
Autenticação da Origem	👍	👍	👍				
Controle de Acesso		👍	👍	👍	👍	👍	
Confidencialidade com conexão				👍	👍		
Confidencialidade sem conexão	👍	👍	👍			👍	👍
Confidencialidade em campos selecionados							
Confidencialidade do Fluxo de Tráfego							👍
Integridade com conexão e com recuperação				👍	👍		
Integridade com conexão sem recuperação							
Integridade sem conexão	👍	👍	👍			👍	👍
Impedimento de Rejeição da Origem	👍						
Impedimento de Rejeição do Destino	👍						

Tab. 3.1

4. CRIPTOGRAFIA

A criptografia surgiu da necessidade de se enviar informações confidenciais através de meios de comunicação não confiáveis; ou seja um meio de comunicação em que não se pode prever a observação de outras pessoas indesejadas, como a de um intruso passivo, ou na pior das hipóteses a não apenas observação e sim alteração de dados flutuantes por pessoas indesejadas, pelos chamados intrusos ativos.

A criptografia funciona através de um método que na teoria é muito simples. Utiliza-se o auxílio de um algoritmo para que seja modificado o texto da mensagem original, que é a mensagem a ser transmitida. As informações são enviadas de maneira criptografada com o objetivo de chegar ao destino previsto pois assim, são indecifráveis para leigos, ou pessoas que não conheçam o método utilizado na encriptação dos dados. Quando a mensagem chega ao destino, ocorre o processo inverso ao da criptografia, ou seja, um algoritmo, semelhante ao usado para criptografar a mensagem, é requerido e colocado sobre a mesma, porém com função inversa, fazendo com que o amontoado de caracteres ilegíveis voltem a ser o texto normal.

Em resumo, criptografia é a metodologia de codificação de dados através de algoritmos padrões de segurança (chaves), atribuindo à informação um modo ininteligível a terceiros.

A criptografia objetiva assegurar a

Confidencialidade dos dados manipulados, ou seja que nenhuma pessoa não autorizada veja os dados que estão sendo enviados. Objetiva também a observação da Autenticação dos dados tanto em sua assinatura como em sua integridade, ou seja para que o dado quando chegue a seu destino ainda esteja intacto e certo de que a pessoa que o enviou é a especificada na mensagem.

Existem três padrões de segurança mundialmente conhecidos que são:

- DES - Data Encryption Standard Algorithm
- DSS - Digital Standard Signature
- RSA - Rivest, Shamir, Adelman

Ao final deste tópico, será apresentado um pequeno algoritmo de encriptação escrito em linguagem "Fortran-Like", para que o leitor possa entender como funciona, na prática, a elaboração de um destes programas.

É válido lembrar que existem "n" estilos de algoritmos para encriptação de dados em várias linguagens de programação.

Existem ainda três tipos de criptografia distintas que dependem do uso dos padrões DES, DSS e RSA, que são: a Criptografia Simétrica, a Criptografia Assimétrica e a Criptografia Híbrida.

A seguir são apresentados três exèmplos gráficos representando a funcionalidade de cada um dos três tipos de criptografia.

4.1 Criptografia Simétrica

A criptografia simétrica trabalha com apenas uma chave de criptografia, que é ao mesmo tempo responsável por criptografar e decriptografar os dados conforme apresentado na **Fig. 4.1** a seguir.

Fig. 4.1

4.2 Criptografia Assimétrica

A criptografia assimétrica por sua vez, trabalha com duas chaves de criptografia: uma chamada pública que é responsável por criptografar as mensagens e outra chamada privada que tem a finalidade de decriptografar os dados (mensagens) conforme apresentado na **Fig. 4.2** abaixo.

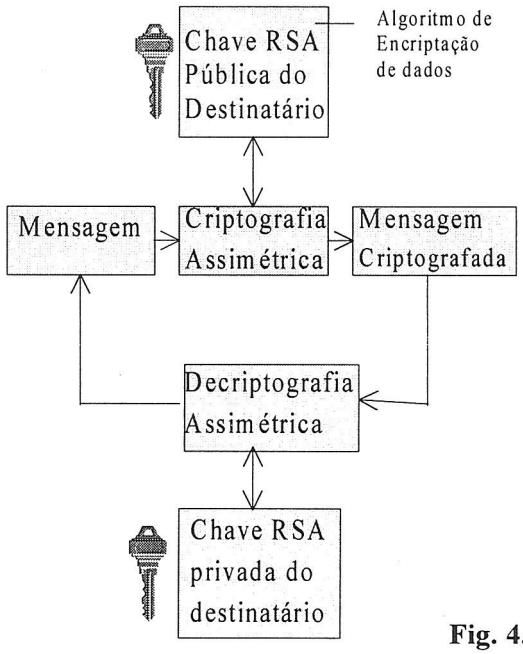


Fig. 4.2

4.3 Criptografia Híbrida

A criptografia híbrida mescla os conceitos das duas anteriores pois trabalha com os dois tipos de chave: DES e RSA conforme apresentado na **Fig. 4.3** abaixo.

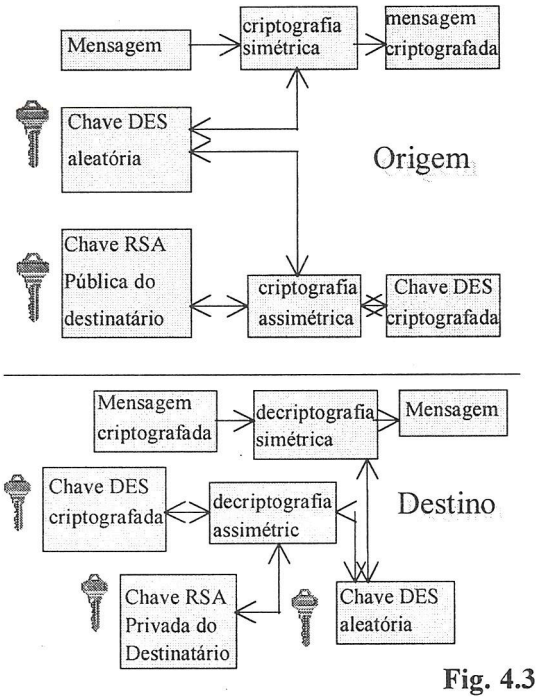


Fig. 4.3

4.4 Algoritmo de Criptografia

Neste tópico é apresentado um pequeno algoritmo, em Fortran-Like, dividido em três rotinas.

A rotina preliminar, que declara e armazena todas as letras, números e caracteres especiais em uma variável ALPH.

A rotina de encriptação, com o auxílio do conteúdo da variável ALPH, indexa através de substituições randômicas por meio de um laço, os textos e mensagens que são criptografados.

A rotina de decriptação de dados por sua vez, utilizando o mesmo laço e código randômicas, executa o processo inverso da substituição de caracteres decriptando a mensagem e convertendo para a forma original.

Preliminary

```
DCL (TEXT, MESS, ALPH) CHAR(48);
ALPH = 'ABCDEFGHIJKLMNOPQRST
UVWXYZ123 4567890-.,)(:;"=+??';
S=23518967;
```

Enciphering Routine

```
GET EDIT (TEXT)(A(48));
DO H=1 TO 48;
   N=INDEX(ALPH,SUBSTR(TEXT,K,1));
   CALL RANDOM (S,R); J=R*48;
   L=J+N; IF L>48 THEN L=L-48;
   SUBSTR(MESS,K,1)=SUBSTR(ALPH,L,1)'
END;
```

Deciphering Routine

```
DO K=1 TO 48;
  L=INDEX(ALPH,SUBSTR(MESS,K,1));
  CALL RANDOM (S,R); J=R*48;
  N=L-J; IF N<1 THEN N=N+48;
  SUBSTR(TEXT,K,1)=SUBSTR(ALPH,N,1);
END;
PUT EDIT (TEXT)(A(48));
```

5. FIREWALL

Neste tópico é abordado um recurso de segurança muito eficiente e interessante que é o uso de Firewall. Este mecanismo, como o próprio nome tenta indicar, é uma espécie de "parede contra fogo".

Firewall pode ter vários conceitos e para entendermos o que é Firewall, é necessário que seja entendido preliminarmente o que não é Firewall.

- Não é simplesmente um hardware como um roteador, etc.
- Não é simplesmente um software.
- Não é um sistema simples (hardware + software).

Visto o que **não** é Firewall, agora podemos saber o que **é** Firewall e o que ele representa à nível de Segurança em Redes de Computadores.

Para melhor entendimento, serão colocados a seguir alguns conceitos sobre esse tão importante aplicativo de segurança que é o Firewall:

- É uma barreira de proteção.
- É uma coleção de componentes. colocadas entre duas redes onde estas duas redes tem a necessidade de possuir as seguintes propriedades:
  → Todo tráfego de dentro para fora da rede, e vice-versa, passa pelo Firewall.
  → Só o tráfego autorizado pela política de segurança pode atravessar o Firewall.
  → O Firewall deve ser a prova de violações.
- É uma abordagem que implementa uma política de segurança a fim de definir serviços e acessos considerados permitidos.

Durante o decorrer deste tópico serão abordadas as idéias básicas sobre Firewall sendo apresentada a sua implementação na Internet, as vantagens e desvantagens que existem no uso dessa ferramenta, as duas principais categorias que são os filtros de pacotes e os Gateways[2] onde podemos dividir especificamente em Dual-Homed Gateway que trata de um modo bidirecional e o próprio Packet-Filtred Gateway que é o Filtro de Pacotes.

Ao final do tópico serão apresentados, através de figuras, alguns exemplos de como funciona a tecnologia Firewall.

5.1 Idéia Básica

Um Firewall pode ser visto como um monitor de referências para uma rede, sendo que seu principal objetivo é garantir a integridade dos recursos ligados a rede. Todavia, a centralização tem como consequência uma administração bem mais cuidadosa por parte das pessoas envolvidas com a administração dos sistemas das máquinas que implementam o Firewall.

Uma análise isolada das máquinas especificadas teria como objetivo central uma configuração para a otimização do desempenho e a facilidade de utilização porém, quando tratamos de Firewall, a conversa muda de rumo e o objetivo principal no sistema passa a ser a segurança.

Uma visão geral de um Firewall pode ser representada na **Fig. 5.1** abaixo:

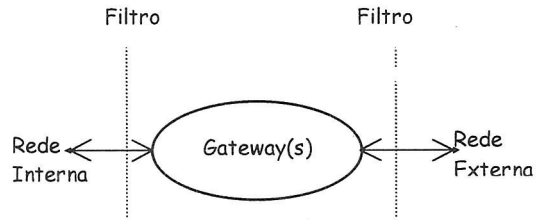


Fig. 5.1

5.2 Vantagens e Desvantagens

Ao se implantar um Firewall, colocar um Gateway com uma configuração especial entre uma rede local e o resto do mundo, temos algumas vantagens e desvantagens.

Como principal vantagem que pode ser observada, têm-se que todos os esforços de segurança podem ser concentrados em uma única máquina.

Sobre as duas categorias principais de Firewall: Dual-Homed Gateway e Packet-Filtred Gateway, são abordados a seguir, o que elas oferecem citando dessa forma, suas vantagens e desvantagens.

5.2.1 Dual-Homed Gateway

Nesta categoria podem ser citados os seguintes aspectos em relação a utilização de Firewall:

- Estação possuindo duas placas de rede.
- Uso Específico versus Uso Geral.
- Relativa "transparência" para o usuário dependendo da política de segurança.
- Limitação causada pela disponibilidade de "proxies" para cada um dos serviços.
- Mudança nos softwares da rede local para

2 - **Gateway** ↳ São extensões dos roteadores. São usados para processar traduções e interpretações mais complexas. A diferença entre roteadores e gateways está no fato de que os roteadores processam as mensagens sem conhecer o seu conteúdo e sua aplicação, funcionando como "guardas de trânsito" que desviam o tráfego de uma rede para a outra. Os gateways fazem a transferência de dados de uma aplicação para a outra através da rede somente depois de identificar a natureza das mensagens explicando assim a sua utilização em Firewalls.

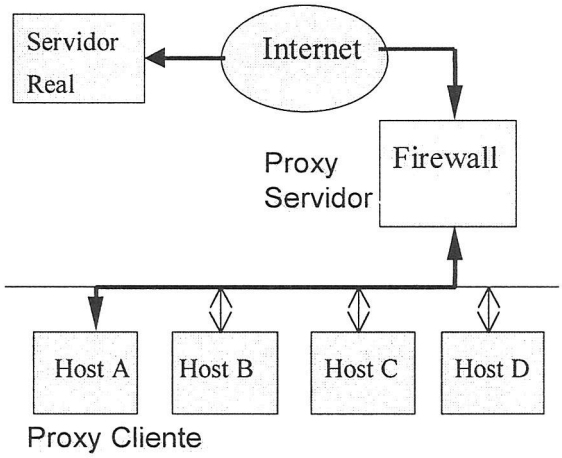
trabalhar corretamente com os "proxies".

- Os "proxies" são executados no gateway.

→Filtragem das mensagens que saem da rede local

→Filtragem das mensagens que chegam na rede local

- Proxy pode ser otimizado. (fazer um FTP para um determinado nó da rede)



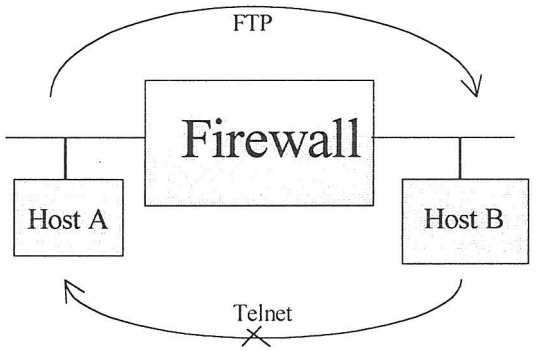
Como principais desvantagens desta categoria podem ser citadas as seguintes:

- Disponibilidade de Proxy Servidores
- Diferentes Proxies Servidores para distintos serviços.
- Geralmente é preciso modificação na aplicação cliente.
- Não protege contra protocolos "inseguros".

5.2.2 Packet-Filtred Gateway

Nesta categoria podem ser citados os seguintes aspectos em relação a utilização de Firewall:

- A utilização de um roteador para fazer a filtragem do tráfego que vem de fora da rede local.
- Apenas as mensagens endereçadas ao gateway são aceitas.
- O mundo não vê a rede local, mas a rede local vê o mundo.
- Pacotes que saem da rede local podem ser proibidos.
- Flexibilidade para permitir que certas máquinas e serviços possam ser acessadas diretamente.
- Geralmente são o de menor custo e indicados para o uso geral.
- Baseados em endereços Fonte/Destino e Port-Number (serviço).
- Transparente para o Usuário.
- Tudo que não é expressamente permitido, é considerado proibido.



Fonte	Destino	Serviço	Ação
Host A	Host B	FTP	Permite
Host B	Host A	Telnet	Proibe

Como principais desvantagens nesta categoria podem ser citadas as seguintes:

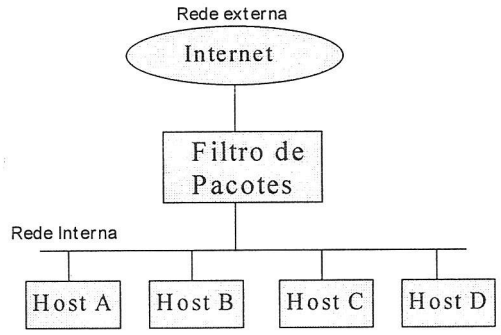
- Ferramentas para filtro de pacotes não são perfeitas.
- Algumas políticas de segurança não podem fazer uso de filtro de pacotes.

A seguir são apresentados 3 Layouts de redes utilizando a tecnologia Firewall.

No primeiro gráfico, são utilizadas duas redes: uma rede interna e uma externa (Internet). Para que uma rede possa ser conectada a outra, é obrigatória a passagem por uma espécie de roteador (filtro de pacotes), que direciona as

informações que trafegam nas redes.

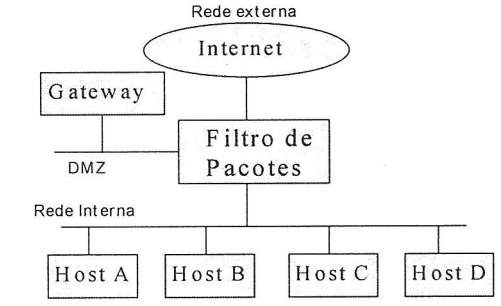
Layout 1



- Duas redes.
- Duas Interfaces para administrar.
- Um dispositivo para filtro (router).
- Sem Proxy.
- Alguns recursos para log (depende do dispositivo)

No segundo gráfico, apresentado a seguir, são administradas três interfaces incluindo um gateway, que ligado ao filtro de pacotes, seleciona as informações que podem ou não trafegar entre as redes elevando assim o custo de criação e administração das mesmas.

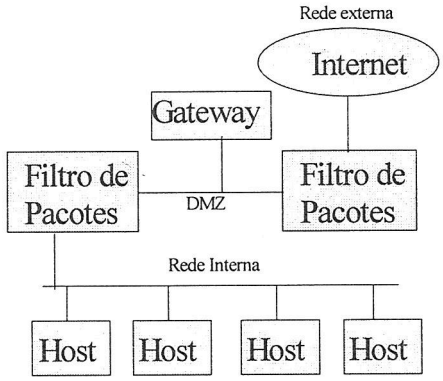
Layout 2



- DMZ (De-Militarized Zone).
- Três interfaces para administrar.
- Proxy.
- Custo Maior.

No terceiro gráfico, apresentado a seguir, são administradas quatro interfaces incluindo um gateway, que é ligado a dois filtros de pacotes, um diretamente com a rede externa e outro com a rede interna. Utilizando três redes e direcionando e selecionando as informações que podem ou não trafegar entre as mesmas, este tipo de layout possui um custo muito elevado na criação e principalmente na administração de ambas.

Layout 3



- Três Redes.
- Quatro interfaces para administrar.
- Proxy.
- Custo mais elevado.

6. CONSIDERAÇÕES FINAIS

Cada dia que passa, com o aumento de informações trocadas via Internet, a segurança cresce em importância para os internautas. Assim como a televisão já foi um luxo de poucos em outrora e hoje é considerada um aparelho normal dentro de casa, a Internet também já está deixando de ser um luxo e se firmando como uma utilidade de fundamental importância para todos, e em um futuro, não tão longínquo, deve se tornar comum, tal qual a televisão, à grande maioria da população global, principalmente as consideradas de "Primeiro Mundo".

Normalmente as primeiras tentativas em se implantar uma medida de segurança maior em

uma rede resultam em sistemas mais pobres ou seja, especificamente críticos se as máquinas são de pequeno porte. Porém com o aperfeiçoamento que envolve a utilização e a modificação das primitivas de serviços oferecidos pelo software padrão em uso, a segurança vai se aprimorando principalmente quando são utilizados recursos de segurança do próprio software para a melhora de performance da rede.

Em se tratando de troca de informações via rede é sempre bom mantermos uma espécie de filtro para saber o que deve e o que não deve ser trocado. Se houver necessidade de sigilo nos dados deve-se ter então um modo de deixar esses dados serem lidos apenas pelo destinatário.

Em se tratando de segurança física, deve-se haver uma preocupação maior com a localidade dos equipamentos, a seleção detalhada dos usuários que podem usar os computadores. Um controle isolado dos servidores. Uma limitação de acessos aos usuários. Deve-se realizar auditorias com frequência para desta maneira resolver problemas existentes ou que possam vir a existir. Seguindo a risca todas estas "dicas", a probabilidade de se ter uma rede segura é muito maior, e na atualidade *vital* para qualquer rede de computadores

7. BIBLIOGRAFIA CONSULTADA

[Soares1995] Luis Fernando G. Soares. Redes de Computadores. Das Lans, Mans e Wans às Redes ATM. Ed. Campus.

[Tanenbaum1994] Andrew S. Tanenbaum. Redes de Computadores. Ed. Campus 1994

[Stang1994] David J. Stang and Sylvia Moon. Segredos de Segurança em Rede. Ed. Idg - Books 1994.

[Katzan1992] Harry Katzan Jr . Segurança de Dados em Computação. Ed. Campus 1992.

[Amoroso1994]Edward Amoroso. Fundamentals of Computer Security Technology. AT&T Bell Laboratories 1994.

[Denning1983] Dorothi Elisabeth Robling Denning. Crhiptografy and Data Security. Ed. Purdue University 1983.

[Wood1994] Michael B. Wood. Introdução à Se gurança do Computador. Ed. Campus 1994

[Swicky1993] Ed Sawicky – Segurança: Seu guia para o uso seguro em redes locais. Ed. Campus 1993.

[Giff82] Grifford, D.K. Criptographic Sealing for information Security and Autentication. Ed. Comm. Acm 1982.

[Neum78] Neumann, P.G., Computer Security Evoluction Vol 47, Ed. AFIPS Press, Montvale, N.J.1978.

[Rush81] Rushby, D.M., Design and Verification of Secure Systems, Proc. 8th Symp. On oper System princ. Acm oper. Vol 15. 1981

[Martin1984] James Martin. Security. Accuaracy and Privacy in Computer Systems.

[Tassel1990] Dennis Van Tassel. Computer Security Management