

Uma Proposta de Rede Segura

Elias Carvalho Silva

Orientador: *Márcio Luiz Bunte de Carvalho*

Abstract

Com o número crescente de empresas, entidades governamentais e instituições conectando-se à *Internet*, a importância de mecanismos de segurança para proteger tais redes privadas tem crescido proporcionalmente. A topologia da rede deve ser planejada, os mecanismos de autenticação devem ser revistos e, principalmente, os usuários devem estar conscientes da importância e das necessidades destas mudanças.

Este trabalho tem o objetivo de propor e implantar uma política de segurança voltada para um ambiente acadêmico, mais especificamente o do nosso departamento, bem como um mecanismo de *Firewall* para limitar e controlar o acesso externo às nossas instalações.

1. Introdução

A *Internet* é uma coleção de redes que utilizam um protocolo comum para comunicação. Muitas organizações estão se conectando à *Internet* para tirar vantagem dos serviços e recursos disponíveis. Instituições, empresas e organizações, privadas ou governamentais, estão utilizando ou considerando o acesso para uma variedade de aplicações, notadamente troca de correio eletrônico, disponibilização de informações, atividades de pesquisa e negócios. Muitas organizações estão conectando suas redes locais internas à *Internet* de forma que cada estação de trabalho possa ter acesso direto aos recursos disponíveis.

Esta conectividade pode oferecer vantagens enormes, entretanto a segurança destas redes internas deve ser dada a devida importância durante o planejamento ou reconfiguração de uma conexão. Existem riscos significantes associados à *Internet* que muito frequentemente não são óbvios para os usuários, tanto para os iniciantes como para os experientes. Em particular, atividades provenientes de acesso não autorizado bem como vulnerabilidades que podem proporcionar tal tipo de acesso são amplamente divulgadas pela própria *Internet*. Tais atividades são extremamente difíceis de prever, muitas vezes difíceis de descobrir e os danos causados são, em sua maioria, irreversíveis. Muitas organizações já perderam produtividade, tempo e dinheiro por conta de tais invasões. Além disso, algumas organizações já tiveram suas reputações marcadas como resultado de atividades de ataque que partiram de suas instalações.

Neste trabalho propomos uma topologia de *Firewall* para limitar e controlar o acesso externo às nossas instalações, bem como especificar uma política de segurança a ser aplicada internamente de forma a garantir a privacidade de nossos usuários e assegurar a boa reputação do nosso Departamento.

2. Dificuldades e Motivações

A principal dificuldade relacionada a segurança em redes de computadores é a conscientização dos usuários com relação à necessidade de se adotar uma política de segurança. O problema pode ser caracterizado em uma única frase:

Todo investimento em segurança reflete-se, de alguma forma, em perda de flexibilidade ou facilidade de utilização dos recursos.

Principalmente em um ambiente acadêmico, onde as redes de computadores são vistas como ferramental para as atividades de pesquisa desenvolvidas na instituição. Mesmo em outros ambientes, é difícil aceitar que aquilo que está dificultando a sua rotina é, de fato, útil e necessário.

Como citado por [Ranum, 1993], existem dois paradigmas de segurança que podem ser adotados:

- *Tudo o que não é expressamente permitido é proibido:* Neste paradigma, somente os serviços sabidamente confiáveis são disponibilizados. Precisamos tomar as devidas providências para que cada serviço a ser suportado funcione adequadamente;
- *Tudo o que não é expressamente proibido é permitido:* Neste caso, somente os serviços considerados inseguros ou não confiáveis são desabilitados.

A primeiro paradigma é claramente mais seguro: o sistema não fica sujeito a falhas de segurança associadas a serviços desnecessários ou pouco conhecidos e as falhas de segurança não documentadas provenientes dos serviços disponibilizados podem ser mais facilmente isoladas e contornadas.

Contudo, o usuário sofre uma perda mais sensível de flexibilidade: vários serviços deixarão de estar a sua disposição e alguns outro que, apesar de estarem disponíveis, podem apresentar-se limitados.

3. Objetivos

Existem vários pacotes comercialmente disponíveis que exercem a função de *Firewall*. Entretanto, estes pacotes impõem uma política de segurança para ambientes de trabalho muito específicos, normalmente empresas. Não existe um pacote de *Firewall* que seja destinado exclusivamente para o uso em ambiente acadêmico. Esta limitação é natural: a topologia de rede, o ambiente de trabalho, o perfil e a necessidade dos usuários determinam a política de segurança para o ambiente em questão.

Este trabalho tem por objetivo propor e implantar uma política de segurança efetiva e operacional para um ambiente acadêmico, em específico uma política que atenda as necessidades do nosso Departamento. Traduzindo em tarefas, esta política consiste de:

- Reestruturação da topologia física da rede do DCC, de forma a suportar um mecanismo de *Firewall*;
- Reconfiguração dos serviços a serem disponibilizados, de forma a torna-los mais seguros e a controlar o acesso a eles;
- Reestruturação lógica da rede interna, subdivisão em sub-redes por grupo de usuários, reestruturação dos serviços internos e reconfiguração individual das estações;

3.1 A Política externa

Inicialmente, pretende-se separar a nossa rede interna da *Internet* através de um mecanismo de *Firewall* baseado *proxies*. A palavra *proxy* significa, no inglês, procurador, ou seja, aquele indivíduo que realiza alguma tarefa em nome de um segundo. No âmbito computacional, o sentido é bem similar. Por exemplo, um *proxy HTTP* é aquela estação que efetua a busca de documentos **WWW** em nome de uma segunda estação, com a vantagem de que o acesso pode ser limitado tendo como base o endereço de origem das requisições ou até mesmo o endereço de destino.

Pretendemos adotar o mecanismo de *proxy* para cada serviço a ser suportado de forma a controlar todo o tráfego de entrada para a rede do **DCC**. *Proxies* para os serviços mais básicos como *smtp*, *ftp* e *telnet* estão publicamente disponíveis na *Internet*, bem como *proxies* genéricos para adaptação a outros protocolos, como **HTTP** e **NNTP**. Mais
Mais informações podem ser encontradas em [Ranum and Avolio, 1992].

Dentre as topologias de *Firewall* apresentadas em [Wack and Carnahan, 1995], escolhemos a que é denominada como *Screened Subnet*. Esta topologia consiste de uma sub-rede separada da *Internet* e da rede interna por dois roteadores, conforme pode ser visto na figura 1. Esta sub-rede é chamada de *linha de fogo* em alusão ao fato de que as máquinas nesta sub-rede são as únicas que podem ser alcançadas a partir da rede externa e que, portanto, estão sujeitas a ataque. Nesta sub-rede são colocados os servidores que provêm os serviços à comunidade externa, todo o software que exerce a função de *Firewall* e os mecanismos de geração de relatórios para posterior acompanhamento e auditoria. Nestas estações deve estar instalado somente o básico e estritamente necessário em termos de software. Nos roteadores são configuradas listas de acesso de forma a garantir que as conexões provenientes da rede externa sejam destinadas somente às estações na *linha de fogo* e somente nas portas **TCP** que oferecem serviços. Somente ao operador é autorizado o uso destas estações que não permitem acesso remoto: toda atividade de manutenção deve ser feita obrigatoriamente no console da estação, a fim de garantir a integridade das mesmas.

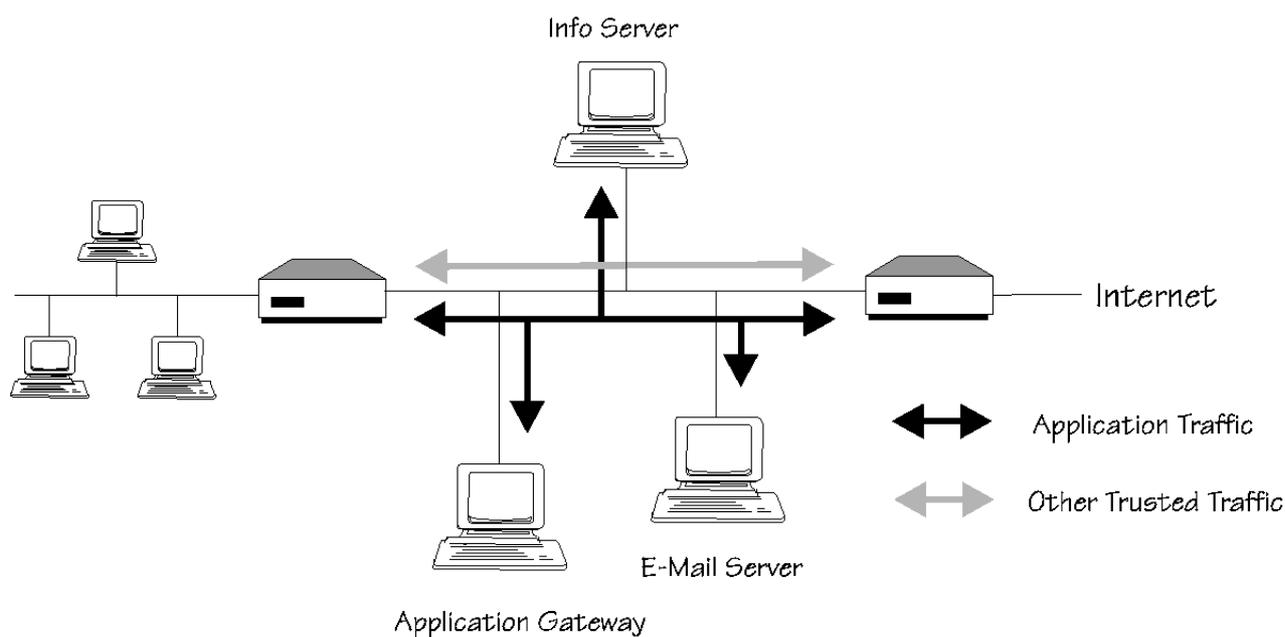


Figura 1. Uma rede com a topologia Screened Subnet.

Para acesso remoto, seja por acesso discado ou conexões telnet, acreditamos que os atuais mecanismos de autenticação do tipo *login/password* são muito vulneráveis. Por experiência, podemos afirmar que a grande parte dos incidentes de segurança ocorrem por culpa de senhas frágeis ou do próprio protocolo de comunicação, que não é confiável: a senha digitada remotamente atinge o seu destino sem nenhum tipo de autenticação, podendo ser facilmente capturada por softwares do tipo *sniffer*, que capturam pacotes que trafegam na rede.

Para contornar o problema, pretendemos utilizar um mecanismo de *autenticação forte*. Tal autenticação é feita através de algum mecanismo que não permita quebra de senhas através de dicionários ou captura por programas do tipo *sniffer*. Por exemplo, o **S/Key** da **Bellcore Labs** (<http://www.bellcore.com>), é um mecanismo de autenticação baseado em desafio e resposta: a cada tentativa de login, o servidor pede uma senha com um número de série *n*. O usuário deve então responde com a senha correspondente e é autenticado. O usuário possui então uma lista de senhas, geradas por um programa cliente do **S/Key**, cada uma válida por apenas por uma autenticação.

Com um mecanismo de segurança operacional que isola as falhas de segurança da rede interna e um procedimento de acesso remoto apropriado, podemos partir para a reconfiguração de nossas máquinas e implantar uma política de segurança interna.

3.2 A política interna

O *Firewall* é um mecanismo que funciona muito bem quando se trata de ataques cuja origem está além dos seus limites. Entretanto, quando o ataque tem como origem e destino máquinas situadas na rede interna, o *Firewall* não tem nenhuma utilidade. No caso particular do nosso departamento, a maioria dos ataques estão situados nesta classe.

Cada estação de trabalho precisa ter seu sistema operacional reconfigurado e os serviços desnecessários desabilitados. Esta reconfiguração consiste em aplicar os *patches* de segurança para cada arquitetura e cada sistema operacional disponível no parque computacional do departamento, a fim de garantir a integridade e a confiabilidade de cada ponto de acesso. Os *patches* são normalmente disponibilizados pelos fabricantes dos sistemas e podem ser facilmente obtidos junto a eles.

Outra postura interessante a ser adotada é a separação do parque computacional do departamento de forma que cada grupo de usuários tenha acesso controlado a cada sub-rede, Por exemplo, haveria uma sub-rede destinada à utilização por alunos e estes poderiam acessar somente os recursos desta sub-rede. Aos professores estaria reservada uma segunda sub-rede, de forma que nenhum aluno tivesse acesso aos seus recursos. Finalmente, uma terceira sub-rede seria destinada a administração dos recursos e somente o pessoal autorizado teria acesso a suas máquinas. O sistema seria hierárquico, de forma que alunos acessariam somente a primeira sub-rede, professores acessariam a segunda e a primeira e administração acessaria as três. Entretanto, muitos aspectos ainda precisam ser abordados e estudados. Por exemplo, recursos de um laboratório são compartilhados por um subconjunto de alunos e professores, não havendo uma separação clara entre classes. Casos como esses ainda precisam ser abordados para que um solução satisfatória seja encontrada.

Acreditamos ser inapropriada a implantação de mecanismos de *autenticação forte* na rede interna pois o custo em flexibilidade suplantaria o benefício em segurança.

4. Comentários

Para o sucesso de qualquer investimento no setor de segurança, é de vital importância a conscientização dos usuários. De nada adianta uma política de segurança, por mais bem comportada e fundamentada que seja, se os usuários não estão dispostos a aceitar e conviver com ela.

Este trabalho não tem a pretensão de criar um ambiente de trabalho totalmente seguro. Mesmo em um ambiente empresarial, governamental ou militar, onde as restrições de segurança são muito mais rígidas e prioritárias em relação a flexibilidade, não é possível criar um ambiente com tal nível de segurança. Como já foi mencionado, trabalhamos em um ambiente acadêmico, onde o objetivo é conciliar a segurança e a flexibilidade. *Um ambiente de trabalho 100% seguro é aquele que não está conectado, sob nenhum aspecto, a outro sistema computacional.*

5. Referências Bibliográficas

[Wack and Carnahan, 1995] John P. Wack and Lisa J. Carnahan - *“Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls”*, National Institute of Standards and Technology, Special Publication 800-10, 1995.

[Kostick and Mancuso, 1995] Chris Kostick and Matt Mancuso - *“Firewall Performance Analysis Report”*, Computer Sciences Corporation, Secure Systems Center - Network Security Department, Hanover, MD, 1995.

[Ranum, 1992] Marcus J. Ranum - *“A Network Firewall”*, Digital Equipment Corporation, Washington Open Systems Resource Center, Greenbelt, MD, 1992.

[Cheswick, 1991] Bill Cheswick - *“The Design of a Secure Internet Gateway”*, AT&T Bell Laboratories, Murray Hill, NJ, 1991.

[Schauer and Wolfhugel, 1991] Hervé Schauer and Christophe Wolfhugel - *“An Internet Gatekeeper”*, 1991.

[Safford, Schales and Hess, 1993] David R. Safford, Douglas Lee Schales and David K. Hess - *“The TAMU Security Package: An Ongoing Response to Internet Intruders in an Academic Environment”*, Supercomputer Center - Texas A&M University, College Station, TX, 1993.

[Ranum and Avolio, 1992] Marcus J. Ranum and Frederick M. Avolio - *“A Toolkit and Methods for Internet Firewalls”*, Trusted Information Systems, Inc., Glenwood, MD, 1992.

[Avolio and Ranum, 1992] Frederick M. Avolio and Marcus J. Ranum - *“A Network Perimeter with Secure External Access”*, Trusted Information Systems, Inc., Glenwood, MD, 1992.

[Chapman, 1994] D. Brent Chapman - *“Network Security Through IP Packet Filtering”*, Great Circle Associates, Mountain View, CA, 1994.

[Ranum, 1993] Marcus J. Ranum - *“Thinking About Firewalls”*, Trusted Information Systems, Inc., Glenwood, MD, 1993.

[Muffett, 1994] Alec Muffett - *“Proper Care and Feeding of Firewalls”*, Sun Microsystems, UK, 1994.

[Treese and Wolman, 1993] G. Winfield Treese and Alec Wolman - *“X Through the Firewall and Other Application Relay”*, Digital Equipment Corporation - Cambridge Research Lab, 1993.

[Robinson, 1994] Andrew T. Robinson - *“Internet Firewalls: An Introduction”*, netMAINE, Inc., Portland, ME, 1994.

[Livingstone, 1995] *“Firewall Application Notes”*, Livingstone Enterprises, Inc., 1995.

[Bellovin, 1993] Steven M. Bellovin - *“Packets Found on an Internet”*, AT&T Bell Laboratories, Murray Hill, NJ, 1993.

[Bellovin, 1992] Steven M. Bellovin - *“There Be Dragons”*, AT&T Bell Laboratories, Murray Hill, NJ, 1992.

[**Bellovin, 1992**] Steven M. Bellovin - “*Security Problems in the TCP/IP Protocol Suite*”, AT&T Bell Laboratories, Murray Hill, NJ, 1993.

[**Farmer and Venema, 1994**] Dan Farmer and Wietse Venema – “*Improving the Security of Your Site by Breaking Into It*”, 1994.

[**Curry, 1990**] David A. Curry – “*Improving the Security of Your UNIX System*”, SRI International, Menlo Park, CA, 1990.

[**Morris, 1985**] Robert T. Morris – “*A Weakness in the 4.2 BSD UNIX TCP/IP Software*”, AT&T Bell Laboratories, Murray Hill, NJ, 1985.

[**Ranum, Leibowitz, Chapman and Boyle, 1994**] Marcus J. Ranum, Allen Leibowitz, Brent Chapman and Brian Boyle - “*Internet Firewalls Frequently Asked Questions*”, 1994.

[**Grennan, 1996**] Mark Grennan - “*Firewalling and Proxy Server HOWTO*”, 1996.

[**Venema, 1992**] Wietse Venema – “*TCP Wrapper: Network Monitoring, Access Control and Booby Traps*”, Mathematics and Computing Science – Eindhoven University of Technology, Netherlands, 1992.

[**Cornwall, 1985**] Hugo Cornwall - “*The Hackers Handbook*”, Century Communications Ltd., London, UK, 1985.

[**Hugues, 1995**] Larry J. Hugues Jr. – “*Actually Useful Internet Security Techniques*”, New Riders Publishing, Indianapolis, IN, 1995.

[**Russell and Gangemi, 1991**] Deborah Russell and G. T. Gangemi Sr. - “*Computer Security Basics*”, O’Reilly & Associates, Inc., 1991.

[**Garfinkel and Spafford, 1991**] Simson Garfinkel and Gene Spafford - “*Practical Unix Security*”, O’Reilly & Associates, Inc., 1991.

[**Stevens, 1994**] W. Richard Stevens - “*TCP/IP Illustrated*”, Addison-Wesley, Vol. 1, 1994.